

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

IN RE: CONDUENT BUSINESS SERVICES
DATA BREACH LITIGATION

Case No. 2:25-cv-16953 (MEF) (MAH)

JURY TRIAL DEMANDED

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs identified below (“Plaintiffs”) bring this Amended Consolidated Class Action Complaint (“Consolidated Complaint”) on behalf of themselves and all others similarly situated against Defendants Conduent Business Services, LLC, Conduent State & Local Solutions, Inc., and Conduent Incorporated (collectively, “Conduent”); and Defendants AIG Procurement Services, Inc. (“AIGPS”), The Cigna Group, Inc. (“Cigna”), Elevance Health, Inc. (“Elevance”), Health Care Services Corporation (“HCSC”), Humana, Inc. (“Humana”), and John Doe I through X (an entity or entities whose identity is not known) (collectively, “Insurer Defendants”), alleging as follows.

NATURE OF THE ACTION

1. This action arises from a significant hub-and-spoke data breach that exposed the personally identifiable information (“PII”) and protected health information (“PHI”) (collectively, “Private Information”) of at least 44.4 million individuals. The breach and ensuing harm to Plaintiffs and Class Members resulted from Defendants’ collective failure to implement basic data security measures or provide timely notification to affected individuals.

2. Conduent is a New Jersey-based company that handles and processes vast amounts of personal and sensitive information on behalf of large corporations, government departments, and several U.S. states. “Each day,” Conduent reports, “our solutions and services interact in the lives of millions of people in many ways.”¹ In fact, Conduent’s technology and operational support services impact more than two-thirds of all insured patients in the U.S., and more than 100 million people in the U.S. across various government healthcare programs.

3. Insurer Defendants are HIPAA-covered entities that contract for Conduent’s administrative and data processing services for the health plans they furnish. AIGPS is part of an

¹ *Annual Report*, CONDUENT (2024), p. 3, at <https://investor.conduent.com/static-files/0d42fa22-18cf-4ae8-995d-9b15cf5e5790>.

industry-leading, global general insurance organization that had \$24 billion in net premiums written in 2024. Cigna is a global health service company with over 73,000 employees, serving more than 182 million customers. Elevance is one of the largest health insurers in the country and provides Anthem Blue Cross and Blue Shield health plans in 14 states. HCSC furnishes Blue Cross and Blue Shield plans in five states, and is the fifth-largest health plan nationally in terms of membership (18.6 million members), and the sixth-largest based on premiums (\$64 billion at 2024 close). Humana is among the top five U.S. health insurers.

4. To receive services from Conduent and to reduce their own costs, Insurer Defendants provide Conduent, and Conduent collects, processes, and stores, Plaintiffs' and Class Members' Private Information. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion and to promptly notify customers if a breach occurs.

5. Despite Conduent's and its Insurer-Defendant clients' duties to Plaintiffs and Class Members, Conduent stored Plaintiffs' and Class Members' Private Information on an internet accessible network that lacked appropriate credential management, encryption, multi-factor authentication, network segregation, and intrusion detection, causing and allowing cybercriminals to target, access, and steal millions of confidential personal records without meaningful resistance. Further, Insurer Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks, including, but not limited to, adequately vetting, auditing, and monitoring Conduent's cybersecurity practices.

6. Beginning on or about October 21, 2024, cybercriminals infiltrated Conduent's network using credentials for a single compromised account and—due to Conduent's grossly inadequate security controls and Insurer Defendants' failure to audit or monitor Conduent's data security—maintained undetected access for nearly three months (the "Data Breach" or "Breach"). During the Data Breach, the hackers targeted, accessed, and stole at least 8.5 terabytes of unencrypted confidential data, including at least 44.4 million individuals' Private Information. The compromised Private Information includes Plaintiffs' and Class Members' names, Social Security numbers, medical information, and health insurance information.

7. Conduent did not detect the Data Breach until January 13, 2025, when significant service disruptions—likely caused by deployed ransomware—finally alerted it to the ongoing attack. After Conduent assured corporate clients in January 2025 that it had secured its network and neutralized the threat, it received a ransom demand from the notorious SafePay ransomware gang in February 2025. In a publicly-available post to its dark web leaksite, SafePay boasted about stealing 8.5T of zipped data from Conduent in the Data Breach, and demanded that Conduent pay an undisclosed ransom within three days while threatening to make the stolen files available on the dark web if Conduent did not comply.

8. On or about April 9, 2025, three months after discovering the Data Breach, Conduent reported the Breach via a Form 8-k Filing with the United States Securities and Exchange Commission ("Form 8-K Notice"). The Form 8-K Notice did not mention the February ransom demand or Conduent's response, nor did it disclose how the Data Breach happened, how many people were impacted, or who might be at risk.

9. Defendants' failures to act as responsible or reasonable guardians of sensitive Private Information continued after the Data Breach, when they made the calculated decision to

protect their own financial and reputational interests by withholding critical information from the very people whose data they failed to secure. Rather than move swiftly to mitigate the mounting harm, Defendants adopted and continue to employ a posture of concealment and delay.

10. Although Conduent informed its Insurer-Defendant clients of the Data Breach within days of discovering it, Defendants did not begin notifying victims or regulators until October 24, 2025—more than 10 months after detection, and more than an entire year after the Data Breach—and Defendants do not expect to send out all victim notifications until April 15, 2026. That timeline is not the product of diligence. Timely notice is the cornerstone of modern data-breach response, and Defendants’ refusal to provide it despite full knowledge of the ongoing risk directly and foreseeably magnified the harm Plaintiffs and Class Members suffered.

11. Defendants’ abject failure to timely notify victims left millions of Americans exposed, uninformed, and completely unprotected from identity theft, fraud, and other foreseeable harms that timely disclosure would have helped prevent. In their notices to victims of the Data Breach, Defendants attempt to excuse their nearly year-long delay by claiming it “took time” to determine whose information was compromised. But this explanation only underscores the severity of Defendants’ failures: no organization entrusted with the sensitive data of hundreds of millions of Americans should ever be so incapable of identifying whose information it holds or whether that information has been exfiltrated. As one report on the Data Breach explains, “Security experts point to this as a wake-up call for govtech oversight. When a contractor serving 100 million Americans can get breached without immediately disclosing the full scope, something’s broken in the notification and accountability process.”²

² *Conduent Breach Explodes: 25M+ Americans Hit in Govtech Hack*, THE TECH BUZZ (Feb. 5, 2026), at <https://www.techbuzz.ai/articles/conduent-breach-explodes-25m-americans-hit-in-govtech-hack>.

12. To this day, Conduent has failed to provide a definitive nationwide accounting of the Data Breach victims affected. Since Conduent first disclosed the Data Breach to regulators in October 2025, the reported number of impacted individuals has exploded from approximately 10 million to at least 44.4 million and continues to rise. In Texas alone, state officials now estimate 15.4 million residents were affected—about half the state’s population and nearly quadruple the 4 million Conduent originally reported. Conduent admits it is still analyzing affected files to determine whose data was taken, while declining to say how many notifications have issued. When reporters asked Conduent in February whether the total number of victims could approach 100 million, “Conduent went radio silent.”³

13. Even at the most recent numbers, the Data Breach stands as the largest healthcare data breach of 2025 and the third-largest healthcare data breach in United States history.

14. As a result of the Data Breach and Defendants’ failure to provide proper notification, Plaintiffs’ and Class Members’ Private Information has already been misused: SafePay hackers targeted the Private Information on Conduent’s systems, stole it, and held it for ransom, threatening to disclose the highly sensitive data to an untold number of nefarious actors on the dark web if Conduent did not pay up. Even if Conduent paid a ransom, attackers often leak or sell the data regardless because there is no way to verify if copies of the data are destroyed; thus it should be “assume[d]” that Plaintiffs’ and Class Members’ Private Information “will be traded to other threat actors, sold, or held for a second/future extortion attempt.”⁴ Consequently, Plaintiffs and Class Members face current and an imminent and substantial risk of fraud, identity theft, and

³ *Id.*

⁴ Lawrence Abrams, *Data leak marketplaces aim to take over the extortion economy*, BLEEPING COMPUTER (May 7, 2021), at <https://www.bleepingcomputer.com/news/security/data-leak-marketplaces-aim-to-take-over-the-extortion-economy/>.

other harms caused by the unauthorized disclosures of their Private Information—a risk that may last for the rest of their lives. Plaintiffs and Class Members must devote time, money, and energy to protect themselves, to the extent possible, from these harms.

15. Plaintiffs bring this action on behalf of themselves and all others similarly situated to hold Defendants accountable for their reckless disregard for consumer privacy, failure to timely notify affected individuals of the Data Breach, and failure to take adequate steps to mitigate the ongoing harm resulting from their Private Information’s wrongful disclosure, all of which injured and continues to injure Plaintiffs and Class Members.

16. Through this action, Plaintiffs seek compensatory damages, exemplary damages, statutory damages, equitable relief including improved data security practices, identity protection and credit monitoring services, and all other relief the Court deems just and appropriate to redress Defendants’ unlawful conduct and to prevent such harm from recurring.

PARTIES

A. Plaintiffs

AIGPS Plaintiffs

17. Plaintiff Russell Dejulio is a natural person and citizen of Pittsburgh, Pennsylvania, where he intends to remain.

18. Plaintiff Alvin Luckett is a natural person and citizen of Spring, Texas, where he intends to remain.

19. Plaintiffs Dejulio and Luckett are hereinafter referred to collectively as “AIGPS Plaintiffs.”

Cigna Plaintiff

20. Plaintiff Karina Lopez is a natural person and citizen of Kissimmee, Florida, where she intends to remain.

Elevance Plaintiffs

21. Plaintiff Rashell Chambers is a natural person and citizen of Lincoln, California, where she intends to remain.

22. Plaintiff Suzan Kirkland is a natural person and citizen of Carpinteria, California, where she intends to remain.

23. Plaintiff Marc Powell is a natural person and citizen of Sacramento, California, where he intends to remain.

24. Plaintiff Lakrishna Long is a natural person and citizen of Decatur, Georgia, where she intends to remain.

25. Plaintiff Anthony Meyer is a natural person and citizen of Columbia Missouri, where he intends to remain.

26. Plaintiff Richard Helm Jr. is a natural person and citizen of Forest Grove, Oregon, where he intends to remain.

27. Plaintiffs Powell, Long, Meyer, and Helm Jr. are hereinafter referred to collectively as “Elevance Plaintiffs.”

HCSC Plaintiffs

28. Plaintiff James Hurd is a natural person and citizen of Millry, Alabama, where he intends to remain.

29. Plaintiff Nathan Cornwell is a natural person and citizen of Almeida, California, where he intends to remain.

30. Plaintiff Jason Frost is a natural person and citizen of Lake Mary, Florida, where he intends to remain.

31. Plaintiff Andrea Rodriguez, on behalf of her minor child, A.R., is a natural person and citizen of West Palm Beach, Florida, where she intends to remain.

32. Plaintiff Anita Burton is a natural person and citizen of Chicago, Illinois, where she intends to remain.

33. Plaintiff Andrea Oliver-Alexander is a natural person and citizen of Chicago, Illinois, where she intends to remain.

34. Plaintiff Rachel Zafra is a natural person and citizen of River Grove, Illinois, where she intends to remain.

35. Plaintiff Kerri Cromer is a natural person and citizen of Danville, Indiana, where she intends to remain.

36. Plaintiff Kevin McShane is a natural person and citizen of Prairie Village, Kansas, where he intends to remain.

37. Plaintiff Tina Gustin is a natural person and citizen of Peabody, Massachusetts, where she intends to remain.

38. Plaintiff Kevin Amende is a natural person and citizen of Bozeman, Montana, where he intends to remain.

39. Plaintiff Amanda Dunn is a natural person and citizen of Helena, Montana, where she intends to remain.

40. Plaintiff Brian Marshall is a natural person and citizen of Woodbridge, New Jersey, where he intends to remain.

41. Plaintiff Michelle Dupuis-Nilsen is a natural person and citizen of Sanford, North Carolina, where she intends to remain.

42. Plaintiff Andrew Cook is a natural person and citizen of Twinsburg, Ohio, where he intends to remain.

43. Plaintiff Emily Gresh is a natural person and citizen of Edmond, Oklahoma, where she intends to remain.

44. Plaintiff Richard Acosta is a natural person and citizen of San Antonio, Texas, where he intends to remain.

45. Plaintiff Ricardo Alamilla is a natural person and citizen of North Richland Hills, Texas, where he intends to remain.

46. Plaintiff Phillip Groll, Jr. is a natural person and citizen of Corpus Christi, Texas, where he intends to remain.

47. Plaintiff Alexis Jackson is a natural person and citizen of Great Falls, Montana, where she intends to remain.

48. Plaintiff Teresa Jones is a natural person and citizen of Dallas, Texas, where she intends to remain.

49. Plaintiff Jared Poli is a natural person and citizen of Houston, Texas, where he intends to remain.

50. Plaintiff Paul Snow is a natural person and citizen of Bellaire, Texas, where he intends to remain.

51. Plaintiff Wesley Triphahn is a natural person and citizen of Pingree Grove, Illinois, where he intends to remain.

52. Plaintiff Andrea Young is a natural person and citizen of Houston, Texas, where she intends to remain.

53. Plaintiffs Hurd, Cornwell, Frost, Rodriguez, Burton, Oliver-Alexander, Zafra, Cromer, McShane, Gustin, Amende, Dunn, Marshall, Dupuis-Nilsen, Cook, Gresh, Acosta, Alamilla, Groll, Jr., Jackson, Jones, Poli, Triphahn, and Young are hereinafter referred to collectively as “HCSC Plaintiffs.

Humana Plaintiff

54. Plaintiff Peggi Bordelon is a natural person and citizen of Metairie, Louisiana, where she intends to remain.

B. Defendants

55. Defendant Conduent Incorporated is a New York company with its principal place of business located at 100 Campus Drive, Suite 200, Florham Park, New Jersey 07932.

56. Defendant Conduent Business Services, LLC is a Delaware limited liability company with its principal place of business located at 100 Campus Drive, Suite 200, Florham Park, New Jersey 07932.

57. Defendant Conduent State & Local Solutions, Inc., formerly Xerox State & Local Solutions, Inc., is a New York corporation with its principal place of business located at 100 Campus Drive, Suite 200, Florham Park, New Jersey 07932.

58. Each Insurer Defendant, listed below, contracted with Conduent as a business associate for Conduent to provide such Insurer Defendants with back-office services.

59. Defendant AIGPS is a Delaware corporation with its principal place of business located at 1271 Avenue of the Americas, New York, New York 10020, and is registered to do business in the state of New Jersey.

60. Defendant Cigna is a Delaware corporation with its principal place of business located at 900 Cottage Grove Rd., Bloomfield, CT 06002.

61. Defendant Elevance is an Indiana corporation with its principal place of business located at 220 Virginia Avenue, Indianapolis, Indiana 46204. Prior to June 2022, Elevance was named Anthem, Inc.

62. Defendant HCSC is an Illinois corporation with its principal place of business located at 300 E. Randolph St., Floor 4, Chicago, Illinois, 60601. HCSC has no parent corporation and no publicly-held owners.

63. Defendant Humana is a Delaware corporation with its principal place of business located at 500 West Main Street, Louisville, Kentucky 40202, and is registered to do business in the state of New Jersey.

64. In addition to the foregoing Insurer Defendants, a number of other Conduent clients provided their customers' PII and/or PHI to Conduent, which Private Information was also compromised in the Data Breach. Defendants John Doe (I through X) represent these entities whose identities are not currently known to Plaintiffs.

JURISDICTION AND VENUE

65. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action in which at least one member of the proposed Class is a citizen of a state different from that of at least one Defendant; the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs; and the proposed class comprises more than 100 Class Members.

66. The Court has personal jurisdiction over Defendants because Defendants engage in substantial and not isolated activity in this state, Plaintiffs' claims arise from Defendants' acts and omissions in this state and a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this state, and Conduent is a citizen of this state.

67. Pursuant to 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District, Conduent resides in this District, and Defendants have harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

I. Defendants Collect, Store, and Share Plaintiffs’ and Class Members’ Private Information.

A. Conduent

68. Conduent provides third-party business processing, software, and back-office support services to HIPAA-covered entities and government agencies. Since its formation in 2017, after Xerox Corporation’s divestiture of Conduent’s previous incarnation, Affiliated Computer Services, Conduent has reported generating annual revenues between \$3–6 billion.

69. Conduent manages the business processes and end-user interactions for “[n]early half of Fortune 100 companies and more than 600 government and transportation agencies.”⁵ Conduent estimates its “addressable market size in the global business process services industry” was “\$210 billion in 2024.”⁶ Conduent holds itself out as a “widely recognized . . . leader in healthcare payer operations, serving 9 of the top 10 U.S. health plans and providing administrative and mission-critical program administration solutions for government healthcare programs serving 119 million recipients in 34 states and the District of Columbia.”⁷

⁵ *About-Conduent*, CONDUENT, https://www.conduent.com/about-conduent/?_gl=1*cypztj*_up*MQ.*_ga*MTUyMjIyMTY2Ni4xNzYxNzY1OTY0*_ga_21KB (last visited Dec. 29, 2025).

⁶ *Annual Report*, CONDUENT (2024), at 5, <https://investor.conduent.com/static-files/0d42fa22-18cf-4ae8-995d-9b15cf5e5790>.

⁷ *Id.* at 9.

70. Conduent’s services include “administration, clinical support, claims management, and patient assistance solutions across the healthcare ecosystem to reduce costs, increase compliance and enhance utilization.”⁸ Conduent boasts that its technology and services “reduce costs, improve efficiencies, and enable revenue growth” for its corporate clients.⁹ Additionally, Conduent provides data mining and analytics technologies and services using its clients’ customers PII and PHI, for marketing and other purposes.

71. Conduent also provides services and solutions to U.S., federal, state, local, and foreign governments for public assistance, healthcare programs and administration, transaction processing, payment services, and case management. These services include “program administration solutions for government healthcare programs . . . such as Medicaid management, provider services, Medicaid business intelligence, pharmacy benefits management, eligibility and enrollment support, customer contact services, application processing, premium billing and case management solutions.”¹⁰ In 2024 alone, Conduent processed nearly 450 million claims.

72. Conduent also holds itself out as “a leader in government payment disbursements for federally sponsored programs including benefit card programs and payment card programs[.]” reporting “approximately \$85 billion disbursed annually.”¹¹ Further, Conduent offers “a broad set of child support services predominately to State Disbursement Units (‘SDUs’), including processing and distributing payments, child support payment cards, childcare credentialing and case management, among others, to help states comply with federal standards.”¹²

⁸ *Id.* at 7.

⁹ *Id.* at 6.

¹⁰ *Id.* at 8.

¹¹ *Id.*

¹² *Id.*

73. In the ordinary course of its business, Conduent obtains, stores, maintains, and uses Plaintiffs' and Class Members' Private Information.

74. Conduent collects Plaintiffs' and Class Members' Private Information to operate its business and to provide the contracted technology and services that are the source of Conduent's revenue, including software and services for the specific purpose of managing and processing Plaintiffs' and Class Members' Private Information.

75. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Conduent assumed legal and equitable duties and knew or should have known that it was responsible to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

B. Insurer Defendants

1. *AIGPS*

76. AIGPS is the internal Global Sourcing & Procurement Services department within American International Group, Inc., a leading global insurance company that serves millions of commercial and individual insurance customers throughout the United States.

77. AIGPS is part of a global insurance conglomerate that wrote \$24 billion in net premiums in 2024 alone, with customers across the United States and operations in over 200 countries. AIGPS contracts with Conduent to provide various digital business solutions for American International Group, Inc. and its subsidiaries and affiliates ("AIG"), such as front-end digitization services, payment integrity audits, and printing/mailroom services.

2. *Cigna*

78. Cigna is a global health service company with over 73,000 employees who serve more than 182 million customers, including in Florida, Illinois, Massachusetts, New York and beyond.

79. Cigna has two growth platforms: Evernorth Health Services® (“Evernorth”) and Cigna Healthcare® (“Cigna Healthcare”). Evernorth, through Cigna’s Pharmacy Benefit Services and Specialty and Care Services operating segments, provides independent and coordinated health solutions and capabilities. Cigna Healthcare is the health benefits segment of The Cigna Group and serves customers for both Cigna’s U.S. Healthcare and International Health operating segments. According to Cigna’s public filings, Evernorth and Cigna Healthcare work in tandem to enable cross-enterprise leverage to meet the customers’ needs.

80. Cigna provides services to managed care organizations, health insurers, third-party administrators, employers, union-sponsored benefit plans, workers’ compensation plans, government health programs, providers, clinics, hospitals and others. Additionally, Cigna’s investment operations provide investment management and related services for its various businesses, including the insurance-related invested assets.

3. *Elevance*

81. Elevance, founded in 1946 as Anthem, Inc., is one of the largest health insurers in the United States, serving approximately 45.7 million medical members through its affiliated health plans. Elevance is an independent licensee of the Blue Cross and Blue Shield Association, and provides Blue Cross Blue Shield (“BCBS”) health plans in 14 states.

82. Elevance is one of two BCBS licensees for California, providing Anthem Blue Cross plans in that state. Elevance is also the BCBS licensee for Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri (excluding 3 counties in the Kansas City area), Nevada, New Hampshire, New York (in the New York City metropolitan area and upstate New York), Ohio, Virginia (excluding the Northern Virginia suburbs of Washington, D.C.) and Wisconsin, and provides Anthem BCBS plans in these states. Elevance also conducts business through arrangements with other BCBS licensees, as well as other strategic partners.

83. In addition, Elevance serves members in numerous states, doing business as Wellpoint, Carelon, MMM and/or Simply Healthcare. Elevance is licensed to conduct insurance operations in all 50 states, the District of Columbia, and Puerto Rico through its subsidiaries. Elevance also offers pharmacy services through its CarelonRx business, and other healthcare related services as Carelon Service.

84. Elevance offers a broad range of network-based managed care risk-based plans to individual, employer group, Medicaid and Medicare markets. In addition, Elevance provides a broad array of managed care services to fee-based customers, including claims processing, stop loss insurance, provider network access, medical management, care management, wellness programs, actuarial services and other administrative services.

85. Elevance provides services to the federal government in connection with its Federal Health Products & Services business, which administers the Federal Employee Program®. Elevance also provides an array of specialty services both to customers of its subsidiary health plans and to unaffiliated health plans, including pharmacy services, stop loss insurance, dental, vision and supplemental health insurance benefits, as well as integrated health services.

86. Upon information and belief, Elevance provides administrative services for Anthem BCBS plans, including services related to information technology and cybersecurity. In 2022, Elevance was paid over \$1 billion in total for the administrative services it provided to Anthem BCBS plans that year. Upon information and belief, in providing information technology and cybersecurity services for Anthem BCBS plans, Elevance received, handled, and oversaw the data security for those plan members' Private Information.

87. Conduent provided administrative and data processing services for each of Elevance’s Anthem BCBS plans, and, as a result, members of each of these health plans were impacted by the Data Breach.

4. HCSC

88. HCSC is one of the largest health insurers in the United States, serving over 26 million members through its BCBS plans in Illinois, Montana, New Mexico, Oklahoma, and Texas.

89. As an independent licensee of the Blue Cross and Blue Shield Association, HCSC operates BCBS of Illinois (“BCBSIL”), BCBS of Montana (“BCBSMT”), BCBS of New Mexico (“BCBSNM”), BCBS of Oklahoma (“BCBSOK”), and BCBS of Texas (“BCBSTX”).

90. BCBSIL serves more than 8.9 million members.

91. BCBSMT serves more than 300,000 members.

92. BCBSNM serves over 700,000 members.

93. BCBSOK serves approximately 850,000 members.

94. BCBSTX serves approximately 10.4 million members.

95. Conduent provided “mailroom, payment and other back-office support services” for each of HCSC’s BCBS plans, and, as a result, members of each of these health plans were impacted by the Data Breach.¹³

5. Humana

96. Humana is a leading provider of health insurance services in the United States. As of December 31, 2024, Humana had approximately 16 million members in its medical benefit plans, as well as approximately 5 million members in its specialty products. Humana’s medical

¹³ See, e.g., *Update on Conduent Cyber Incident*, BCBSIL (Oct. 24, 2025), at <https://www.bcbsil.com/about-us/alerts-and-announcements/10-24-25-update-conduent-cyber-incident>.

and specialty insurance products allow members to access health care services primarily through the company's networks of health care providers. In addition, Humana offers health and wellness services to its health plan members and third parties, including pharmacy solutions, primary care, and home solutions.

97. Humana's insurance segment is comprised of insurance products serving Medicare and state-based contract beneficiaries, as well as individuals and employers. This segment also includes Humana's Pharmacy Benefit Manager business. Humana has participated in the Medicare program for private health plans for over 30 years and has established a national presence, offering at least one type of Medicare plan in all 50 states.

98. The majority of Humana's services revenue is derived from its contracts with the federal government, including individual Medicare Advantage contracts in Florida with the Centers for Medicare and Medicaid Services ("CMS"). Humana contracts with CMS under the Medicare Advantage program to provide health insurance benefits, including wellness programs, chronic care management, and care coordination, to Medicare-eligible persons under HMO, PPO, Private Fee-For-Service, or PFFS, and Special Needs Plans, including Dual-Eligible Special Needs Plans, in exchange for contractual payments received from CMS. As of December 31, 2024, Humana provided health insurance coverage under CMS contracts to approximately 5,661,800 individual Medicare Advantage members, including approximately 924,800 members in Florida.

99. Through its state-based contracts, Humana serves members enrolled in Medicaid, a program funded by both the federal and state governments and administered by states to care for their most vulnerable populations. Humana has contracts in multiple states to serve Medicaid-eligible members, including Florida, Kentucky, Illinois, Indiana, Louisiana, Ohio, Oklahoma, South Carolina, and Wisconsin.

100. Humana also serves members who qualify for both Medicaid and Medicare, through its Medicaid, Medicare Advantage, and stand-alone prescription drug plans (“PDPs”). Humana offers PDPs under Medicare Part D, including a PDP offering co-branded with Walmart Inc., or the Humana-Walmart plan. Additionally, Humana offers products that enable employers that provide post-retirement health care benefits to replace Medicare wrap or Medicare supplement products with Medicare Advantage or stand-alone PDPs.

101. Under Humana’s TRICARE contracts with the United States Department of Defense, Humana provides administrative services to arrange health care for active-duty and retired military personnel and their dependents. Humana delivered services under the T2017 East Region contract, comprising 32 states and approximately 6 million TRICARE beneficiaries, until the contract’s expiration in December 2024. The T-5 East Region contract, which commenced on January 1, 2025, comprises 24 states and Washington D.C., and includes approximately 4.6 million beneficiaries.

102. In addition to its government contracts, Humana also provides specialty and ancillary insurance benefits consisting of dental, vision, life and disability to employer groups. Humana also sells dental and vision specialty insurance benefits to individuals.

* * *

103. In the course of providing services, Insurer Defendants and other Conduent clients collect and maintain large volumes of sensitive Private Information from their customers and employees, including names, dates of birth, Social Security numbers, insurance identification numbers, insurance claims data and information, and other sensitive personal and health data.

104. As a condition of transacting with Insurer Defendants, individuals who are employed with or enroll with them through their various services or insurance offerings, including

Plaintiffs and Class Members, are required to entrust Insurer Defendants with their sensitive Private Information.

105. In the ordinary course of their involvement with Plaintiffs' and Class Members' insurance applications, claims, and associated documentation, Insurer Defendants required Plaintiffs and Class Members to provide their highly sensitive Private Information as a condition of their contractual relationships with Insurer Defendants, *i.e.*, by entering into a direct business relationship with an insurance company.

106. To operate their respective businesses, save costs, and store and analyze their customers' Private Information, Insurer Defendants contracted Conduent for back-office and other administrative technology and services, including services related to data mining, analytics, consumer interactions, and claims processing that necessarily required Insurer Defendants' customers' Private Information.

107. To facilitate Conduent's contracted services, and save costs, Insurer Defendants provided their customers', including Plaintiffs' and Class Members', Private Information to Conduent for Conduent to maintain, analyze, use, and store.

108. Insurer Defendants derived economic benefits from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Insurer Defendants could not perform their respective operations, furnish their products and services, analyze insurance risks, or process claims.

109. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Insurer Defendants assumed legal and equitable duties to their respective customers and employees and knew or should have known they were responsible for

keeping that Private Information confidential and protected against unauthorized disclosure, including by their service provider and business associate Conduent.

110. At all relevant times, Insurer Defendants knew Conduent was storing and using its networks to store and transmit valuable, sensitive Private Information belonging to Plaintiffs and Class Members, and that as a result, Conduent's systems would be attractive targets for cybercriminals. Insurer Defendants also knew any breach of Conduent's systems and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the millions of individuals whose Private Information was compromised, as well as intrusion into those individuals' confidential and sensitive personal matters.

II. Defendants Promise to Protect Plaintiffs' and Class Members' Private Information.

A. Conduent

111. As evidenced by Conduent's *Privacy Policy*, available on Conduent's website, Conduent understood its obligation to safeguard Plaintiffs' and Class Members' Private Information. Conduent's *Privacy Policy* "applies to the personal data collection, use, and disclosure practices of Conduent and its affiliated entities . . . it also applies to the collection, use and disclosure of information we collect from vendors, clients, individuals and entities who contact us."¹⁴

112. Conduent's *Privacy Policy* states that it maintains robust, executive-level oversight of data privacy and security:

Conduent's commitment to data privacy goes beyond minimum legal and regulatory requirements and strives for best-in-class data protection and privacy management. This commitment is overseen at the executive level by the Chief Privacy Officer, who reports to the General Counsel, and the Chief Information Security Officer, who reports to the Chief Information Officer (with the General Counsel and Chief Information Officer both reporting directly to the Chief

¹⁴ *Data Privacy at Conduent*, CONDUENT, at <https://www.conduent.com/privacy-policy/> (last visited Jan. 6, 2026).

Executive Officer). The Board receives reports from both the Chief Privacy Officer and Chief Security Officer. The Risk Oversight Committee agenda includes coverage of data privacy at every meeting.¹⁵

113. Conduent's *Privacy Policy* represents that Conduent and its affiliates "respect and are committed to safeguarding the confidentiality, data privacy, and security of the information that our customers have entrusted to us, including the confidential information, personally identifiable information, proprietary information, and trade secrets gathered across all of our business operations."¹⁶

114. Conduent's *Privacy Policy* also promises and warrants as follows:

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymise it or, if this is not possible . . . then we will securely store your personal information and isolate it from any further processing until deletion is possible. . . .

Conduent uses technical, organizational, and physical measures designed to protect the integrity, confidentiality, security, and availability of personal information. Among other measures, only authorized personnel of Conduent and of our third-party service providers with a legitimate need to know are provided access to personal data, and these employees and third-party service providers are required to treat this information as confidential where applicable. . . .

Data Security Risk Approach: Conduent's security program is aligned with applicable industry regulatory requirements, including but not limited to NIST, HITRUST, GDPR, HIPAA, ISO, and PCI. The program encompasses information security and cyber operations capabilities that protect Conduent and our clients. It is continuously reviewed and strengthened as necessary to ensure responsiveness to and protection against emerging threats. Conduent maintains a highly qualified workforce and utilizes external experts to support the program. We administer internal education, training, and communication programs to ensure ongoing awareness and vigilance. We maintain and communicate formal documented policies and standards. We monitor and assess the overall operating effectiveness of our program through risk assessments that include identification and remediation of vulnerabilities and threats. We maintain and test our cyber incident response plan, and undertake various independent reviews in conjunction with PCI DSS, external audits, internal audits, and client assurance efforts. Various additional operational protections, controls, and processes exist, including but not limited to malware protection, intrusion prevention, and detection protocols, user access

¹⁵ *Id.*

¹⁶ *Id.*

reviews, network segmentation, implementation and maintenance of network and application firewalls, vulnerability scanning, data encryption, penetration testing, and patching.¹⁷

115. Likewise, Conduent’s *Code of Conduct* promises to safeguard Plaintiffs’ and Class Members’ Private Information. Conduent’s *Code of Conduct*, which applies to all “employees and those who do business on Conduent’s behalf, including agents, representatives and independent contractors,” states:

We respect and are committed to safeguarding the confidentiality, data privacy and security of information that our customers have entrusted to us, including confidential information, personally identifiable information, proprietary information and trade secrets. We exercise appropriate care at all times to prevent unauthorized disclosure and use of customer information. We take our responsibilities for customer confidentiality, data privacy and security seriously and implement appropriate safeguards for the use and handling of this information in accordance with our information security and privacy policies and in accordance with all applicable laws.¹⁸

B. Insurer Defendants

116. Because Insurer Defendants required Plaintiffs’ and Class Members’ Private Information in exchange for the provision of insurance, by accepting their Private Information, Insurer Defendants owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, and knew or should have known that they were responsible for protecting Plaintiffs’ and Class Members’ Private Information and keeping it confidential, safe, and secure from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach, including by ensuring that their third-party service providers implemented adequate, secure, and compliant safeguards to protect their own platforms.

¹⁷ *Id.*

¹⁸ *Conduent Code of Business Conduct*, CONDUENT (2025), at https://downloads.conduent.com/content/usa/en/document/Code-of-Conduct_032825_English.pdf?_gl=1*uw4uuu*_up*MQ..*_ga*MTEzNzQxMzcyOC4xNzYxNz

117. Because of the highly sensitive and personal nature of the information that Insurer Defendants acquire, they have a nondelegable duty to Plaintiffs and Class Members to implement reasonable and adequate security measures to protect their Private Information. Insurer Defendants promise, among other things, to keep customers' files private; comply with regulation and industry standards, including HIPAA and FTC guidelines, related to data security and maintenance of their clients' customers' files and the Private Information contained therein; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiffs and Class Members obtain from Defendants; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

118. As sophisticated business entities handling highly sensitive and confidential consumer data, Insurer Defendants' data security obligations were particularly important.

119. Insurer Defendants, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard Plaintiffs' and Class Members' Private Information from theft and misuse.

I. AIGPS

120. AIGPS, through its *Privacy Policy*, *Codes of Conduct*, company security practices, and other conduct, implicitly and explicitly promises to safeguard AIGPS Plaintiffs' and Class Members' PII and PHI from theft and misuse.

121. AIGPS's *Privacy Policy*, published on the company website, provides that AIGPS may collect and use AIGPS Plaintiffs' and Class Members' PII and PHI to, *inter alia*, "[c]ommunicate with you and others as part of our business; [r]espond to your requests; [s]end you important information regarding changes to our policies, other terms and conditions, our AIGPS On-line Services and other administrative information; [m]ake decisions about whether to

provide insurance and assistance services, and other products and services which we offer, and provide such products and services, including claim assessment, processing and settlement, and, where applicable, manage claim disputes; [i]mprove and develop our business operations, products, and services.”¹⁹

122. AIGPS states in its *Privacy Policy* that the PII that it collects and uses, may include “[y]our name; address; e-mail and telephone details; gender; marital status; family status; date of birth; passwords on our systems; educational background; physical attributes; activity records, such as driving records; photos; employment history, skills and experience; professional licenses and affiliations; relationship to the policyholder, insured or claimant; and date and cause of death, injury or disability.”²⁰ This information may also include “Social Security or national insurance number; passport number; tax identification number; military identification number or driver’s or other license number,” as well as “payment card number; bank account or other financial account number and account details; credit history and credit score; assets; income; and other financial information.”²¹

123. AIGPS also provides in its *Privacy Policy* that “[i]n certain cases, we may receive sensitive information about you for example, if you apply for insurance through a third party marketing partner that is a professional, trade, political, religious or community organization.”²² AIGPS may also “obtain information about your criminal record or civil litigation history in the process of preventing, detecting and investigating fraud.”²³ Furthermore, AIGPS may obtain “[p]hotographs or video recordings created in connection with our insurance or other business

¹⁹ *Privacy Policy*, AIG, at <https://www.aig.com/privacy-policy> (last updated Aug. 8, 2025).

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

²³ *Id.*

activities, including for claims assessment, processing, settlement, and disputes.”²⁴ The PII that AIGPS collects and uses may also include “[l]ocation and identification of property insured (for example, property address, vehicle license plate or identification number); travel plans; age categories of individuals you wish to insure; policy and claim numbers; coverage/peril details; cause of loss; prior accident or loss history; your status as director or partner; or other ownership or management interest in an organization; other insurance you hold; and details on products for which you have or seek a warranty.”²⁵ In addition, AIGPS “may receive certain Personal Information about you when you use our Apps or Social Media Pages, including your social media account ID and profile picture.”²⁶

124. AIGPS states in its *Privacy Policy* that the PHI that it collects and uses, may include “[c]urrent or former physical or mental or medical condition; health status; injury or disability information; medical procedures performed; personal habits (for example, smoking or consumption of alcohol); prescription information; and medical history.”²⁷

125. AIGPS states in its *Privacy Policy* that it may share AIGPS Plaintiffs’ and Class Members’ PII and PHI with “[e]xternal third-party service providers, such as medical professional, accountants, actuaries, auditors, experts, lawyers and other outside professional advisors; travel and medical assistance providers; call center service providers; IT systems, support and hosting service providers; printing, advertising, marketing and market research and analysis service providers; banks and financial institutions that service our accounts; third-party claim administrators; document and records management providers; claim investigators and adjusters;

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

construction consultants; engineers; examiners; jury consultants; translators; and similar third-party vendors and outsourced service providers that assist us in carrying out business activities.”²⁸

126. AIGPS’s *Privacy Policy* assures that “AIG will take appropriate technical, physical, legal and organizational measures, which are consistent with applicable privacy and data security laws.”²⁹ AIGPS’s *Privacy Policy* further states that “[w]hen AIG provides Personal Information to a service provider, the service provider will be selected carefully and required to use appropriate measures reasonably designed to protect the confidentiality and security of the Personal Information.”³⁰

127. AIGPS’s *Code of Conduct* applies to all AIGPS officers and employees and contains “the rules and guidelines that each of us should keep in mind as we engage in our daily activities.”³¹ It states: “Our customers expect us to carefully handle and safeguard the information they share with us. Never compromise a customer’s trust by disclosing a customer’s Highly Confidential or Confidential Information, including Personal Information, in a manner contrary to AIG’s Global Information Handling Policy and Standard or our customer facing privacy policy or to those without a legitimate business need for such information. . . . In all cases we must maintain appropriate physical, administrative and technical safeguards for a customer’s Highly Confidential or Confidential Information, including Personal Information. We must be especially vigilant in following laws, regulations and policies when sharing Personal Information with other parties (even for legitimate business purposes)”³²

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.*

³¹ *Code of Conduct*, AIG (2025), at <https://www.aig.com/content/dam/aig/america-canada/us/documents/about-us/code-of-conduct/aig-employee-code-of-conduct-english.pdf>.

³² *Id.*

128. AIGPS also maintains a *Supplier Code of Conduct*, which “presents principles and minimum standards for Suppliers to follow in their dealings with AIG.”³³

129. The *Supplier Code of Conduct* states: “Suppliers must keep confidential all AIG proprietary and non-public information, including nonpublic personal information received from, processed on behalf of, or disclosed by AIG. Suppliers must take precautions to safeguard this information, including ensuring that Suppliers’ personnel (including the personnel of suppliers with whom they work in providing goods and services to AIG) are under appropriate confidentiality obligations and adequately trained to safeguard confidential information.”

130. AIGPS’s *Supplier Code of Conduct* requires suppliers to “comply with all applicable data privacy and security laws and regulations, including laws and regulations regarding the cross-border transfer of or access to personal information (or data derived from personal information). Suppliers must prohibit and prevent any access to U.S. personal information by any individuals or entities that are the subject of U.S. data access laws and regulations, such as Executive Order 14117 (including, if applicable, access by Suppliers or their affiliates, or third parties). Suppliers must maintain appropriate procedures, safeguards, and controls to secure and protect the confidentiality integrity and availability of confidential information, including personal information, received from, processed on behalf of, or disclosed by AIG or third parties on AIG’s behalf. Suppliers must promptly notify AIG of any suspected or actual compromise or risk of compromise to the confidentiality, integrity or availability of such confidential information.”³⁴

131. Under AIGPS’s *Supplier Code of Conduct*, “AIG reserves the right to review or audit Supplier’s compliance.”³⁵

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

132. AIGPS maintains a “Cyber and Information Security” page on its website that states: “Our customers expect and deserve a safe and secure digital experience. As our world becomes increasingly connected, providing a best-in-class cyber security program has never been more important . . . We recognize the importance of information security in maintaining a resilient business and understand that responding to an evolving threat landscape is critical to effective risk management. . . . AIG is committed to continually developing and honing our overall security capabilities and putting the security and safety of our data, and our customers’ data, at the forefront of our efforts. . . . Validation of the AIG security posture is conducted using a multifaceted approach. Assurance is obtained from independent internal and external organizations to assess the effectiveness of our control environment. . . . Protecting the safety, including the confidentiality, availability, and integrity of information assets is a priority at AIG. Whether we are working with customer data, employee data or AIG proprietary information, AIG is committed to delivering ongoing user cybersecurity awareness training designed to help protect our assets and information”³⁶

133. On a “Cyber & Information Security Resources” webpage, AIGPS acknowledges the risk from cyber threats: “At AIG, we anticipate an increase in cyber business interruption on a global level as ransomware and extortion attacks evolve. . . . At a time of increased remote work, employees are more vulnerable than ever to exploitation by malicious actors. Phishing is one of the most common types of cyberattacks used by malicious actors to access an organization’s network and confidential information.”³⁷

³⁶ *Cyber and Information Security*, AIG, at <https://www.aig.com/home/about/cyber-and-information-security> (last visited March 14, 2026).

³⁷ *Cyber & Information Security Resources*, AIG, at <https://www.aig.com/home/about/cyber-and-information-security/cyber-and-information-security-resources> (last visited March 14, 2026).

134. AIGPS recognizes the increasing risk of cybersecurity incidents, and uses this as selling point for marketing its services. In its *Cyber Sales Playbook*, a “broker guide to selling cyber insurance,” AIGPS acknowledges that “all companies are at risk, presenting brokers with a significant opportunity to assist clients with assessing their exposures and working with carriers to craft solutions. . . . Cyber is consistently one of the top risks businesses face.”³⁸ AIGPS further represents that “[a]ny company that relies on technology and stores, manipulates, or transmits data is at risk of a cyber incident. . . . The experts agree: service providers, financial services, insurance, real estate, and healthcare organizations are the most commonly targeted industries.” The *playbook* includes a variety of scenarios where a potential customer objects to purchasing AIGPS’s services, AIGPS provides example answers including: “We don’t need it. We outsource our security. Companies are increasingly moving towards outsourced service providers and cloud-based storage. Still, such providers must be properly vetted. Insureds should read the fine print, as contracts often limit the providers’ liability in the event of a breach.”

135. AIGPS also maintains a *Global Employee and Non-Employee Worker Personal Information Privacy Notice* (“*Employee Privacy Notice*”) that “applies to employees and other workers that are not employed by AIG but have access to AIG facilities and/or corporate networks and systems.”³⁹

136. AIGPS’s *Employee Privacy Notice* includes a variety of examples of how or when AIGPS will use employees’ Personal Information, and includes the disclaimer, “AIG will not

³⁸ *Cyber Sales Playbook*, AIG, at <https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-sales-playbook-final.pdf> (last visited March 14, 2026).

³⁹ *Global Employee and Non-Employee Worker Personal Information Privacy Notice*, AMERICAN INTERNATIONAL GROUP, INC. (June 25, 2021), at <https://www.aig.com/content/dam/aig/america-canada/us/documents/about-us/suppliers/aig-notice-global-employee-non-employee-privacy-notice-excludes-us-japan-gdpr-english.pdf.coredownload.pdf>.

process Personal Information for any other purpose incompatible with the purposes described in this Notice.”⁴⁰ Providing employees’ Personal Information to a negligent supplier is not one of the examples.

137. The *Employee Privacy Notice* includes representations as to the security of employees’ Personal Information:

- a. “AIG will take appropriate measures to protect Personal Information that are consistent with applicable privacy and data security laws and regulations. . . .”
- b. “We use appropriate technical, physical, legal, and organizational security measures which comply with data protection laws to keep Personal Information secure. . . .”
- c. “When AIG engages a third party (including service providers) to collect or otherwise process Personal Information on our behalf, the third party is required by AIG to undergo a review of their security measures and enter an agreement that requires use of appropriate security measures to protect the confidentiality and security of Personal Information.”⁴¹

138. The *Employee Privacy Notice* also includes the representation that AIGPS “will keep your Personal Information only for as long as necessary given the reasons we collect and hold it.”⁴²

139. Conduent was required to implement appropriate privacy and security safeguards consistent with AIGPS’s *Supplier Code of Conduct*.

140. AIGPS has a non-delegable duty to ensure that all Private Information it collects and stores is secure, and that any vendors or business associates with whom it shares information

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

also maintain adequate and commercially reasonable data security practices to ensure the protection of the insureds' Private Information.

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

142. Despite its obligations to safeguard AIGPS Plaintiffs' and Class Members' Private Information, AIGPS failed to adequately vet or oversee Conduent's data security practices, in violation of its own policies requiring vendors to maintain robust privacy protections. AIGPS also failed to verify whether Conduent had implemented the required privacy training, risk management systems, and contractual safeguards outlined in its *Supplier Code of Conduct*.

143. AIGPS's failure to ensure that its vendor adhered to basic privacy and security practices—despite its public commitments and legal obligations—constitutes a breach of its own policies and directly contributed to the exposure of AIGPS Plaintiffs' and Class Members' sensitive Private Information.

2. Cigna

144. Cigna's *Website Privacy Notice*, which “applies to Personal Information collected through the Cigna Healthcare website,” states that Cigna collects and uses Cigna Plaintiff's and Class Members' PII to, *inter alia*, “provide and operate our Services, communicate [] about your

use of the Services, provide you with information about our Services, including information about health care, health related services, resources and benefits that will help you manage your health; sending administrative information . . . provide troubleshooting and technical support, respond to your inquiries, fulfill your orders and requests, process your payments and claims, communicate with you about the Services, complete transactions, and provide quotes.”⁴³ Cigna also collects and uses Cigna Plaintiff’s and Class Members’ Private Information to “tailor content we may send or display on the Services,” as well as “[f]or marketing and advertising purposes,” and to “better understand how users access and use the Services, and our other products and offerings, and for other research and analytical purposes, such as to evaluate and improve our Services and business operations, to develop services and features.”⁴⁴ Additionally, Cigna collects and uses Cigna Plaintiff’s and Class Members’ Private Information “[t]o administer surveys and questionnaires,” “[t]o maintain [Cigna’s] facilities and infrastructure,” “[t]o authenticate or confirm your identity,” “[t]o protect the Services and our business operations,” as well as for general business and operational support, such as “[t]o consider and implement mergers, acquisitions, reorganizations, bankruptcies, and other business transactions such as financings, and related to the administration of our general business, accounting, auditing, compliance, recordkeeping and legal functions.”⁴⁵

145. Cigna further states in its *Website Privacy Notice* that the Private Information it collects and uses includes Cigna Plaintiff’s and Class Members’ “name, contact information, online identifiers, and government-issued ID numbers.”⁴⁶ This Private Information also includes Class Members’ “Characteristics of Protected Classifications under state or federal law such as age

⁴³ *Privacy Notice*, CIGNA (2024), at <https://www.cigna.com/static/www-cigna-com/docs/website-privacy-notice.pdf>.

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

and medical conditions,” as well as “transactional information and purchase history.”⁴⁷ Additionally, Cigna Plaintiff’s and Class Members’ Private Information collected and used by Cigna includes their internet and network activity information “such as browsing history;” geolocation data, “such as device location;” audio, electronic, and visual information, “such as call and video recordings;” and professional or employment-related information, “such as place of employment and job title.”⁴⁸

146. Cigna’s *Notice of Privacy Practices*, which governs Cigna’s processing of its insureds’ PHI, acknowledges that Cigna collects PHI “[i]n the normal course of doing business[.]” and that it uses and discloses Cigna Plaintiff’s and Class Members’ PHI “to health care professionals or other third parties to provide, coordinate and manage the delivery of health care.”⁴⁹ For instance, in order for Cigna Plaintiffs and Class Members to “obtain services and treatment such as ordering lab tests and using results of your pharmacist,” Cigna “may disclose PHI about you to your doctor.”⁵⁰ Further, Cigna “may use and disclose PHI about [Cigna Plaintiffs and Class Members]” to “receive payment for [Cigna’s] services or premiums for your coverage, manage your account, fulfill [Cigna’s] responsibilities under your benefit plan and process your claims for drugs you have received.”⁵¹ Cigna may also use and disclose PHI collected from Cigna Plaintiffs and Class Members “to carry on [Cigna’s] business planning and administrative operations,” as well as “use and disclose PHI about you for research purposes” and other uses.⁵²

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ *HIPAA Notice of Privacy Practices*, CIGNA (Aug. 2025), at <https://www.cigna.com/static/www-cigna-com/docs/cigna-health-care-and-cigna-supplemental-benefits-privacy-notice-eng.pdf>.

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

147. Cigna contracts with Conduent to provide various digital business solutions for Cigna, such as front-end digitization services, payment integrity audits, and printing/mailroom services. In order to obtain Conduent's services, Cigna provided Conduent with the Private Information of Cigna's customers.

148. Cigna, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promises to safeguard Cigna Plaintiff's and Class Members' Private Information from theft and misuse. For instance, Cigna's *HIPAA Notice of Privacy Practices* provides that "[w]e take our obligation to keep your PHI secure and confidential very seriously."⁵³ It further provides that Cigna is "required by state and federal law to protect the privacy of your PHI."⁵⁴ Cigna also assures its customers, "[w]e understand the importance of protecting your PHI," and, "[w]e maintain technical, physical and administrative safeguards to ensure the privacy of your PHI."⁵⁵

149. Cigna has a non-delegable duty to ensure that all Private Information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintains adequate and commercially reasonable data security practices to ensure the protection of the insureds' Private Information.

150. Indeed, Cigna's entire business depends on the insureds entrusting it with their Private Information. Without the insureds' Private Information, Cigna would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to

⁵³ *HIPAA Notice of Privacy Practices*, CIGNA (Aug. 2025), at <https://www.cigna.com/static/www-cigna-com/docs/cigna-health-care-and-cigna-supplemental-benefits-privacy-notice-eng.pdf>.

⁵⁴ *Id.*

⁵⁵ *Id.*

provide health insurance benefits, Cigna knows that its insureds must trust that Cigna is keeping their Private Information private and secure. If Cigna's insureds lack trust in Cigna or knew Cigna would insecurely store, safeguard, or transmit their Private Information, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

151. Despite its obligations to safeguard Cigna Plaintiff's and Class Members' Private Information, Cigna failed to adequately vet or oversee Conduent's data security practices. Cigna also failed to verify whether Conduent had maintained adequate privacy training, risk management systems, and contractual safeguards.

152. Cigna's failure to ensure that its vendor adhered to basic privacy and security practices—despite its public commitments and legal obligations—constitutes a breach of its own policies and directly contributed to the exposure of Cigna Plaintiff's and Class Members' sensitive Private Information.

3. *Elevance*

153. Elevance's *Privacy Policy*, published on the company website, provides that Elevance may collect and use Elevance Plaintiffs' and Class Members' Private Information to, *inter alia*, “perform administrative, technical, hosting or other functions.”⁵⁶ It further provides that Elevance “may use your personal information with technology to better support and enable services provided to you.”⁵⁷ Elevance's *Privacy Policy* applies to both its employees and non-employee members/customers.

⁵⁶ *Privacy Policy*, ELEVANCE HEALTH (Jan. 1, 2020), at <https://www.elevancehealth.com/privacy-policy>.

⁵⁷ *Id.*

154. Elevance contracts with Conduent to provide various digital business solutions for Elevance, such as front-end digitization services, payment integrity audits, and printing/mailroom services. In order to obtain Conduent's services, Elevance provides Conduent with the Private Information of Elevance's customers.

155. Elevance, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promises to safeguard Elevance Plaintiffs' and Class Members' Private Information from theft and misuse. Elevance's *Privacy Policy* promises that "privacy is very important to us and we will make every reasonable effort to safeguard any information we collect."⁵⁸ Elevance further maintains that "[w]e maintain administrative, technical, and physical safeguards to protect information."⁵⁹

156. Elevance has a non-delegable duty to ensure that all Private Information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintains adequate and commercially reasonable data security practices to ensure the protection of the insureds' Private Information.

157. Indeed, Elevance's entire business depends on the insureds entrusting it with their Private Information. Without the insureds' Private Information, Elevance would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, Elevance knows that its insureds must trust that Elevance is keeping their Private Information private and secure. If Elevance's insureds lack trust in Elevance or knew Elevance would insecurely store, safeguard, or transmit their Private Information, then

⁵⁸ *Id.*

⁵⁹ *Id.*

they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

158. Indeed, Elevance in particular was at all times acutely aware of the need for adequate, industry-standard cybersecurity measures for insured customers' data, and the risk of breach and harm to those individuals that deficient safeguards would cause: In 2015—a time when it was operating under the name Anthem—Elevance experienced a devastating cyberattack of its own network systems. It is still one of the largest known data breaches ever, resulting in the wrongful disclosure of 78.8 million individuals' PII to cybercriminals.

159. Elevance also knew from past experience the importance of sufficiently supervising its vendors that handled Private Information, and the need to vet and ensure those vendors used sufficient data security measures to protect sensitive customer data: In 2023, criminal hackers stole Elevance's customers' PII and PHI through a data breach involving another Anthem BCBS third-party administrator, compromising 2.5 million individuals' confidential information in total.

160. Despite its obligations to safeguard Elevance Plaintiffs' and Class Members' Private Information, Elevance failed to adequately vet or oversee Conduent's data security practices. Elevance also failed to verify whether Conduent had maintained adequate privacy training, risk management systems, and contractual safeguards.

161. Elevance's failure to ensure that its vendor adhered to basic privacy and security practices—despite its public commitments and legal obligations—constitutes a breach of its own policies and directly contributed to the exposure of Elevance Plaintiffs' and Class Members' sensitive Private Information.

4. HCSC

162. Through its Blue Cross Blue Shield divisions, HCSC promises its customers, like HCSC Plaintiffs and Class Members: “Your trust is earned through our actions. All technology

cybersecurity measures we implement are designed with one goal. We strive to keep your health information safe so you can focus on what matters—your health and wellbeing.”⁶⁰ And HCSC likewise warrants to its customers that “[p]rotecting your private health information is our responsibility.”⁶¹

163. HCSC also directly acknowledges its responsibility for protecting individuals’ Private Information in its *Code of Conduct*, which states: “We respect and protect the privacy and security of the information we maintain about our members, customers, business partners, and workers.”⁶² Further,

The improper use or disclosure of PII can:

- a. Damage an individual’s reputation, cause embarrassment, or result in identity theft.
- b. Violate federal or state privacy and security laws which could lead to lawsuits or serious penalties for individual workers or the Company.
- c. Damage the Company’s reputation and negatively impact our finances.
- d. Violate a provision within a government or customer contract.⁶³

164. HCSC also recognizes that the risk to its customers extends to its vendors. Accordingly, HCSC developed a *Code of Ethics and Conduct for Vendors*.

⁶⁰ *Keeping Your Health Data and Personal Information Safe is Our Goal*, BCBSIL, at <https://www.bcbsil.com/about-us/cybersecurity> (last visited Jan. 8, 2026); *Keeping Your Health Data and Personal Information Safe is Our Goal*, BCBSMT, at <https://www.bcbsmt.com/about-us/cybersecurity> (last visited Jan. 8, 2026); *Keeping Your Health Data and Personal Information Safe is Our Goal*, BCBSOK, at <https://www.bcbsok.com/about-us/cybersecurity> (last visited Jan. 8, 2026); *Keeping Your Health Data and Personal Information Safe is Our Goal*, BCBSNM, at <https://www.bcbsnm.com/about-us/cybersecurity> (last visited Jan. 8, 2026); *Keeping Your Health Data and Personal Information Safe is Our Goal*, BCBSTX, at <https://www.bcbstx.com/about-us/cybersecurity> (last visited Jan. 8, 2026).

⁶¹ *Id.*

⁶² *Code of Ethics and Conduct*, HCSC, (Aug. 2025), p. 50, at <https://www.hcsc.com/documents/hcsc-code-conduct.pdf>.

⁶³ *Id.* at 51.

165. Within the *Code of Ethics and Conduct for Vendors*, HCSC requires that its vendors comply with applicable laws and regulations, including HIPAA, and to “manage risk and implement reasonable and appropriate security measures.”⁶⁴

166. HCSC reserves the ability to exercise oversight of its vendors, requiring that vendors “respond to HCSC inquiries and request for information within the timeframe set by HCSC.”⁶⁵

167. Yet, HCSC failed to ensure that HCSC Plaintiffs’ and the Class’s Private Information in Conduent’s custody was adequately protected.

168. As a result, the Private Information of HCSC’s customers was compromised and impacted in the Data Breach, including names, dates of birth, addresses, Social Security numbers, medical service information (treatment and diagnosis codes, provider names, dates of service and claim amounts), group numbers and subscriber numbers.

169. HCSC, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard HCSC Plaintiffs’ and Class Members’ Private Information from theft and misuse.

170. HCSC has a non-delegable duty to ensure that all member information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintain adequate and commercially reasonable data security practices to ensure the protection of the insureds’ Private Information.

171. Indeed, HCSC’s entire business depends on the insureds entrusting it with their Private Information. Without the insureds’ Private Information, HCSC would not be able to

⁶⁴ *Code of Ethics and Conduct for Vendors*, HCSC, (Aug. 2025), p. 3, 5, at <https://www.hcsc.com/documents/hcsc-coc-vendor.pdf>.

⁶⁵ *Id.* at 3.

provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, HCSC knows that its insureds must trust that HCSC is keeping their Private Information private and secure. If HCSC's insureds lack trust in HCSC or knew HCSC would insecurely store, safeguard, or transmit their Private Information, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

172. Despite its obligations to safeguard HCSC Plaintiffs' and Class Members' Private Information, HCSC failed to adequately vet or oversee Conduent's data security practices. HCSC also failed to verify whether Conduent had maintained adequate privacy training, risk management systems, and contractual safeguards.

173. HCSC's failure to ensure its vendor adhered to basic privacy and security practices—despite its public commitments and legal obligations—constitutes a breach of its own policies and directly contributed to the exposure of HCSC Plaintiffs' and Class Members' sensitive Private Information.

5. Humana

174. Humana's *Privacy Policy*, published on the company website, states that Humana collects and uses Humana Plaintiff's and Class Members' Private Information to, *inter alia*, provide them with "[s]ervices, including health insurance products, wellness products or providers, or health care," to provide "non-insurance or health care products or services," as well as to "process [Class Member] payments and send notifications," and to enable Class Members "to access and use [Humana's] websites and mobile applications."⁶⁶ Humana also collects and uses

⁶⁶ *Privacy Policy*, HUMANA (March 2023), at <https://www.humana.com/legal/privacy-policy>.

Humana Plaintiff's and Class Members' Private Information to communicate with Class Members and respond to their "requests, questions, comments, and other inquiries," as well as to offer Class Members "personalized advertisements," and "send marketing and promotional materials, including information relating to [Humana's] products, [s]ervices, sales, or promotions."⁶⁷ Additionally, Humana collects and uses Humana Plaintiff's and Class Members' Private Information "[t]o administer, maintain, evaluate, and improve [Humana's] websites, mobile applications, and [s]ervices, and to develop new products and services," as well as "[t]o conduct research and analytics related to [Humana's] websites and [s]ervices, including combining any or all of the information that we collect or obtain," and "[t]o manage [Humana's] business operations."⁶⁸

175. Humana also states that "[i]n addition to the purposes noted above," it collects and uses Humana Plaintiff's and Class Members' Private Information "to fulfill [Humana's] business operations and provide the requested [s]ervices . . . such as processing or fulfilling claims, coordinating benefits, and processing payments; managing administrative matters such as invoicing, renewal or to audit customer transactions; developing, maintaining, provisioning, or upgrading networks, [s]ervices, or devices; and conducting analytics to determine how to improve our [s]ervices and develop new ones."⁶⁹ Humana states that it "may de-identify and aggregate" Humana Plaintiff's and Class Members' Private Information "to conduct analytics and improve our [s]ervices."⁷⁰

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Id.*

⁷⁰ *Id.*

176. Humana states in its *Privacy Policy* that the Private Information that it collects and uses includes Humana Plaintiff's and Class Members' "name, email, any user name and password," as well as their "address, [their] tax identification number or social security number, unique identifiers (such as a mobile device ID) and [their] email and other personal contact information."⁷¹ This Private Information also includes Class Members' demographic information "regarding [their] gender, race, or other protected classification data."⁷² Additionally, Humana Plaintiff's and Class Members' Private Information collected and used by Humana includes their commercial information, payment or banking information, geolocation information, audio and visual information (including photographs), as well as information regarding Class Members' use of Humana's electronic network activity.⁷³

177. Humana's *Notice of Private Practices*, which governs Humana's processing of its insureds' PHI, states that Humana collects Humana Plaintiff's and Class Members' PHI when they "complete application and forms," and other "dealings" with Humana.⁷⁴ For instance, Humana may obtain Humana Plaintiff's and Class Members' PHI "from participants in the healthcare system, such as [their] doctor or hospital, as well as from employers or plan administrators."⁷⁵ Humana may use Humana Plaintiff's and Class Members' PHI "[f]or healthcare operation activities, including processing and enrollment," as well as "[f]or payment activities," and numerous other uses.

⁷¹ *Id.*

⁷² *Id.*

⁷³ *Id.*

⁷⁴ *Insurance ACE Notice of Privacy Practices*, HUMANA (May 2023), at <https://assets.humana.com/is/content/humana/GN14474HHpdf>.

⁷⁵ *Id.*

178. Humana Plaintiff's and Class Members' PHI collected and used by Humana "includes information regarding [Humana Plaintiff's and Class Members'] medical benefit plan, [their] health benefits, and health risk assessment."⁷⁶

179. Humana contracts with Conduent to provide various digital business solutions for Humana, such as front-end digitization services, payment integrity audits, and printing/mailroom services. In order to obtain Conduent's services, Humana provided Conduent with the Private Information of Humana's customers.

180. Humana, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard Humana Plaintiff's and Class Members' Private Information from theft and misuse. Humana states in its *Privacy Policy* that it is "committed to maintaining the highest level of confidentiality with all of the information" it receives from Humana Plaintiff and Class Members.⁷⁷ Humana further maintains that it "respect[s] the importance of privacy."⁷⁸

181. Humana's *Notice of Private Practices* provides: "We have a responsibility to protect the privacy of your information in all formats including electronic and oral information."⁷⁹ It further provides that Humana is "required by law to maintain the privacy and security of your protected health information."⁸⁰ Humana also assures its customers: "We have administrative, technical, and physical safeguards in place to protect your information."⁸¹

⁷⁶ *Id.*

⁷⁷ *Privacy Policy*, HUMANA (March 2023), at <https://www.humana.com/legal/privacy-policy>.

⁷⁸ *Id.*

⁷⁹ *Insurance ACE Notice of Privacy Practices*, HUMANA (May 2023), at <https://assets.humana.com/is/content/humana/GN14474HHpdf>.

⁸⁰ *Id.*

⁸¹ *Id.*

182. Humana has a non-delegable duty to ensure that all Private Information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintains adequate and commercially reasonable data security practices to ensure the protection of the insureds' Private Information.

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

184. Despite its obligations to safeguard Humana Plaintiff's and Class Members' Private Information, Humana failed to adequately vet or oversee Conduent's data security practices. Humana also failed to verify whether Conduent had maintained adequate privacy training, risk management systems, and contractual safeguards.

185. Humana's failure to ensure its vendor adhered to basic privacy and security practices, despite its public commitments and legal obligations, constitutes a breach of its own policies and directly contributed to wrongful disclosure of Humana Plaintiff's and Class Members' Private Information.

III. The Data Breach

186. On or about January 13, 2025, cybercriminals deployed ransomware on Conduent’s IT network, encrypting one of Conduent’s operating systems and causing major operational outages that disrupted services to millions of people.

187. As a result of the attack on January 13, 2025, Conduent discovered that the cybercriminals had successfully hacked into Conduent’s IT network nearly *three months* earlier, on October 21, 2024, using a single set of compromised VPN credentials—and that the cybercriminals had enjoyed undetected access to Conduent’s IT network since then.

188. By the time Conduent learned of the Breach, the cybercriminals had allegedly exfiltrated 8.5 terabytes of unencrypted confidential files containing the Private Information of Plaintiffs and over 44.4 million Class Members obtained by Conduent’s clients, including Insurer Defendants. The unencrypted Private Information exfiltrated during the Data Breach includes names, postal addresses, dates of birth, Social Security numbers, medical service information (treatment and diagnosis codes, provider names, dates of service and claim amounts), and health insurance information (group number and subscriber number).

189. News of the January 2025 outages became public when the Wisconsin Department of Children and Families told state residents that Conduent was experiencing a system outage preventing them from processing payments received by mail. Wisconsin officials reported that the outage impacted “payees who receive their payments via electronic transfer or an EBT card from receiving their scheduled support payment,” acknowledging “the gravity of this outage and the

impact it has on Wisconsin families' livelihoods.”⁸² Conduent told news sources that “[t]he required disciplined recovery caused several days of disruptions to many of our operations.”⁸³

190. After purportedly restoring its systems, Conduent disclosed that the disruption had been “due to a third-party compromise.”⁸⁴

191. One of Elevance’s affiliates later revealed that “[t]he breach was traced to compromised VPN credentials” which required Conduent to “rebuild[] the affected ESX environment.”⁸⁵

192. In mid-January 2025, Conduent notified Insurer Defendants and its corporate clients about the Data Breach, including, upon information and belief, that Plaintiffs’ and Class Members’ Private Information was likely exfiltrated by cybercriminals. Conduent reported to clients that the Data Breach was “contained” and that there was “no longer an active threat” by the end of January 2025.⁸⁶

193. Despite Conduent’s public representation that it promptly notified law enforcement of the Data Breach, recent disclosures reveal that Conduent waited over two weeks, until February 5, 2025, to report the Data Breach to the FBI.

194. On February 19, 2025, Conduent reportedly posted a data breach notice letter to the California AG’s website, which stated that there had been no additional threat activity following

⁸² Jonathan Greig, *Government IT contractor Conduent says ‘third-party compromise’ caused outages*, THE RECORD (Jan. 21, 2025), at <https://therecord.media/government-contractor-conduent-outage-compromise>.

⁸³ *Id.*

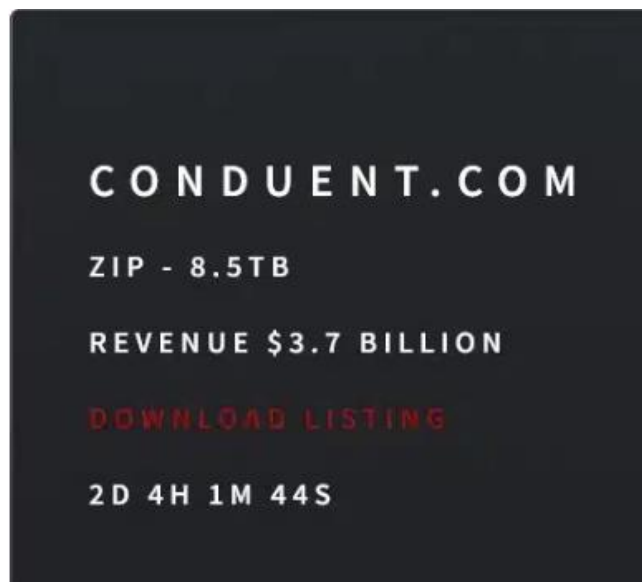
⁸⁴ *Id.*

⁸⁵ *Anthem | Cybersecurity Breach May Have Impacted Your Small Group Clients*, AMWINSCONNECT (Dec. 29, 2025), at <https://www.amwinsconnect.com/knowledge-hub/news-desk/news-detail/anthem--cybersecurity-breach-may-have-impacted-your-small-group-clients>.

⁸⁶ *See Conduent Cybersecurity Incident Frequently Asked Questions*, BLUE CROSS BLUE SHIELD OF NEW MEXICO (Oct. 2025), at https://www.nmrhca.org/wp-content/uploads/2025/10/NM_Group_FAQs-1.pdf.

the Breach. That same day, Conduent filed its 2024 Annual Report with the SEC. Instead of disclosing the Data Breach, Conduent stated: “As of the date of this report, we do not believe that any risks from cybersecurity threats, including as a result of any known cybersecurity incidents, have materially affected, or are reasonably likely to materially affect, the Company.”

195. Only days later, in a February 21, 2025, post on its dark web data leak website, SafePay claimed it had stolen 8.5 terabytes of data from Conduent and threatened to leak it if Conduent did not pay a ransom within three days:



Screenshot of the post on SafePay's data leak site

196. SafePay is a foreign, likely Russian-based cybercriminal ransomware gang that emerged in 2024. The group has actively targeted both public and private sectors worldwide, including significant targeting of organizations within the United States. Cybersecurity experts report that SafePay's observed attack methodology includes gaining initial access using valid credentials that are most likely purchased on dark web marketplaces or obtained through

infostealer malware,⁸⁷ and bypassing multi-factor authentication through misconfigured firewalls or weak password policies.⁸⁸ SafePay is also known to apply the double-extortion technique, meaning it exfiltrates data prior to encrypting a company's systems, demanding payment in cryptocurrency, and threatens to leak the stolen data on its leak site if the ransom is not paid. As one source reports, successful exploitation by SafePay ransomware will almost certainly result in the encryption and exfiltration of significant quantities of data held on the compromised system, prior to a ransom of a predetermined value being issued.⁸⁹ Data stolen in these types of cyberattacks can be leveraged by threat actors in future attacks.

197. To date, Conduent has not publicly acknowledged the ransom demand or disclosed what actions—if any—Defendants took in response. Yet, Conduent's sudden disappearance from SafePay's leak site is a strong indicator that “a ransom has been paid or the stolen data has been sold,” a pattern well-recognized in the cybersecurity industry.⁹⁰

198. Palo Alto Networks' Unit 42, which reportedly assisted Conduent in its investigation, makes clear that, even if Conduent paid a ransom to SafePay, this action provided no meaningful protection for victims. As Unit 42 warns, “even if you pay the ransom, ***there's no guarantee that the cybercriminal will follow through*** on their end of the bargain. Even if your

⁸⁷ *SafePay Ransomware: An Emerging Threat in 2025*, CHECK POINT, at <https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/> (last visited Feb. 17, 2026).

⁸⁸ *Conduent Ransomware Attack: SafePay Gang Exfiltrates 8.5TB of Data Impacting Over 10.5 Million Americans*, BREACHED COMPANY (Nov. 3, 2025), at <https://breached.company/conduent-ransomware-attack-safepay-gang-exfiltrates-8-5tb-of-data-impacting-over-10-5-million-americans/>.

⁸⁹ *Threat Intelligence SafePay Ransomware Report*, QUORUM CYBER (April 2, 2025), at <https://www.quorumcyber.com/wp-content/uploads/2025/04/QC-SafePay-Ransomware-Report-TI-1.pdf>.

⁹⁰ Steve Alder, *Conduent Business Services Data Breach Victim Count Swells to More Than 14.7M*, THE HIPAA JOURNAL (Jan. 7, 2026), at <https://www.hipaajournal.com/conduent-business-solutions-data-breach/>.

files are restored to their original state, it's possible that the perpetrator will maintain a copy of the stolen data and could potentially sell it on the dark web or use it against you in future attacks.”⁹¹

199. Industry experts agree that Plaintiffs' and Class Members' Private Information should still be assumed to have been copied, traded, sold, or held for a future extortion attempt. Ransomware groups routinely market stolen data in cybercriminal forums and dark web marketplaces to generate additional revenue, meaning paying a threat actor not to leak stolen data “provides almost no benefit to the victim.”⁹²

200. Many organizations have paid ransom to cybercriminals, who then leaked the stolen data anyway, including the following:⁹³

- a. FatFace (2021): The UK-based clothing retailer was attacked in January 2021 and paid a \$2 million ransom. Despite the payment, customer data was reportedly leaked online.
- b. CNA Financial (2021): CNA Financial, one of the largest insurance companies in the US, paid a \$40 million ransom after a ransomware attack in March 2021. Despite the payment, some data was leaked online.
- c. Quanta Computer (2021): This Taiwanese manufacturer, a supplier for Apple, was hit by the REvil ransomware group in April 2021. Despite

⁹¹ David Jones, *Conduent warns January breach impacted a 'significant' number of people*, CYBERSECURITY DIVE (April 22, 2025), at <https://www.cybersecuritydive.com/news/conduent-breach-significant-number/745963/>; Jeremy Brown, *Breaking Down Ransomware Attacks*, PALO ALTO NETWORKS (May 21, 2021), at <https://unit42.paloaltonetworks.com/breaking-down-ransomware-attacks/> (emphasis in original).

⁹² *Ransomware: The Data Exfiltration and Double Extortion Trends*, COVEWARE (Nov. 4, 2020), at <https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends>; <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>.

⁹³ See generally *Ransomware Groups Break Promises, Leak Data Anyway*, PHISHLABS. DIGITAL RISK PROTECTION (Nov. 25, 2020), at <https://www.phishlabs.com/blog/ransomware-groups-break-promises-leak-data-anyway>.

paying the ransom, some of the schematics and internal documents related to Apple products were leaked online.

- d. Kingfisher Insurance (2023): In early 2023, the hackers leaked sensitive customer information from this Australian insurance company despite the company paying a ransom.
- e. Australian Clinical Labs (2023): Another Australian entity, Australian Clinical Labs, experienced a ransomware attack in 2023. Despite the payment, patient data was leaked.
- f. MoveIt (2023): The MoveIt data transfer software, used by numerous organizations, was breached in late 2023. Several companies using MoveIt paid ransoms, but the attackers still leaked sensitive data, affecting thousands of users across different organizations.
- g. Enzo Biochem (2023): Enzo Biochem, a diagnostics company, experienced a ransomware attack in late 2023. Despite paying a ransom, the attackers leaked patient data and sensitive company information.
- h. Steris (2024): In early 2024, Steris, a medical equipment company, faced a ransomware attack. After paying the ransom, the company discovered that the attackers had already leaked proprietary information and sensitive data.

201. The FBI, the National Security Agency, the Multi-State Information Sharing and Analysis Center, and the Cybersecurity and Infrastructure Agency (“CISA”) uniformly agree that ransom payments do not ensure the safety of compromised data. For this reason, “[t]he FBI does

not support paying a ransom in response to a ransomware attack” because doing so “doesn’t guarantee you or your organization will get any data back.”⁹⁴

202. Thus, regardless of Conduent’s actions following the ransom demand, Plaintiffs’ and Class Members’ Private Information likely has been, or will be, disseminated on the dark web or through other underground markets, leaving them exposed to ongoing and potentially lifelong risks of identity theft, fraud, and further exploitation.

IV. Defendants Delayed Notice to Plaintiffs and Class Members by Over 10 Months.

203. Conduent warns its clients that a strong incident response framework is non-negotiable for organizations looking to protect their assets and reputation. Conduent advises, “When cybersecurity events happen, *organizations need to quickly mobilize a rapid response process that* minimizes the impact of data loss, ensures compliance requirements are met, and *enables accurate and timely notifications to the right people at the right time.*”⁹⁵

204. Yet, in the wake of the Data Breach, Conduent and Insurer Defendants made the deliberate choice to protect their own financial and reputational interests rather than safeguard Plaintiffs’ and Class Members’ privacy. Instead of acting swiftly to mitigate the damage, Defendants opted for silence and delay—an approach that not only concealed the Breach but also shielded Defendants from immediate financial and regulatory consequences. Their calculated inaction materially raised the risks faced by millions whose sensitive data Defendants were duty-bound to protect.

205. Although Conduent is required to disclose material cybersecurity incidents on Form 8-K within four business days of determining an incident is material and detail the incident’s

⁹⁴ *Ransomware*, FBI, at <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware> (last visited March 16, 2026).

⁹⁵ *Post Incident Privacy Review Brochure*, CONDUENT (2023), at <https://insights.conduent.com/brochures/post-incident-privacy-review> (emphasis added).

nature, scope, timing, and impact, Conduent did not disclose the Data Breach to the SEC until April 9, 2025—three months after discovering the Data Breach, and nearly two months after receiving a ransom demand for 8.5 terabytes worth of Private Information.

206. Conduent claimed in its April disclosure that it was “recently informed of [the Data Breach’s] nature, scope, and validity, confirming that the data sets contained a significant number of individuals’ personal information associated with our clients’ end-users.”⁹⁶ In statements to the press, Conduent emphasized that its Form 8-K was prompted by “information it recently learned from its eDiscovery vendor.”⁹⁷

207. The Form 8-K did not inform Plaintiffs and the Class about the Data Breach, including its scope and whether they were impacted. No similar disclosure or warning was filed by any Insurer Defendant, or provided to Plaintiffs and Class Members.

208. Instead, Conduent and Insurer Defendants agreed to delay notice to Plaintiffs and Class Members until October 2025.

209. Defendants did not begin notifying regulators, including various state attorneys general offices and the United States Department of Health and Human Services (“HHS”) Office of Civil Rights (“OCR”), of the Data Breach until October 2025. Since then, the number of victims has continued to rise exponentially:

- a. On October 8, 2025: Conduent reported to the New Hampshire Attorney General that 1 New Hampshire resident had their Private Information

⁹⁶ *Form 8-K*, CONDUENT (April 9, 2025), at <https://investor.conduent.com/static-files/a989f788-c11c-485f-8630-010d15fbf06e>.

⁹⁷ Kyle Alspach, *Conduent Discloses Theft of Client Data in Hack, ‘Significant Number’ of Individuals Impacted*, CRN (April 14, 2025), at <https://www.crn.com/news/security/2025/conduent-discloses-theft-of-client-data-in-hack-significant-number-of-individuals-impacted>.

impacted by the Data Breach, based on information that individual provided to Humana.⁹⁸

- b. On October 24 & 25, 2025: Conduent reported the data breach to the Oregon Department of Justice, stating 10,515,849 individuals were impacted.⁹⁹ HCSC report to the Montana state auditor that the Data Breach impacted more than 462,000 Montanans.¹⁰⁰ Conduent disclosed an additional 10,879 New Hampshire residents.¹⁰¹ Conduent reported to the Maine Attorney General that 374 Maine residents were impacted by the Data Breach.¹⁰² Conduent reported to the Washington State Office of the Attorney General that 87,975 Washingtonians had their names, social security numbers, full dates of birth, health insurance policy or ID numbers, and medical information compromised in the Data Breach.¹⁰³ Conduent reported to Iowa's Office of the Attorney General that 643 Iowa residents were impacted by the Data Breach, and that the impacted files included names and Social Security numbers.¹⁰⁴ Conduent reported to South Carolina that 430,332 South Carolina residents were impacted by the Data Breach.¹⁰⁵ Conduent reported to the Massachusetts Office of Consumer Affairs and Business Regulation that 142,314 Massachusetts residents were impacted by the Data Breach, including their social security numbers and medical records.¹⁰⁶

⁹⁸ *Conduent letter to the New Hampshire Office of the Attorney General* (Oct. 8, 2025), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-services-20251008.pdf>.

⁹⁹ *Search Data Breaches*, OREGON DOJ, at <https://justice.oregon.gov/consumer/databreach/> (last visited Jan. 16, 2026).

¹⁰⁰ Steve Alder, *Conduent Business Services Data Breach Victim Count Swells to More Than 14.7M*, THE HIPAA JOURNAL (Jan. 7, 2026), at <https://www.hipaajournal.com/conduent-business-solutions-data-breach/>.

¹⁰¹ *Conduent letter to the New Hampshire Office of the Attorney General* (Oct. 24, 2025), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-services-20251024.pdf>.

¹⁰² *Data Breach Notifications*, MAINE ATTORNEY GENERAL, at <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/389e9d0d-8e23-497d-aaab-1c4c8a80707f.html> (last visited Jan. 16, 2026).

¹⁰³ *Conduent Business Services LLC*, WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL, at <https://www.atg.wa.gov/conduent-business-services-llc> (last visited Jan. 16, 2026).

¹⁰⁴ *Letter from Conduent to Office of the Attorney General of Iowa's Consumer Protection Division* (Oct. 24, 2025), at https://www.iowaattorneygeneral.gov/media/cms/10242025_Conduent_Business_Services_BEB2AC7689CF4.pdf.

¹⁰⁵ *Security Breach Notices*, SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS, at <https://consumer.sc.gov/identity-theft-unit/security-breach-notices> (last visited Jan. 16, 2026).

¹⁰⁶ *Data Breach Notification Report*, COMMONWEALTH OF MASS. OFFICE OF CONSUMER AFFAIRS AND BUSINESS REGULATION (2025), at <https://www.mass.gov/doc/data-breach-report-2025/download>.

- c. On November 19, 2025: Conduent reported 915 more New Hampshire residents.¹⁰⁷ Conduent reported to the Maine Attorney General that an additional 25 Maine residents that were impacted by the Data Breach through its client South Carolina State Disbursement Unit (“SC-SDU”).¹⁰⁸ Conduent told the Washington Attorney General’s Office that it had begun notifying an additional 11,690 Washington state residents that their Private Information was impacted by the Data Breach.¹⁰⁹ Conduent reported to South Carolina that an additional 33,927 South Carolina residents were impacted.¹¹⁰ Conduent reported that an additional 44 Massachusetts residents had their social security numbers impacted by the Data Breach.¹¹¹
- d. On December 18, 2025: Conduent disclosed 44,010 New Hampshire residents.¹¹² Conduent told the Washington Attorney General’s Office that it had begun notifying an additional 330,819 Washington state residents that their Private Information was impacted by the Data Breach.¹¹³
- e. On January 2, 2026: Conduent reported to the New Hampshire Attorney General that an additional 12,666 New Hampshire residents were impacted by the Data Breach.¹¹⁴ Conduent told the Washington Attorney General’s Office that it had begun notifying an additional 9,459 Washington state residents that their Private Information was impacted by the Data Breach.¹¹⁵ Conduent reported to the Texas Attorney General that 14.7 million individuals in Texas alone were impacted, along with 31.5 million individuals nationwide.

¹⁰⁷ *Conduent letter to the New Hampshire Office of the Attorney General* (Nov. 19, 2025), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-state-local-solutions-20251119.pdf>.

¹⁰⁸ *Data Breach Notifications*, MAINE ATTORNEY GENERAL, at <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5824868b-e7f7-4495-8e1e-4cd95f55e80c.html> (last visited Jan. 16, 2026).

¹⁰⁹ *Conduent Letter to the Washington State Attorney General’s Office* (Nov. 19, 2025), at <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA35139.pdf>.

¹¹⁰ *Security Breach Notices*, SOUTH CAROLINA DEPARTMENT OF CONSUMER AFFAIRS, at <https://consumer.sc.gov/identity-theft-unit/security-breach-notices> (last visited Jan. 16, 2026).

¹¹¹ *Id.*

¹¹² *Conduent letter to the New Hampshire Office of the Attorney General* (Dec. 18, 2025), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-20251218.pdf>.

¹¹³ *Conduent Letter to the Washington State Attorney General’s Office* (Dec. 18, 2025), at <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA35139.pdf>.

¹¹⁴ *Conduent letter to the New Hampshire Office of the Attorney General* (Jan. 2, 2026), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-services-20260102.pdf>.

¹¹⁵ *Conduent Letter to the Washington State Attorney General’s Office* (Jan. 2, 2026), at <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA35139.pdf>.

- f. January 30, 2026 - February 2, 2026: Conduent reported that an additional 150,313 impacted Washington State residents were being notified.¹¹⁶ Conduent reported to the Texas Attorney General that the number of impacted Texans had increased to 15,494,592, and the number impacted nationwide had increased to 44,499,385. Conduent reported that approximately half of the population of Illinois was impacted.¹¹⁷ Conduent notified the New Hampshire Attorney General that it began notifying an additional 112,952 New Hampshire residents.¹¹⁸

210. Defendants have not explained why the number of impacted victims continues to rise, or why they did not understand the scope of the Breach when first reported.

211. Defendants waited even longer to directly notify victims. On or about October 24, 2025, roughly nine months after Conduent and Insurer Defendants first learned the Class's Private Information was compromised, Defendants finally began notifying Plaintiffs and Class Members of the Data Breach through mailed Notice of Data Incident letters ("Notice Letters").

212. In the Notice Letters, Conduent described the Data Breach as an "incident" involving Plaintiffs' and Class Members' Private Information, which came into Conduent's possession due to the services that it provides to Insurer Defendants.

213. Omitted from the Notice Letters are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, the unauthorized actor responsible for the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. Further, many Notice Letters do not identify the Insurer Defendant that provided Conduent with the victim's Private Information. To date, these critical facts have not been explained or clarified to Plaintiffs

¹¹⁶ *Conduent Letter to the Washington State Attorney General's Office* (Jan. 30, 2026), at <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA35139.pdf>.

¹¹⁷ *Data Breach Notice to Office of the Illinois Attorney General*, at <https://databreachnoticetoattorneygeneral.illinoisattorneygeneral.gov/portal/Workflow/Run?workflowId=g8b79c5d8-c80a-41eb-987c-27cb35a94332&ewd=UHO2SsQxEbvjNdQbMD2R4FdaYdSmQTHJCnM0CKvsiaquVBabzQC65wVjDjdTE%2fxMH9x6%2bA%3d%3d>.

¹¹⁸ *Supplemental Notice of Security Incident* (Feb. 2, 2026), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-services-20260202.pdf>.

and Class Members, who retain a vested interest in ensuring that their Private Information is protected. Instead, the Notice Letters mischaracterize the Data Breach and downplay the risk to victims:

What Happened? On January 13, 2025, we discovered that we were the victim of a cyber incident that impacted a limited portion of our network. . . . Our investigation determined that an unauthorized third party had access to our environment from October 21, 2024, to January 13, 2025, and obtained some files associated with [your current or former health plan]. . . . We are providing you with this notice upon the recent conclusion of this time-intensive data analysis as your personal information was contained in the affected files.

What We Are Doing? Upon discovery of the incident, we safely restored our systems and operations and notified law enforcement. We are also notifying you in case you decide to take further steps to protect your information should you feel it appropriate to do so....

214. Defendants’ notice to victims uniformly state that Defendants have “no evidence” of actual or attempted misuse of victims’ Private Information, ignoring that consumers’ Private Information had been targeted by financially motivated cybercriminals who then exfiltrated it and held for ransom.

215. Defendants’ purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach’s critical facts with any degree of specificity. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

216. Further, the Notice Letters offer no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing, in some instances, a year of credit monitoring—an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach.

217. Defendants have represented to various regulators that, in addition to the Notice Letters, they have provided “substitute notice provided by website notice and media notice.”¹¹⁹

218. Defendants’ purported substitute notices provide even less information than the individual notices sent to impacted individuals, and are similarly inadequate because Defendants downplay the scope of the Data Breach and the risk to Plaintiffs and Class Members.

219. Further Conduent configured its website notices so that Plaintiffs and Class Members cannot locate Conduent’s website notices by searching on Google, Bing, or other search engines. Specifically, Conduent’s website notices each contain a “Noindex, nofollow” tag, excluding the website notices from appearing in search results.

220. Defendants’ decision to wait until October 24, 2025, to begin providing substantive notice to victims and regulators—more than 10 months after detecting the Data Breach, and more than an entire year after the Data Breach occurred—is indefensible. This extraordinary delay violates Defendants’ responsibilities to Plaintiffs and Class Members and various data breach notification statutes, which require that disclosure be made in the most expedient time possible and without unreasonable delay.

221. Publicly available information about Defendants’ conduct during the ten-month gap between their discovery of the Breach and when Defendants began notifying victims confirms that this delay was unjustified. Nothing suggests Defendants faced any legal, technical, or operational barrier that prevented earlier notification. To the contrary, the available facts demonstrate

¹¹⁹ See, e.g., *Conduent Letter to the New Hampshire Office of the Attorney General* (Oct. 8, 2025), at <https://mm.nh.gov/files/uploads/doj/remote-docs/conduent-business-services-20251008.pdf>; *Conduent Letter to the Office of the Attorney General of Iowa* (Oct. 24, 2025), at https://www.iowaattorneygeneral.gov/media/cms/10242025_Conduent_Business_Services_BEB2AC7689CF4.pdf.

Defendants' silence was the result of choice not necessity, and that the delay served their own interests at the expense of those they were required to protect.

222. For example, Cigna has confirmed Conduent notified Cigna about the Data Breach on January 15, 2025. Cigna claims Conduent confirmed Cigna data was impacted on September 3, 2025. Yet Conduent and Cigna did not begin notifying impacted victims of the Data Breach until December 11, 2025.

223. Further, a partner of Elevance confirmed Defendants "took extra time" to assess the data, resulting in Elevance and Conduent failing to begin notifying victims until the week of December 1, 2025."¹²⁰

224. Likewise, HCSC confirmed that it received notice of the Data Breach on January 17, 2025. HCSC reported that Conduent performed a data analysis that took until July 2025, when Conduent "provided the raw data to us."¹²¹ However, Conduent apparently did not "provide[] specific data elements" that were breached for each person.¹²² "Due to the way the data was compiled when provided to [HCSC]," HCSC reported that it "subsequently undertook an evaluation to determine and verify the identity of the impacted members and which groups the individuals belonged to, which was a time-consuming process."¹²³

¹²⁰ *Anthem | Cybersecurity Breach May Have Impacted your Small Group Clients*, AMWINS CONNECT (Dec. 29, 2025), at <https://www.amwinsconnect.com/knowledge-hub/news-desk/news-detail/anthem---cybersecurity-breach-may-have-impacted-your-small-group-clients>.

¹²¹ *Conduent Cybersecurity Incident Frequently Asked Questions*, BCBSNM (Oct. 2025), at https://www.nmrhca.org/wp-content/uploads/2025/10/NM_Group_FAQs-1.pdf.

¹²² *Conduent Cybersecurity Incident Frequently Asked Questions*, BCBSTX, at <https://healthselect.bcbstx.com/pdf/conduent-incident-faq.pdf> (last visited Feb. 4, 2026); *Conduent Cybersecurity Incident Frequently Asked Questions*, BCBSNM (Oct. 2025), at https://www.nmrhca.org/wp-content/uploads/2025/10/NM_Group_FAQs-1.pdf.

¹²³ *Id.*

225. By withholding notice, including, for many, for a year or more, Defendants materially compounded the harm the Data Breach caused. Plaintiffs and Class Members were deprived of the opportunity to monitor their financial accounts, credit reports, and medical or insurance records during the critical period when misuse was most likely. Because Defendants concealed the Breach for 10 months, victims were left entirely unaware their Private Information had been stolen and held for ransom by a known cybercriminal group, preventing them from taking even the most basic steps to protect themselves from identity theft and fraud.

226. Regulators have called Defendants' failure to disclose the data breach "disturbing." Montana law requires that any regulated company report a data breach involving residents' PII "without unreasonable delay," yet, the Montana Commissioner of Securities and Insurance received notice of the Breach for the first time on October 8, 2025. The Commissioner has opened an investigation into whether HCSC (through its division BCBSMT) failed to report the Breach in a timely manner and failed to notify potentially affected policyholders. "While we acknowledge that investigation of security incidents can take time, the [office] is troubled by the length of time that has expired between awareness of the data breach, notification to our agency, and member notification, the provision for credit monitoring and identity protection services," Deputy Commissioner of Insurance Erin Snyder wrote in an October 16 letter to Blue Cross Blue Shield.¹²⁴

227. When asked about the Data Breach, Montana Auditor and insurance commissioner James Brown's office stated as follows:

This breach is not just a technical lapse. This is a deeply disturbing incident with far-reaching and jaw-dropping consequences for our citizens. . . . Montanans have every right to expect their personal data, especially sensitive health information, to

¹²⁴ Carly Graf, *Data breach puts medical info of 462,000 Blue Cross Blue Shield Montana Customers at Risk*, INDEPENDENT RECORD (Oct. 28, 2025), at <https://insurancenewsnet.com/oarticle/data-breach-puts-medical-info-of-462000-blue-cross-blue-shield-montana-customers-at-risk>.

be protected by the entities they trust. The severity of this breach underscores the urgent need for robust oversight and our agency to take swift and immediate action to protect Montana consumers.^[125]

228. Further, Defendants have *still* failed to notify all victims of the Data Breach; as the numbers of impacted victims continue to grow exponentially, Defendants' notice efforts will not be complete until April 15, 2026.

V. The Data Breach Was a “Striking Example of Preventable Failure” by Defendants.¹²⁶

229. Data breaches concerning medical records and/or healthcare have been on a steady upward trend for over a decade. According to the *HIPAA Journal*, these incidents have increasingly involved millions of affected patients. High-profile breaches at healthcare providers and related service companies in recent years include Change Healthcare, Inc. (affecting 190 million individuals in 2024); Anthem, Inc. (affecting 78.8 million individuals in 2015); American Medical Collection Agency (affecting more than twenty-six million individuals in 2019); Welltok, Inc. (affecting 14.7 million individuals in 2023); Premiera Blue Cross (affecting eleven million individuals in 2015); CareSource (affecting more than three million individuals in 2023); Perry Johnson & Associates, Inc. (affecting 9.3 million people in 2023); Excellus Health Plan, Inc. (affecting ten million individuals in 2015); and many more.

230. Data breaches in the healthcare sector outnumber those in other sectors by a wide margin. An analysis of data breaches recorded on the Privacy Rights database between 2015 and

¹²⁵ *Commissioner James Brown Launches Formal Investigation Into Blue Cross Blue Shield Following Major Data Breach*, COMMISSIONER OF SECURITIES & INSURANCE (Oct. 22, 2025), at <https://csimt.gov/2025/10/27/commissioner-james-brown-launches-formal-investigation-into-blue-cross-blue-shield-following-major-data-breach/>.

¹²⁶ *See* Joan Levin, *HIPAA Compliance in 2026: What IT Healthcare Leaders Need to Know*, CALCOM (Jan. 12, 2026), at <https://calcomsoftware.com/hipaa-compliance-in-2026-what-it-healthcare-leaders-need-to-know/>.

2022 showed that 32% of all recorded data breaches were in the healthcare sector—almost double the number recorded in the financial and manufacturing sectors.

231. In 2018, the healthcare sector reported the second largest number of data breaches among all measured sectors, with the highest rate of exposure per breach.

232. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 victims' sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the healthcare industry. The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), an increase from the 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

233. In 2022, entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors, with the highest rate of exposure per breach.

234. In 2023, 725 data breaches were reported to the HHS Office for Civil Rights (“OCR”), exposing over 133 million records.

235. According to the HIPAA Journal, “[t]here are so many more data breaches in the healthcare sector than in other sectors because healthcare data is more valuable on the black market than any other type of data.”¹²⁷ “This is because it takes longer for healthcare fraud to be discovered and stolen data can be used for longer compared to (for example) a stolen credit card.”¹²⁸

236. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that victims were often

¹²⁷ Steve Alder, *Healthcare Data Breach Statistics*, THE HIPAA JOURNAL (Jan. 4, 2026), at <https://www.hipaajournal.com/healthcare-data-breach-statistics/>.

¹²⁸ *Id.*

forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.¹²⁹ Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.

237. Put differently, companies in the healthcare sector “sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security numbers and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹³⁰

238. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendants have become so notorious that the FBI and U.S. Secret Service have issued warnings to potential targets so they are aware of, and prepared for, a potential attack.

239. For example, in August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated, “The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”¹³¹

¹²⁹ See Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), at <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>.

¹³⁰ Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXECUTIVE (Apr. 4, 2019), at <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks>.

¹³¹ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), at <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcarefirms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820>.

240. Further, in October 2020, in response to growing cybersecurity threats, the Federal Bureau of Investigation (“FBI”), CISA, and HHS issued a Joint Cybersecurity Advisory warning U.S. healthcare entities of a “credible and imminent cybercrime threat” and urging immediate implementation of robust, layered security defenses.¹³²

241. The American Medical Association has also warned healthcare companies about the importance of protecting their patients’ confidential information, explaining,

Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that *cyberattacks not only threaten the privacy and security of patients’ health and financial information, but also patient access to care.*^[133]

242. Health-related breaches carry outsized risk. The Department of Health and Human Services’ Office for Civil Rights has repeatedly flagged the downstream harm and regulatory exposure when business associates—contractors that handle protected health information—are compromised. Unlike payment card numbers, which can be reissued, health and identity data have a long shelf life on criminal markets.

243. Business associates of healthcare organizations, like Conduent, “represent a particularly concerning risk.”¹³⁴ Two-thirds of the largest healthcare data breaches in U.S. history

¹³² *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY (October 28, 2020), at https://www.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.

¹³³ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS’N (Oct. 4, 2019), at <https://www.ama-assn.org/practicemanagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals> (emphasis added).

¹³⁴ *Study: Impact of Cloud Vendor Breaches on Healthcare*, CENSINET, at <https://www.censinet.com/perspectives/impact-cloud-vendor-breaches-healthcare> (last visited Jan. 8, 2026).

originated from third-party vendors such as business associates, according to federal records and independent breach analyses.

244. During the third quarter of 2025 alone, business associates were linked to 30 breaches (21.58% of incidents), affecting 796,552 patients. These numbers highlight the critical vulnerabilities posed by third-party vendors in healthcare cybersecurity, showing both the frequency and the far-reaching consequences of such breaches.

245. Consequently, both Conduent and Insurer Defendants knew or should have known of the importance of safeguarding Plaintiffs' and Class Members' Private Information and of the foreseeable consequences that would occur if Conduent's data security system was breached, including the significant costs that would be imposed on victims as a result of a breach.

A. Conduent Failed to Implement Basic Security Controls.

246. The Data Breach was caused by Conduent's failure to implement basic security controls to protect Plaintiffs' and Class Members' Private Information.

247. Conduent's clients report that during the Data Breach, the cybercriminals accessed Conduent's network through a single set of compromised VPN credentials, demonstrating that Conduent failed to institute appropriate credential management practices that allowed the cybercriminals to initially access Conduent's systems. Further, Conduent failed to maintain a strong authentication process, including multi-factor authentication, making the cybercriminals' sustained, unauthorized significantly easier.

248. According to Conduent's notification to the Texas Attorney General, the impacted Private Information stored on Conduent's systems was *not encrypted*—a major departure from industry-standard safeguards.

249. By virtue of the cybercriminals' access to millions of customers' Private Information, Conduent also lacked appropriate network segmentation, leaving sensitive data

accessible across broad portions of its environment rather than compartmentalized in restricted, high-security zones, which is a basic safeguard that should have limited attackers' lateral movement and contained the Data Breach.

250. Further, Conduent's systems lacked internal monitoring to such a degree that the cybercriminals' access to Conduent's network was not detected until *the hackers chose* to reveal themselves during the January 13, 2025, ransomware attack. SafePay's activity in Conduent's network should have been noticed by Conduent through proper endpoint and network monitoring and scanning, which would have prevented the attackers from exfiltrating terabytes of Private Information without alarm bells going off. Such actions should have only been possible by Conduent network administrators and should have required even administrators to pass additional security features. Such exfiltration activity should have been detected and raised numerous red flags to Conduent had it properly monitored its network.

251. At all relevant times, Conduent was aware that its lax data security infrastructure put Plaintiffs' and Class Members' Private Information at severe risk.

252. Since its formation, Conduent has acknowledged in its annual reports that deficiencies in its ability to safeguard the sensitive information entrusted to it—including the Private Information of Plaintiffs and Class Members—pose material risks to the company's financial performance, regulatory exposure, and overall operational stability.

253. In its first annual report, filed in March 2017, Conduent acknowledged that it is subject to numerous laws and regulators "designed to protect both individually identifiable information and personal health information, including [HIPAA] . . . governing, among other things, the privacy, security, and electronic transmission of individually identifiable health information" and that "failure to comply with those laws, whether or not inadvertent," could

subject it to “ additional costs or changes to our business practices, liability for monetary damages, fines and/or criminal prosecution, unfavorable publicity, *restrictions on our ability to obtain and process information* and allegations by our customers and clients that we have not performed our contractual obligations, any of *which could materially adversely affect our results of operations and financial condition*.”¹³⁵

254. Conduent stated that it understood the grave risks of a data breach to its systems, explaining, “If unauthorized parties gain physical access to one of our . . . information systems . . . *any theft or misuse of such information could result in*, among other things, unfavorable publicity, governmental inquiry and oversight, *difficulty in marketing our services*, allegations by our customers and clients that we have not performed our contractual obligations, litigation by affected parties and possible financial obligations for damages related to the theft or misuse of such information, any of which could materially adversely affect our results of operations and financial condition. Moreover, a security breach could require us to devote significant management resources to address the problems created by the security breach and to expend significant additional resources to upgrade further the security measures that we employ to guard such important personal information against cyber attacks maintain various systems and data centers for our customers.”¹³⁶

255. Thus, Conduent explained that it had “implemented security systems . . . with the intent of maintaining . . . the data security of our customers’, clients’ and suppliers’ confidential information and information related to identifiable individuals . . . against unauthorized access

¹³⁵ *Conduent 2016 Annual Report*, CONDUENT, INC. (2016), at <https://investor.conduent.com/static-files/d650864e-1415-45c1-8b8f-131a954a1e28> (emphasis added).

¹³⁶ *Id.*

through our information systems[.],” representing that these measures included “for example, the appropriate encryption of information.” Conduent acknowledged that “we may be required to expend significant capital and other resources to protect against potential security breaches” and that “faulty password management” may result in a breach of its IT systems.¹³⁷

256. In its 2017 annual report, Conduent disclosed that it was “subject to breach of security systems which may result in unauthorized access to our facilities and those of our customers and/or *the information we and our customers are trying to protect.*” Conduent explained that not only had “[h]acking, malware, phishing, viruses, and other ‘cyber-attacks’ . . . become more prevalent,” but that such cyber-attacks “*have occurred in our systems in the past.*”¹³⁸ Conduent emphasized that Conduent’s receipt of “substantial volumes” of sensitive identifiable information, meant that “the integrity, security, accuracy, and non-interruption of our systems... are *extremely important* to our business, operating results, growth, prospects, and reputation.”¹³⁹

257. Then, in its 2018 annual report, Conduent disclosed that “failures or delays in our efforts to modernize our information technology infrastructure” was a material risk to the company’s operations, explaining that it had “experienced certain disruptions in our operations and service delivery performance issues as a result of some of our information technology infrastructure that is outdated and needs to be enhanced and updated.” “As a result,” Conduent announced it was “investing in modernizing a significant portion of our information technology

¹³⁷ *Id.*

¹³⁸ 2017 Annual Report, CONDUENT, INC. (2017), at <https://investor.conduent.com/static-files/54a4950a-9b13-434c-85b9-487e8a3c3bce>

¹³⁹ See, e.g., *id.*; 2022 Annual Report, CONDUENT, INC. (2022), at p. 22, <https://www.sec.gov/Archives/edgar/data/1677703/000167770323000022/conduent-2022xannualxrep.htm>; 2024 Annual Report, CONDUENT, INC. (2024), at <https://investor.conduent.com/static-files/d1e7d57e-8ec7-43dc-b9c0-ac84d46469a9>.

infrastructure with new systems and processes” including “investments in our data centers and networks, enhancement, modernization, and consolidation of our IT infrastructure[,] [and] *enhanced cybersecurity*.” Conduent stated that it “expect[ed] that these changes will provide . . . better control of our systems and processes[,]” but that there was a risk that the modernization efforts “could occur over a longer period than planned.”¹⁴⁰

258. Conduent has included a similar statement about the risks of its outdated IT infrastructure in every yearly report since 2018; in 2022, Conduent began referring to its project to modernize its IT structure as “a long-term project,” suggesting that Conduent is still operating with immature IT systems.

259. These disclosures make clear that Conduent has long understood that failures in its data-security practices could lead to significant legal liability, government investigations, lost business, and reputational harm. Yet despite recognizing these risks at the highest levels of corporate governance and warning investors of the consequences, Conduent failed to take the basic, industry-standard precautions necessary to prevent the Data Breach. These filings underscore that the harm suffered by Plaintiffs and Class Members was not only foreseeable, but directly tied to vulnerabilities Conduent had already identified internally and publicly conceded could have catastrophic consequences if left unaddressed.

260. Conduent repeatedly uses the risky cybersecurity landscape in which it operates as a marketing tool to corporate clients. Representing on its website that “[a] data breach costs Fortune 500 companies an average of \$347M in legal fees, penalties, remediation and more,”¹⁴¹

¹⁴⁰ See, e.g., *2018 Annual Report*, CONDUENT, INC. (2018), at <https://investor.conduent.com/static-files/b9532ac5-b2f8-4d46-9187-2fd771c9e767>.

¹⁴¹ *Outsourcing Transformation*, CONDUENT, at <https://www.conduent.com/outsourcing-transformation/> (last visited Jan. 8, 2026).

Conduent uses this point to market its services: “Business-critical communications require airtight data security. . . . Properly vetting a potential provider is crucial since cybersecurity attacks are on the rise and can prevent third parties in the transactional space from getting critical communications out in a timely, compliant manner.”¹⁴²

261. In 2022 Conduent published a “2022 Post Incident Privacy Review: The key to successful cyber incident response” white paper. In the blog advertising this white paper, Conduent acknowledges, “Organizations are dealing with more cyberattacks than ever, with 50% more attacks on corporate networks in 2021 than in 2020.”¹⁴³

262. In a blog titled “What is incident response in cybersecurity” Conduent acknowledges the risks it and companies face. “‘2TB of user data was breached in the latest cyber-attack.’ That’s unfortunately a real headline that is all too common. . . . Entire industries, jobs and lives can be impacted for an indeterminate amount of time and require a swift response. It’s a hard truth: With new technologies comes new risks of a data breach. But there are ways to proactively protect your organization, end users and yourself. Incident response (IR) is the systematic approach taken to manage and mitigate the effects of a cyber incident. Understanding incident response is crucial for organizations of all sizes.”¹⁴⁴

¹⁴² Pamela Visconti, *Considerations for mitigating risk when outsourcing critical communications*, CONDUENT BLOG, at https://insights.conduent.com/conduent-blog/considerations-for-mitigating-risk-when-outsourcing-critical-communications?_gl=1*lvf4uq*_up*MQ..*_ga*NzI0Mjk1MDYyLjE3NjE3ODk5NTU.*_ga_21 (last visited Jan. 8, 2026).

¹⁴³ *2022 Post Incident Privacy Review: The key to successful cyber incident response*, CONDUENT (2022), at <https://www.conduent.com/insights/2022-post-incident-privacy-review/>.

¹⁴⁴ *What is incident response in cybersecurity?*, CONDUENT BLOG, at <https://insights.conduent.com/conduent-blog/what-is-incident-response-in-cybersecurity> (last visited Jan. 8, 2026).

263. In the same article, Conduent recognizes the psychological terror victims of identity theft and cybercrime experience: “If you’ve ever experienced a data breach or had your identity stolen, you understand the sheer sense of panic that sets in as you watch sensitive information altered or even currency stolen right out of your bank accounts. It’s a helpless feeling[.]”¹⁴⁵

264. Conduent lays out the five key phases of incident response: (1) preparation: “[o]rganizations must ensure they have the right tools and technologies in place to detect and respond to incidents effectively”; (2) identification: “organizations must quickly detect and ascertain the nature of the incident. This involves monitoring security alerts, analyzing logs and investigating potential threats to confirm that an incident has occurred”; (3) containment: “[o]nce an incident is identified, immediate action must be taken to contain the threat”; (4) eradication: “it is essential to ensure that the threat is fully eradicated before moving on to the next phase.”; and (5) recovery: “organizations work to restore systems and services to normal operation while monitoring for any signs of weaknesses or further incidents.” Although styled as a five phase plan, Conduent includes a sixth Lesson Learned: “[O]rganizations should conduct a thorough review of the response process. This phase is focused on analyzing what worked, what didn’t and how to improve future incident response efforts.”¹⁴⁶

265. According to Conduent, “a strong incident response framework is non-negotiable for organizations looking to protect their assets and reputation.”¹⁴⁷ Despite this representation, Conduent did not have a strong incident response framework.

¹⁴⁵ *Id.*

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

266. Conduent repeatedly acknowledges and bases its advertisements on the increasing frequency of data breaches: “Look to providers whose core competencies include shoring up their infrastructure to keep customers information secure.”¹⁴⁸

267. Yet Conduent ignored basic data security best practices, causing the Data Breach and at least three other highly preventable data breaches in the past six years.

268. For example, in May 2020, Conduent suffered a ransomware attack during which cybercriminals known as the Maze ransomware gang encrypted Conduent’s devices and stole corporate data, disrupting Conduent’s European operations. Maze then posted 1GB worth of Conduent’s stolen files to the dark web. The files, titled “BusinessIntelligence.zip” and “Compliance1.zip,” included various financial spreadsheets, customer audits, invoices, commission statements, and other miscellaneous documents. Reports of the data breach reveal that Maze gained access to Conduent’s environment by targeting a “widely publicized Citrix vulnerability” that had been disclosed in December 2019.¹⁴⁹ According to one source, Conduent left the Citrix server unpatched for at least eight weeks despite receiving notice of the vulnerability, resulting in the attack.

269. In 2023, an unnamed threat actor used a series of phishing attacks targeting Conduent employees to carry out a data breach of Conduent’s network that—just like the Data Breach—went undetected by Conduent for three months.

¹⁴⁸ Pamela Visconti, *Considerations for mitigating risk when outsourcing critical communications*, CONDUENT BLOG, at https://insights.conduent.com/conduent-blog/considerations-for-mitigating-risk-when-outsourcing-critical-communications?_gl=1*lvf4uq*_up*MQ..*_ga*NzI0Mjk1MDYyLjE3NjE3ODk5NTU.*_ga_21 (last visited Jan. 8, 2026).

¹⁴⁹ Phil Muncaster, *IT Services Firm Conduent Felled by Maze Ransomware*, INFOSECURITY MAGAZINE (June 8, 2020), at <https://www.infosecurity-magazine.com/news/it-services-firm-conduent-felled/>.

270. The attacker reportedly breached Conduent’s network through a high-ranking HR personnel’s account, which was devoid of multi-factor authentication. Through the compromised account, the attacker claimed he had unauthorized access to company emails, chatrooms, and confidential data. In an article titled *Conduent Data Breach: Threat Actor Frustrated With Organizational Negligence*, the Cyber Express reported the attacker expressing “frustration” over the fact that he had not been caught:

For three months, I had full access to an employee in a cybersecurity role within the company whose email revealed the information of MANY, if not all, critical infrastructure.... At one point, she had changed her password, which shockingly, I guessed was the new one.... I have never met such a dumb company; it’s honestly shocking... [t]his company is a prime example of what not to do, first off this ENTIRE situation could have been avoided if they implemented a system to stop people using similar passwords and I would have lost access MONTHS ago.^[150]

271. The 2023 breach “exposed a glaring security lapse, with the attacker criticizing the company’s weak password practices and emphasizing the urgency of implementing robust password policies.”¹⁵¹

272. Finally, in or around March 2024, an unknown actor used a Conduent employee’s login credentials to hack into an unstructured SharePoint data repository Conduent managed with one of its corporate clients, HealthEquity, Inc., resulting in the access to and exfiltration of 4.3 million individuals’ PII. Conduent failed to discover the March 2024 breach until three months after it took place. This 2024 breach and the prolonged period until Conduent discovered it again highlights Conduent’s weak password practices and deficient monitoring and alerting methods.

¹⁵⁰Ashish Khaitan, *Conduent Data Breach: Threat Actor Frustrated With Organizational Negligence*, THE CYBER EXPRESS (Sept. 27, 2023), at <https://thecyberexpress.com/conduent-data-breach-detected-after-3-months/>.

¹⁵¹ *Id.*

B. Insurer Defendants Failed to Exercise Appropriate Vendor Management.

273. Each Insurer Defendant failed to exercise appropriate oversight and vendor management practices to continuously monitor and ensure the safety of the Private Information it shared with Conduent. Conduent's failure to implement basic credential management, authentication processes, encryption, network segmentation, and internal monitoring were basic security failures that should have been discovered by or known to Insurer Defendants before the Data Breach.

274. Insurer Defendants knew or should have known that they were putting Plaintiffs' and Class Members' Private Information at severe risk.

275. At all relevant times, Insurer Defendants knew or should have known that their customers' data, including data belonging to Plaintiffs, and Class Members, would be targeted by cybercriminals and ransomware attack groups.

276. Described above, the healthcare industry has been increasingly targeted by cyberattacks, and Insurer Defendants are and were well aware of the high risk of data breaches.

277. High profile data breaches in for similar industry leaders in healthcare put them on notice of this fact, *e.g.*, American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), put Defendants on notice that their electronic records would be targeted by cybercriminals.

278. As a particularly salient example, in February 2024—eight months before the Data Breach began—a massive attack on Change Healthcare, a subsidiary of insurer UnitedHealth,

disrupted health care operations on an unprecedented national scale, endangering patients' access to care, disrupting critical clinical and eligibility operations, and threatening the solvency of the nation's provider network.

279. Insurer Defendants themselves have been impacted by recent major data breaches. For example, Humana contracted with Cotiviti, a healthcare analytics company, for processing requests for medical records sent to CMS. Cotiviti subcontracted with Visionary for some of this work. Between October and December 2020, a Visionary employee used security credentials to transfer private and confidential medical records of Humana members to a personal Google Drive account, as part of a personal coding business. Humana alerted 65,000 individuals that their data was exposed as part of this breach.

280. In 2022, Choice Health, a third party used by which Humana and Anthem, experienced a cyber-attack in which an unauthorized party gained access to Choice Health's system and stole customer data, including PHI. Those customers impacted included (but was not limited to) Humana and Anthem customers. Humana reportedly disclosed to the Maine Attorney General that 22,767 individuals (*not* limited to Maine) were impacted. Anthem disclosed to the Maine Attorney General that 13,406 individuals (*not* limited to Maine) were impacted.

281. In 2023, Forta experienced a ransomware attack from Russian-linked group Cl0p. NationsBenefits stored patient data on Forta's platform. The Forta/NationsBenefits breach compromised the private information of 3,037,302 current and former plan members of Elevance, Cigna, and others.

282. Thus, Insurer Defendants knew or should have known the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences if their

systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

283. Despite such knowledge, Insurer Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' private information from cyberattacks, including, but not limited to, adequately vetting, auditing, and monitoring their third-party vendors.

284. According to Conduent: "Properly vetting a potential provider is crucial since cybersecurity attacks are on the rise and can prevent third parties in the transactional space from getting critical communications out in a timely, compliant manner."¹⁵² Yet, Insurer Defendants each failed to appropriately vet Conduent's cybersecurity infrastructure to ensure the safety of Plaintiffs' and Class Members' Private Information.

285. Insurer Defendants failed to appropriately vet Conduent's cybersecurity infrastructure despite publicly acknowledging the risk caused by Insurer Defendants' choice to share Plaintiffs' and Class Members' Private Information with vendors like Conduent.

286. For example, AIG acknowledges in its annual reports that deficiencies in its ability to safeguard the sensitive information entrusted to it—including the Private Information of Plaintiffs and Class Members—pose material risks to the company's financial performance, regulatory exposure, and overall operational stability.

287. In AIG's 2024 Annual Report for the enterprise, it acknowledges:

Like other global companies, the systems and networks we maintain and third-party systems and networks we or our vendors use are currently, and may in the future

¹⁵² Pamela Visconti, *Considerations for mitigating risk when outsourcing critical communications*, CONDUENT BLOG, at https://insights.conduent.com/conduent-blog/considerations-for-mitigating-risk-when-outsourcing-critical-communications?_gl=1*lvf4uq*_up*MQ..*_ga*NzI0Mjk1MDYyLjE3NjE3ODk5NTU.*_ga_21 (last visited Jan. 8, 2026).

continue to be, subject to or targets of unauthorized or fraudulent access... as well as attempted cybersecurity threats such as “denial of service” attacks, phishing, automated attacks, and other disruptive attacks, including ransomware.

288. American International Group, Inc. represents that the group of companies maintains a documented Information Security Program that includes, as a “key element” a “Third-Party Assessment and Oversight” program “designed to identify and manage cybersecurity risks from third-party service providers, including initial due diligence as well as initial and periodic re-assessments of the service provider’s control environment.” According to American International Group, Inc., that program is “evaluated on an ongoing basis, both internally and through third-party audit firms, to address and protect against the evolving cyber threat landscape. . . . Control adequacy and design are reviewed at least annually. Independent audits and penetration tests assist in identifying areas for continued focus, improvement and/or inclusion, and are designed to provide assurance that controls are appropriately designed and operating effectively. Additionally, our Internal Audit group performs independent testing of our control environment, including key components of the Program.”¹⁵³ American International Group, Inc.’s Board “oversees the Program . . . given the increasing importance of cybersecurity to our risk profile, as well as the significant role our technology strategy plays in our strategic priorities.”¹⁵⁴

289. Likewise, Cigna acknowledges in its annual reports that deficiencies in its ability to safeguard the sensitive information entrusted to it—including the Private Information of Cigna Plaintiffs and Class Members—pose material risks to the company’s financial performance, regulatory exposure, and overall operational stability.

¹⁵³ 2024 Form 10K, AIG, at <https://www.sec.gov/Archives/edgar/data/5272/000000527225000012/aig-20241231.htm>.

¹⁵⁴ *Id.*

290. For example, in Cigna’s 2023 Annual Report, Cigna acknowledged that its “business depends on our clients' and customers' willingness to entrust us with their health-related and other personal information (“PI”), including Protected Health Information (“PHI”) that is subject to privacy, security or data breach notification laws” and that “as a large global company we *and our vendors* are subject to cyberattacks. . . . *If we are unable to prevent or contain the effects of any such attacks, or fail to ensure vendors do the same*, we may suffer exposure to substantial liability, reputational harm, loss of revenue or other damages.” Further, Cigna acknowledged that “the unauthorized access, acquisition, use, disclosure or dissemination of personal information . . . could expose our customers' and their private information to the risk of financial or medical identity theft.”¹⁵⁵

291. Past security incidents of third-party vendors put Cigna on notice of the importance of appropriate third-party vendor oversight practices. From July 31 to August 3, 2023, Cigna’s administrative services vendor, Prospect Medical Holdings, Inc., experienced a data security incident that involved unauthorized access to Prospect’s IT environment. Prospect notified Cigna of the data breach on September 29, 2023—yet Cigna did not begin notifying members whose information was impacted until January 31, 2024. Further, in February 2024, Change Healthcare, a health technology company owned by UnitedHealth Group and a service provider for certain of Cigna’s pharmacy benefit management services, was the victim of a ransomware attack that resulted in disruption of Cigna’s services and necessitated security validations for certain systems.

292. Acknowledging the role of its inadequate third-party vendor oversight activities in the Data Breach, Cigna has announced that “several services have been transitioned to other

¹⁵⁵ 2023 Form 10K, CIGNA, at <https://www.sec.gov/Archives/edgar/data/1739940/000173994024000005/ci-20231231.htm>.

vendors, reducing [Conduent’s] role in Cigna Healthcare’s operations. Cigna Healthcare continues to review its relationship with this vendor through our third-party vendor oversight activities. This includes periodic security assessments and ensuring appropriate privacy and security controls.”¹⁵⁶

293. Further, Elevance acknowledges in its annual reports that deficiencies in its ability to safeguard the sensitive information entrusted to it—including the Private Information of Plaintiffs and Class Members—pose material risks to the company’s financial performance, regulatory exposure, and overall operational stability.

294. For example, in Elevance’s 2024 Annual Report, it explains: “We have programs in place to detect, contain and respond to data, privacy and security incidents and provide employee awareness training regarding phishing, malware, and other risks to protect against privacy and cybersecurity incidents. Our facilities and systems, and those of our third-party service providers, including our business associates, are regularly the target of, and may be vulnerable to, cyber-attacks,” and “[o]ur management implements ongoing and annual risk assessment processes to identify and manage risks that could affect our ability to safeguard sensitive data or provide reliable transaction processing and to minimize financial risk exposure. These risks include . . . third-party management.”

295. HCSC’s Chief Information Security Officer has publicly acknowledged that the company is “a target with a very capable and highly motivated adversary” because of the “vast amounts of information that’s highly sensitive” in its possession, custody, and control. Underscoring the risk, he explained that cyber threats to HCSC’s customer information “aren’t [from] loose knit organizations of a few people working in the basement of somebody’s building.

¹⁵⁶ *Re: Notice of Data Breach*, CIGNA (Dec. 11, 2025), at <https://www.mass.gov/doc/2025-2038-massachusetts-mutual-life-insurance-company/download>.

They're run like Fortune 500 companies. They have a staff. They hire, they fire, they promote. They have pizza parties in the break room when a large company is hacked. They have research and development that's focused on doing nothing other than getting around technical controls. We must be ever vigilant and focus on information security as an enterprise capability to help protect our employees and members."¹⁵⁷

296. Humana also acknowledges in its 2024 Annual Report that deficiencies in its ability to safeguard the sensitive information entrusted to it—including the Private Information of Humana Plaintiffs and Class Members—pose material risks to the company's financial performance, regulatory exposure, and overall operational stability, explaining, "A cybersecurity attack that bypasses our information technology systems, or the security of our third-party service providers, could materially affect us due to the theft, destruction, loss, misappropriation or release of confidential information or intellectual property, operational or business delays resulting from the disruption of our IT systems, extortion attempts, or negative publicity resulting in reputation or brand damage with our members, customers, providers, and other stakeholders." As a result, Humana purportedly maintains "a program to identify cybersecurity risks associated with certain third-party vendors, which is one component of an overall vendor risk management program."

297. These disclosures make clear: Insurer Defendants have long understood that failures in their data-security practices, including appropriate vendor management, could lead to significant legal liability, government investigations, lost business, and reputational harm. Yet despite recognizing these risks at the highest levels of corporate governance and warning investors of the consequences, Insurer Defendants failed to take the basic, industry-standard precautions

¹⁵⁷ *Q&A: Applying Cyber Defense Experience to Protect Member Data*, HCSC (Oct. 14, 2021), at <https://www.hcsc.com/newsroom/category/company-news/ciso-interview-cyber-defense-protecting-member-data>.

necessary to prevent the Data Breach—underscoring that the harm suffered by Plaintiffs and Class Members was not only foreseeable, but directly tied to vulnerabilities Insurer Defendants had already identified internally and publicly conceded could have catastrophic consequences if left unaddressed.

VI. Defendants Violated Their Duties to Provide Adequate Data Security.

298. Defendants were in an exclusive position to protect Plaintiffs’ and Class Members’ Private Information from the unauthorized access and exfiltration that resulted from the Data Breach. Plaintiffs and Class Members relied on Defendants to implement reasonable and industry standard data security protections and had no way to audit or influence the integrity of Defendants’ data security practices.

299. Conduent and Insurer Defendants had obligations arising under the FTC Act, HIPAA, industry standards, common law, and their own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

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

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

302. Conduent’s duty to protect Plaintiffs and Class Members from the foreseeable risk of injury that inadequate data protection and unauthorized exposure of their Private Information

would case obligated Conduent to implement reasonable practices to keep Plaintiffs' and Class Members' sensitive Private Information confidential and securely maintained through reasonable, industry-standard and legally-compliant measures including encryption in storage and transit, to use and disclose the data for necessary and authorized purposes only, and to delete it from network systems when no longer necessary for legitimate business purposes. Insurer Defendant had a duty to adequately supervise their vendor Conduent to require and ensure the foregoing data security protocols and procedures were in place for Plaintiffs' and Class Members' Private Information.

303. Conduent's duty to Plaintiffs and Class members further required it to implement processes that would detect a compromise of Private Information in a timely manner, and to act upon data security warnings and alerts in a timely fashion. Insurer Defendants owed Plaintiffs and Class Members the duty to require and ensure such security tools and protocols were implemented and maintained by their vendor Conduent.

304. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their and/or their vendor's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons, especially notorious cybercriminals like SafePay.

305. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including data security consistent with industry standards and requirements, and to ensure that their and all their vendors' computer systems, networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

306. Defendants owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in their own and/or their vendor's possession, including adequately training their employees and vendors who

accessed Private Information within their computer systems on how to adequately protect Private Information.

307. Defendants owed a duty to Plaintiffs and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

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

VII. Defendants Violated HIPAA.

309. To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) included Administrative Simplification provisions that required the U.S. Department of Health and Human Services (“HHS”) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of federal privacy protections for PHI.

310. HIPAA’s standards and security requirements inform the duty of care and industry practices Defendants were and are obligated to follow.

311. Defendants are covered by HIPAA (see 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Specifically, Insurer Defendants are each HIPAA covered entities, and Conduent is a HIPAA business associate.

312. These rules establish national standards for the protection of patient information, including personal health information, defined as “individually identifiable health information”

which either “identifies the individual” or where there is a “reasonable basis to believe the information can be used to identify the individual,” that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

313. HIPAA limits the permissible uses of “protected health information” and prohibits unauthorized disclosures of “protected health information.”¹⁵⁸

314. HIPAA requires that Defendants implement appropriate safeguards for this information.¹⁵⁹

315. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.*, non- encrypted data.¹⁶⁰

1. The HIPAA Privacy Rule

316. HHS published its *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”) in December 2000, which sets national standards for the protection of individually identifiable health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically (“covered entities”).

317. The Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual’s authorization.

¹⁵⁸ 45 C.F.R. § 164.502.

¹⁵⁹ 45 C.F.R. § 164.540(c)(1).

¹⁶⁰ 45 C.F.R. §§ 164.402, 404.

318. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and wellbeing.

319. Under the Privacy Rule, when a covered entity uses a contractor or non-workforce member to perform "business associate" services or activities, the covered entity must include certain protections for the information in a Business Associate Agreement ("BAA"). In the BAA, the covered entity must impose specified written safeguards on the PHI used or disclosed by its business associates. Further, a covered entity may not contractually authorize its business associate to make any use or disclosure of PHI that would violate the Privacy Rule.

320. Under the Privacy Rule, covered entities must provide a notice of its privacy practices, which must describe the ways in which the covered entity may use and disclose PHI, state the covered entity's duties to protect privacy, and provide a notice of privacy practices.

321. Under the Privacy Rule, a covered entity must:

- a. develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.
- b. mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of PHI by its workforce or business associates in violation of its privacy policies and procedures or the Privacy Rule.
- c. maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding

documents containing protected health information before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes.

2. *The HIPAA Security Rule*

322. HHS published a final Security Rule in February 2003, which sets national standards for protecting the confidentiality, integrity, and availability of *electronic* PHI (“ePHI”).

323. Section 13401 of the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), enacted as part of the American Recovery and Reinvestment Act of 2009, provides that the administrative, physical, and technical safeguards of the Security Rule, as well as its policies and procedures and documentation requirements, apply to business associates in the same manner that they apply to covered entities.

324. Before HITECH Act Section 13401, the Security Rule already indirectly applied to business associates because it requires covered entities to enter into BAAs with business associates to ensure the confidentiality, integrity, and availability of PHI.

325. Specifically, under the Security Rule, a covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on its behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

326. The Security Rule requires covered entities and business associates to implement reasonable and appropriate administrative, physical, and technical safeguards for protecting ePHI. Specifically, covered entities and business associates must:

- a. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit.

- b. Protect against reasonably anticipated threats to the security or integrity of the information.
- c. Protect against reasonably anticipated, impermissible uses or disclosures.
- d. Ensure compliance by their workforce.

327. The Security Rule defines “confidentiality” to mean that data or information is not made available or disclosed to unauthorized persons or processes. The confidentiality requirements of the Security Rule support the Privacy Rule's prohibitions against improper uses and disclosures of PHI.

328. The Security Rule also promotes the two objectives of maintaining the integrity and availability of ePHI. Under the Security Rule, “integrity” means that data or information has not been altered or destroyed in an unauthorized manner.

3. The HIPAA Breach Notification Rule

329. HIPAA’s Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification within 60 days of discovering a breach of unsecured PHI.

330. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

331. Defendants must notify each individual affected regarding the nature of the Breach, the PHI compromised, steps the individual should take to protect against potential resulting harm, what Defendants are doing to investigate the Breach, mitigate harm, and protect against future breaches, and contact information for the covered entity or applicable business associate. 45 C.F.R. § 164.404(b).

332. Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. Further, business associates must notify covered entities if a breach occurs at or by the business associate.

333. ***Notification by a Business Associate.*** If a breach of unsecured PHI occurs at or by a business associate, like Conduent, the business associate must notify the covered entity following the discovery of the data breach without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

334. ***Individual Notice.*** Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI.

335. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.

336. These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.

337. The individual notifications must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a description of what

the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, and contact information for the covered entity (or business associate as applicable).

338. Even when a breach is at or by a business associate, like Conduent, covered entities, like Insurer Defendants, are ultimately responsible for ensuring individuals are notified.

339. **Media Notice.** Covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the state or jurisdiction.

340. Like individual notice, this media notification must be provided without unreasonable delay, and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

341. **Notice to the Secretary.** In addition to notifying affected individuals and the media, covered entities must notify the Secretary of breaches of unsecured PHI. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach.

342. Despite this requirement, Defendants failed to report the Data Breach to the Secretary until October 8, 2025, almost nine months after learning of the Data Breach.

* * *

343. As alleged herein, Defendants' violations of HIPAA and HITECH include, but are not limited to:

- a. Failing to maintain adequate security practices, systems, and protocols to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and protection of PHI;

- d. Failing to implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights;
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;
- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity;
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of ePHI;
- i. Failing to protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted under the privacy rules regarding individually identifiable health information;
- j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce;
- k. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons;
- l. Failing to require or ensure that Conduent used appropriate safeguards to prevent the unauthorized disclosure of Plaintiffs' and Class Members' Private Information, and
- m. Failing to provide the required Data Breach notice within 60 days of discovering the Data Breach.

344. While monetary relief may compensate Plaintiffs and Class Members for some of their injuries, injunctive relief is also necessary to ensure Defendants' approach to information security is adequate and appropriate going forward. Defendants still maintain the Private Information of their current and former patients, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent theft and misuse.

VIII. Defendants Failed to Comply with FTC Guidelines.

345. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.¹⁶¹

346. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act, 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015).

347. In 2016, the FTC updated its publication titled *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines recommend as follows:

- a. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

¹⁶¹ *See Start with Security: A Guide for Business*, FEDERAL TRADE COMMISSION, at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> (last visited March 14, 2026).

- b. Businesses should encrypt sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- c. Businesses should thoroughly understand the types of vulnerabilities on their network and how to address those vulnerabilities;
- d. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and
- e. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.¹⁶²

348. The FTC further instructs that companies should not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.¹⁶³

349. The FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act.

350. Indeed, 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

351. These FTC enforcement actions include actions against healthcare entities that fail to adequately protect individuals' data, like Defendants. *See, e.g., In the Matter of LabMD, Inc., a*

¹⁶² *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), at <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

¹⁶³ *See Start with Security: A Guide for Business*, FEDERAL TRADE COMMISSION (June 2015), <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

352. As evidenced by the Data Breach, Conduent failed to properly implement one or more of the basic data security practices recommended by the FTC. Conduent’s failure to employ reasonable and appropriate data security measures to protect against unauthorized access to individuals’ Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

353. Insurer Defendants also failed to properly implement the foregoing recommended data security practices and ensure the same from their vendor Conduent. As such, Insurer Defendants failed to follow the FTC’s recommendation that companies verify that third-party service providers have implemented reasonable security measures.

IX. Defendants Failed to Comply with Industry Standards.

354. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

355. The Center for Internet Security’s (“CIS”) Critical Security Controls (“CSC”) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security

Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

356. The U.S. Government’s National Institute of Standards and Technology (“NIST”) provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.

357. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.

358. NIST recommends certain practices to safeguard systems, such as the following:

- a. Control who logs on to your network and uses your computers and other devices.
- b. Use security software to protect data.
- c. Encrypt sensitive data, at rest and in transit.
- d. Conduct regular backups of data.
- e. Update security software regularly, automating those updates if possible.
- f. Have formal policies for safely disposing of electronic files and old devices.
- g. Train everyone who uses your computers, devices, and network about cybersecurity.

359. Further still, CISA makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that “remote access to the organization’s network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing

updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization’s IT personnel have disabled all ports and protocols that are not essential for business purposes,” and other steps; (b) taking steps to quickly detect a potential intrusion, including “[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization’s entire network is protected by antivirus/antimalware software and that signatures in these tools are updated,” and (c) “[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs,” and other steps.¹⁶⁴

360. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, or to require the same from their vendor, including failing to meet or require the minimum standards of the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs’ and Class Members’ Private Information, resulting in the Data Breach.

361. These foregoing frameworks are existing and applicable industry standards for a business and healthcare provider’s obligations to provide adequate data security for its patients’ sensitive information. Defendants failed to comply with at least one, or all, of these accepted standards, thereby opening the door to SafePay criminals to carry out the Data Breach.

¹⁶⁴ *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/shields-guidance-organizations> (last visited Nov. 10, 2025).

362. Further, proper vetting and routine audits of vendors' data security practices, including vetting of Conduent's cybersecurity practices, could have prevented the Data Breach. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."¹⁶⁵

363. Finally, several best practices have been identified that a minimum should be implemented by businesses in possession of Private Information, like Defendants, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Upon information and belief, Defendants failed to follow these industry best practices, including a failure to implement encryption, strong passwords, and multi-factor authentication, and as to Insurer Defendants, failing to ensure these security measures by their vendor Conduent.

X. Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' Private Information.

364. Despite Defendants' knowledge of the continued risks to Plaintiffs' and Class Members' Private Information, Defendants failed to use reasonable security procedures and practices appropriate to the nature of the Private Information they maintained, used, shared, and stored. Had Defendants implemented industry-standard security measures and adequately invested in data security, unauthorized cybercriminals would not have been able to access Conduent's systems and the Data Breach would have been prevented, or at the very least, much smaller in scope.

¹⁶⁵ Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UPGUARD (Sept. 4, 2023), at <https://www.upguard.com/blog/how-to-identifyvulnerable-third-party-software>.

365. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to require and ensure Conduent properly maintained and safeguarded its computer systems, servers, and data containing Plaintiffs' and Class Members' Private Information.

366. Conduent's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain adequate data security systems that would reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect its clients' customers' Private Information from foreseeable risk;
- c. Failing to encrypt or sanitize files and data containing Private Information;
- d. Failing to properly monitor its data security systems for existing intrusions;
- e. Failing to sufficiently train its employees regarding credential protection and the proper handling of Private Information;
- f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTC Act;
- g. Violating HIPAA data security requirements for PHI;
- h. Failing to adhere to industry standards for cybersecurity as discussed above;
and
- i. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

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

- a. Failing to require and periodically ensure that Conduent adopted, implemented, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Private Information, including through data encryption and employee training;
- b. Failing to adequately monitor the security of Conduent's information technology networks and systems;
- c. Failure to require and periodically ensure that Conduent's network systems had reasonable logging and alerting methods in place to detect unauthorized access;
- d. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information provided to their vendor Conduent;
- e. Failing to fully comply with FTC guidelines for cybersecurity, or ensure Conduent's compliance with same, in violation of the FTC Act;
- f. Violating, and allowing Conduent to violate, HIPAA data security requirements for PHI;
- g. Failing to require and ensure Conduent adhered to industry standards for cybersecurity as discussed above; and
- h. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

368. Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cybercriminals to access Conduent's computer systems that contained unsecured and unencrypted Private Information.

369. Had Defendants remedied the deficiencies in their or their vendor's information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they would have prevented, or at least curtailed, intrusion into Conduent's information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information in the Data Breach.

XI. Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft.

370. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers, like Plaintiffs and Class Members, suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.¹⁶⁶ Exposure of highly sensitive Private Information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

371. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

372. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a

¹⁶⁶ *FTC Information Injury Workshop, BE and BCP Staff Perspective*, FTC (Oct. 2018), at https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcpstaff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

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

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

374. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.¹⁶⁷ With Fullz packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data

¹⁶⁷ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)

available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

375. The development of Fullz packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

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

378. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the

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

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

380. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."¹⁶⁸ The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry.

381. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200. Experian reports a stolen card number can sell for \$5 to \$110 on the dark web and that the Fullz sold for \$30 in 2017.

¹⁶⁸ See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), at <https://www.justice.gov/opa/speech/attorney-general-william-p-barrannounces-indictment-four-members-china-s-military> (last visited Nov. 10, 2025).

382. PHI is especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.¹⁶⁹

383. A robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

384. PHI can sell for as much as \$363 on the black market per stolen record, according to the Infosec Institute.

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

386. In short, PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

387. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Defendants collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and share it with third parties for similar purposes.

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

¹⁶⁹ *What to know about identity theft*, FTC (Sept. 2024), at <https://consumer.ftc.gov/articles/what-know-about-identity-theft>.

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

390. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."¹⁷⁰

391. Social Security numbers are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases."¹⁷¹ "Because many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."¹⁷²

¹⁷⁰ Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), <https://kffhealthnews.org/news/rise-of-identity-theft/>.

¹⁷¹ *Avoid Identity Theft: Protect Social Security Numbers*, SOCIAL SECURITY ADMINISTRATION, at <https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases> (last visited March 14, 2026).

¹⁷² *Id.*

392. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

Scammers use your Social Security number (SSN) to get other Private Information about you. They can use your SSN and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your SSN until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.^[173]

393. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

394. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."¹⁷⁴

395. The ramifications of Defendants' failure to keep its customers' patients' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when personal information is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches,

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

¹⁷³ *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 6, 2025).

¹⁷⁴ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>.

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.^[175]

XII. Plaintiffs and Class Members Suffered Damages.

396. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and members of the Class must immediately devote time, energy, and money to: (a) closely monitor their bills, records, and credit and financial accounts; (b) change login and password information on any sensitive account even more frequently than they already do; (c) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (d) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

397. Crucially, Plaintiffs' and Class Members' Private Information has already been misused: SafePay cybercriminals targeted the data on Conduent's systems, stole it, and held it for ransom, threatening to publish it on the dark web if Conduent did not pay.

398. Once Private Information is exposed to criminal organizations like SafePay, there is virtually no way to recover the data or prevent future misuse. This is especially true here, where the information stolen during the Data Breach has been stolen in a targeted attack and held for ransom. As a result, Plaintiffs and Class Members must maintain heightened vigilance indefinitely. Further, Plaintiffs and Class Members have not been compensated for the unconsented and unauthorized disclosure of their Private Information, for which there is a robust market.

399. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer economic and other concrete harms, including but not limited to:

¹⁷⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), at <https://www.gao.gov/assets/270/262904.html>.

- a. Unauthorized disclosure of their confidential information;
- b. Misuse of their Private Information;
- c. Loss of the control of their Private Information;
- d. Loss of the benefit of their bargain in choosing organizations promising data protection;
- e. Identity theft, fraud, and misuse of financial information;
- f. Out-of-pocket expenses for credit monitoring, mitigation efforts, and fraud prevention tools;
- g. Unauthorized charges and restricted access to financial accounts;
- h. Emotional distress, anxiety, and loss of privacy;
- i. Time and productivity lost dealing with the consequences of the Breach;
- j. Damage to credit scores, including from fraudulent inquiries; and
- k. Continued and imminent risk of future fraud and identity theft due to their data being in the hands of unauthorized third parties.

400. Individuals suffer harm each time their personal data is compromised and circulated on underground markets—even if they have been affected by prior breaches. The dark web contains vast, fragmented repositories of stolen information that can be aggregated by different criminals for varied forms of fraud. Each subsequent breach increases the likelihood that a victim's sensitive data will be accessed by more actors and exploited in new and damaging ways.

401. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes.

402. Plaintiffs and Class Members place significant value on data security and consider a company's ability to protect personal information a key factor in their purchasing decisions. Many consumers are willing to pay more for services from organizations that demonstrate strong cybersecurity practices. Conversely, consumers are far less likely to share personal data with companies that have suffered a data breach—reflecting the reputational damage and business consequences that flow from failing to safeguard sensitive information (which is a fact Conduent capitalizes on in their advertising).

403. Because of the premium consumers place on data privacy, companies including companies in the healthcare sector with robust security practices are viewed more favorably and can command higher prices than those that do not. Had Conduent's clients and clients' customers including Plaintiffs known the truth about its lack of cybersecurity—or that it entrusted their sensitive data to an entity with inadequate security practices—they would not have enrolled in Conduent's clients' plans and services; paid less; complained to their brokers, employers or plan sponsors; or otherwise sought alternative arrangements for services. As a result, Plaintiffs and Class Members were deprived of the benefit of their bargain, having paid for secure and responsible handling of their Private Information but receiving substantially less in return.

404. By collecting and storing Plaintiffs' and Class Members' sensitive information, Defendants undertook a duty to safeguard it and avoid increasing the risk of identity theft or fraud. Because Defendants failed to uphold that duty, Plaintiffs seek the present value of identity protection services and other compensatory measures to address the current and future harm stemming from the Data Breach. Plaintiffs and Class Members are entitled to damages in the amount of the present value of ongoing, long-term identity protection and credit monitoring

services, to attempt to return Plaintiffs and Class Members to the status quo in existence before Defendants' Data Breach foisted that ongoing risk of fraud and identity theft upon them.

405. Additionally, Plaintiffs and Class Members are entitled to recover the reasonable use value of their Private Information that was accessed and exfiltrated without authorization. This form of compensation mirrors damages awarded in intellectual property cases for unauthorized use of intangible assets. As with a patent or trade secret, Private Information is non-rivalrous: their unauthorized use by a third party does not eliminate the owner's ability to use them but still justifies compensation based on market value. Thus, Plaintiffs and Class Members were damaged in an amount equaling the value of access to their Private Information, akin to a royalty or license fee.

406. Defendants delayed and then issued incomplete notice of the Data Breach, which caused additional harm to Plaintiffs and Class Members. The communication failed to disclose critical information, including the scope of the Breach, the nature of the information stolen, the number of individuals affected, and the identity of the threat actors. Instead, Defendants issued vague and unsupported reassurances, claiming it was "unaware of any attempted or actual misuse of any information involved in this incident"—despite the fact that the stolen data was obtained by a well-known ransomware gang and the Conduent Breach was advertised on the ransomware gang's website. Many victims have likely still not received formal notice. This lack of transparency has deprived victims of the ability to take timely, informed, and proactive measures to mitigate harm caused by the Data Breach.

407. Upon information and belief, Defendants continue to retain the Private Information of Plaintiffs and all Class Members. As long as Defendants maintain possession of this information, Plaintiffs and Class Members have a strong and ongoing interest in ensuring that adequate safeguards are in place to prevent further unauthorized access or disclosure.

XIII. Plaintiffs' Experiences

AIGPS Plaintiffs

A. Plaintiff Russell Dejulio

408. Plaintiff Russell Dejulio is a former employee of AIG who provided Conduent with his Private Information.

409. As a condition of obtaining services from Defendants, Plaintiff Dejulio was required to provide Conduent, either directly or indirectly through AIG, his Private Information.

410. Conduent was in possession of Plaintiff Dejulio's Private Information before and during the Data Breach and continues to possess Plaintiff Dejulio's Private Information to the present.

411. At the time of the Data Breach, Conduent retained Plaintiff Dejulio's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Dejulio's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

412. On or around October 24, 2025, Plaintiff Dejulio received Notice that his Private Information, including his name and Social Security number, and address, were compromised as a result of the Data Breach.

413. Plaintiff Dejulio reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Dejulio would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

414. Plaintiff Dejulio greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Dejulio is very

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

415. Plaintiff DeJulio stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff DeJulio diligently chooses unique usernames and passwords for his various online accounts.

416. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff DeJulio has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

417. Following the Data Breach, Plaintiff DeJulio has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

418. Following the Data Breach, Plaintiff DeJulio experienced attempted fraud, evidencing misuse of his Private Information. Plaintiff DeJulio received a call from an individual purporting to be a representative of the United States Social Security Administration, who possessed Private Information belonging to Plaintiff DeJulio.

419. As a result of the Data Breach, Plaintiff DeJulio has spent 20 hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff DeJulio would have spent on other activities, including but not limited to work and/or recreation.

420. The Data Breach has caused Plaintiff DeJulio to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been

compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff DeJulio fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

421. As a result of the Data Breach, Plaintiff DeJulio faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

422. Plaintiff DeJulio anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

423. Plaintiff DeJulio's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff DeJulio to the imminent prospect of additional harm. Thus, Plaintiff DeJulio has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

B. Plaintiff Alvin Luckett

424. Plaintiff Alvin Luckett is a current policyholder of AIG who provided Conduent with Plaintiff Luckett's Private Information.

425. As a condition of obtaining services from Defendants, Plaintiff Luckett was required to provide Conduent, either directly or indirectly through AIG, his Private Information.

426. Conduent was in possession of Plaintiff Luckett's Private Information before and during the Data Breach and continues to possess Plaintiff Luckett's Private Information to the present.

427. At the time of the Data Breach, Conduent retained Plaintiff Luckett's Private Information on its network with inadequate data security and in unencrypted form, causing

Plaintiff Luckett's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

428. On or around November 11, 2025, Plaintiff Luckett received Notice that his Private Information, including his name and Social Security number, were compromised as a result of the Data Breach.

429. Plaintiff Luckett reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Luckett would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

430. Plaintiff Luckett greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Luckett is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

431. Plaintiff Luckett stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Luckett diligently chooses unique usernames and passwords for his various online accounts.

432. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Luckett has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

433. Following the Data Breach, Plaintiff Lockett has received alerts that his Private Information was published on the dark web.

434. Following the Data Breach, Plaintiff Lockett has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

435. Following the Data Breach, Plaintiff Lockett experienced actual fraud when unauthorized charges were made on his credit card, evidencing misuse of his Private Information.

436. As a result of the Data Breach, Plaintiff Lockett has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Lockett would have spent on other activities, including but not limited to work and/or recreation.

437. The Data Breach has caused Plaintiff Lockett to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Lockett fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

438. As a result of the Data Breach, Plaintiff Lockett faces a lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

439. Plaintiff Lockett anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

440. Plaintiff Luckett's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Luckett to the imminent prospect of additional harm. Thus, Plaintiff Luckett has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

Cigna Plaintiff

C. Plaintiff Karina Lopez

441. Plaintiff Karina Lopez is a current policyholder of Cigna, who provided Conduent with Plaintiff Lopez's Private Information.

442. As a condition of obtaining services from Defendants, Plaintiff Lopez was required to provide Conduent, either directly or indirectly through Cigna, her Private Information.

443. Conduent was in possession of Plaintiff Lopez's Private Information before and during the Data Breach and continues to possess Plaintiff Lopez's Private Information to the present.

444. At the time of the Data Breach, Conduent retained Plaintiff Lopez's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Lopez's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

445. On or around November 25, 2025, Plaintiff Lopez received Notice that her Private Information, including name, health care ID, date of service, treatment cost, and claims numbers were compromised as a result of the Data Breach.

446. Plaintiff Lopez reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Lopez would not have allowed Defendants, or anyone in Defendants' position, to

maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

447. Plaintiff Lopez greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Lopez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

448. Plaintiff Lopez stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Lopez diligently chooses unique usernames and passwords for her various online accounts.

449. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Lopez has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

450. Following the Data Breach, Plaintiff Lopez has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

451. As a result of the Data Breach, Plaintiff Lopez has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Lopez would have spent on other activities, including but not limited to work and/or recreation.

452. The Data Breach has caused Plaintiff Lopez to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was

acquired by criminals as a result of the Data Breach. Plaintiff Lopez fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

453. As a result of the Data Breach, Plaintiff Lopez faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

454. Plaintiff Lopez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

455. Plaintiff Lopez's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Lopez to the imminent prospect of additional harm. Thus, Plaintiff Lopez has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

Elevance Plaintiffs

D. Plaintiff Rashell Chambers

456. Plaintiff Rashell Chambers is a former policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Chambers's Private Information.

457. As a condition of obtaining services from Defendants, Plaintiff Chambers was required to provide Conduent, either directly or indirectly through Elevance, her Private Information.

458. Conduent was in possession of Plaintiff Chambers's Private Information before and during the Data Breach and continues to possess Plaintiff Chambers's Private Information to the present.

459. At the time of the Data Breach, Conduent retained Plaintiff Chambers's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Chambers's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

460. In or around January 2026, Plaintiff Chambers received Notice that her Private Information, including her name, address, and Social Security number, were compromised as a result of the Data Breach.

461. Plaintiff Chambers reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Chambers would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

462. Plaintiff Chambers greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Chambers is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

463. Plaintiff Chambers stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity.

Moreover, Plaintiff Chambers diligently chooses unique usernames and passwords for her various online accounts.

464. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Chambers has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

465. Plaintiff Chambers's Private Information compromised in the Data Breach has already been misused, evidenced by multiple notifications she has received following the Data Breach alerting that her Private Information has been found published on the dark web.

466. Following the Data Breach, Plaintiff Chambers has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

467. As a result of the Data Breach, Plaintiff Chambers has spent several researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords online, and remediating the fraud perpetrated against her. This is valuable time that Plaintiff Chambers would have spent on other activities, including but not limited to work and/or recreation.

468. The Data Breach has caused Plaintiff Chambers to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Chambers fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information.

469. As a result of the Data Breach, Plaintiff Chambers faces a present and continuing lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

470. Plaintiff Chambers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

471. Plaintiff Chambers's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Chambers to the imminent prospect of additional harm. Thus, Plaintiff Chambers has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

E. Plaintiff Suzan Kirkland

472. Plaintiff Suzan Kirkland is a current policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Kirkland's Private Information.

473. As a condition of obtaining services from Defendants, Plaintiff Kirkland was required to provide Conduent, either directly or indirectly through Elevance, her Private Information.

474. Conduent was in possession of Plaintiff Kirkland's Private Information before and during the Data Breach and continues to possess Plaintiff Kirkland's Private Information to the present.

475. At the time of the Data Breach, Conduent retained Plaintiff Kirkland's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Kirkland's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

476. On or around February 26, 2026, Plaintiff Kirkland received Notice that her Private Information, including name, address, Social Security number, health insurance information, and date of birth, were compromised as a result of the Data Breach.

477. Plaintiff Kirkland reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Kirkland would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

478. Plaintiff Kirkland greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Kirkland is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

479. Plaintiff Kirkland stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Kirkland diligently chooses unique usernames and passwords for her various online accounts.

480. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Kirkland has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

481. Following the Data Breach, Plaintiff Kirkland has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

482. As a result of the Data Breach, Plaintiff Kirkland has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Kirkland would have spent on other activities, including but not limited to work and/or recreation.

483. The Data Breach has caused Plaintiff Kirkland to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Kirkland fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

484. As a result of the Data Breach, Plaintiff Kirkland faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

485. Plaintiff Kirkland anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

486. Plaintiff Kirkland's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Kirkland to the imminent prospect of additional harm. Thus, Plaintiff Kirkland has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

F. Plaintiff Marc Powell

487. Plaintiff Marc Powell is a former policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Powell's Private Information.

488. As a condition of obtaining services from Defendants, Plaintiff Powell was required to provide Conduent, either directly or indirectly through Elevance, his Private Information.

489. Conduent was in possession of Plaintiff Powell's Private Information before and during the Data Breach and continues to possess Plaintiff Powell's Private Information to the present.

490. At the time of the Data Breach, Conduent retained Plaintiff Powell's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Powell's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

491. On or around December 31, 2025, Plaintiff Powell received Notice that his Private Information, including his name, address, and Social Security number were compromised as a result of the Data Breach.

492. Plaintiff Powell reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Powell would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

493. Plaintiff Powell greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Powell is very

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

494. Plaintiff Powell stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Powell diligently chooses unique usernames and passwords for his various online accounts.

495. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Powell has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

496. Following the Data Breach, Plaintiff Powell has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

497. As a result of the Data Breach, Plaintiff Powell has spent several researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Powell would have spent on other activities, including but not limited to work and/or recreation.

498. The Data Breach has caused Plaintiff Powell to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Powell fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

499. As a result of the Data Breach, Plaintiff Powell faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

500. Plaintiff Powell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

501. Plaintiff Powell's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Powell to the imminent prospect of additional harm. Thus, Plaintiff Powell has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

G. Plaintiff Lakrishna Long

502. Plaintiff Lakrishna Long is a current policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Long's Private Information.

503. As a condition of obtaining services from Defendants, Plaintiff Long was required to provide Conduent, either directly or indirectly through Elevance, her Private Information.

504. Conduent was in possession of Plaintiff Long's Private Information before and during the Data Breach and continues to possess Plaintiff Long's Private Information to the present.

505. At the time of the Data Breach, Conduent retained Plaintiff Long's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Long's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

506. On or around December 31, 2025, Plaintiff Long received Notice that her Private Information was compromised as a result of the Data Breach.

507. Plaintiff Long reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Long would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

508. Plaintiff Long greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Long is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

509. Plaintiff Long stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Long diligently chooses unique usernames and passwords for her various online accounts.

510. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Long has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

511. Following the Data Breach, Plaintiff Long has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

512. As a result of the Data Breach, Plaintiff Long has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Long would have spent on other activities, including but not limited to work and/or recreation.

513. The Data Breach has caused Plaintiff Long to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Long fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

514. As a result of the Data Breach, Plaintiff Long faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

515. Plaintiff Long anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

516. Plaintiff Long's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Long to the imminent prospect of additional harm. Thus, Plaintiff Long has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

H. Plaintiff Anthony Meyer

517. Plaintiff Anthony Meyer is a former policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Meyer's Private Information.

518. As a condition of obtaining services from Defendants, Plaintiff Meyer was required to provide Conduent, either directly or indirectly through Elevance, his Private Information.

519. Conduent was in possession of Plaintiff Meyer's Private Information before and during the Data Breach and continues to possess Plaintiff Meyer's Private Information to the present.

520. At the time of the Data Breach, Conduent retained Plaintiff Meyer's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Meyer's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

521. On or around February 10, 2026, Plaintiff Meyer received Notice dated December 31, 2025 that his Private Information, including his name, address, and Social Security number were compromised as a result of the Data Breach.

522. Plaintiff Meyer reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Meyer would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

523. Plaintiff Meyer greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Meyer is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

524. Plaintiff Meyer stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may Meyer any information that could otherwise be used to compromise his identity.

Moreover, Plaintiff Meyer diligently chooses unique usernames and passwords for his various online accounts.

525. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Meyer has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

526. Following the Data Breach, Plaintiff Meyer has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

527. As a result of the Data Breach, Plaintiff Meyer has spent several researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Meyer would have spent on other activities, including but not limited to work and/or recreation.

528. The Data Breach has caused Plaintiff Meyer to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Meyer fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

529. As a result of the Data Breach, Plaintiff Meyer faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

530. Plaintiff Meyer anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

531. Plaintiff Meyer's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Meyer to the imminent prospect of additional harm. Thus, Plaintiff Meyer has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

I. Plaintiff Richard Helm Jr.

532. Plaintiff Richard Helm Jr. is a former policyholder of an Anthem Blue Cross Blue Shield plan provided by Elevance, who provided Conduent with Plaintiff Helm's Private Information.

533. As a condition of obtaining services from Defendants, Plaintiff Helm was required to provide Conduent, either directly or indirectly through Elevance, his Private Information.

534. Conduent was in possession of Plaintiff Helm's Private Information before and during the Data Breach and continues to possess Plaintiff Helm's Private Information to the present.

535. At the time of the Data Breach, Conduent retained Plaintiff Helm's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Helm's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

536. On or around December 31, 2025, Plaintiff Helm received Notice that his Private Information, including his name, address, and Social Security number were compromised as a result of the Data Breach.

537. Plaintiff Helm reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Helm would not have allowed Defendants, or anyone in Defendants' position, to

maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

538. Plaintiff Helm greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Helm is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

539. Plaintiff Helm stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Helm diligently chooses unique usernames and passwords for his various online accounts.

540. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Helm has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

541. Following the Data Breach, Plaintiff Helm has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

542. As a result of the Data Breach, Plaintiff Helm has spent several researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Helm would have spent on other activities, including but not limited to work and/or recreation.

543. The Data Breach has caused Plaintiff Helm to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been

compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Helm fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

544. As a result of the Data Breach, Plaintiff Helm faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

545. Plaintiff Helm anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

546. Plaintiff Helm's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Helm to the imminent prospect of additional harm. Thus, Plaintiff Helm has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

HCSC Plaintiffs

J. Plaintiff James Hurd

547. Plaintiff James Hurd is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Hurd's Private Information.

548. As a condition of obtaining services from Defendants, Plaintiff Hurd was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

549. Conduent was in possession of Plaintiff Hurd's Private Information before and during the Data Breach and continues to possess Plaintiff Hurd's Private Information to the present.

550. At the time of the Data Breach, Conduent retained Plaintiff Hurd's Private Information on its network with inadequate data security and in unencrypted form, causing

Plaintiff Hurd's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

551. On or around November 4, 2025, Plaintiff Hurd received Notice that his Private Information, including his name, address, date of birth, and Social Security Number, was compromised as a result of the Data Breach.

552. Plaintiff Hurd reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Hurd would not have allowed Defendants, or anyone in Defendants' position, to his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

553. Plaintiff Hurd greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Hurd is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

554. Plaintiff Hurd stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Hurd diligently chooses unique usernames and passwords for his various online accounts.

555. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Hurd has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

556. Following the Data Breach, Plaintiff Hurd received alerts that his Private Information was published on the dark web.

557. Following the Data Breach, Plaintiff Hurd has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

558. Following the Data Breach, Plaintiff Hurd experienced actual and attempted fraud, evidencing misuse of his Private Information. On several instances, Plaintiff Hurd received email correspondence from financial institutions informing him that an attempt to take out a loan under his name was made. Moreover, after the Data Breach Plaintiff Hurd experienced several unauthorized charges on his credit accounts.

559. As a result of the Data Breach, Plaintiff Hurd has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords and performing other necessary mitigation efforts. This is valuable time that Plaintiff Hurd would have spent on other activities, including but not limited to work and/or recreation.

560. The Data Breach has caused Plaintiff Hurd to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Hurd fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

561. As a result of the Data Breach, Plaintiff Hurd faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

562. Plaintiff Hurd anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

563. Plaintiff Hurd's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Hurd to the imminent prospect of additional harm. Thus, Plaintiff Hurd has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

K. Plaintiff Nathan Cornwell

564. Plaintiff Nathan Cornwell is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Cornwell's Private Information.

565. As a condition of obtaining services from Defendants, Plaintiff Cornwell was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

566. Conduent was in possession of Plaintiff Cornwell's Private Information before and during the Data Breach and continues to possess Plaintiff Cornwell's Private Information to the present.

567. At the time of the Data Breach, Conduent retained Plaintiff Cornwell's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Cornwell's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

568. In November of 2025, Plaintiff Cornwell received Notice that his Private Information was compromised as a result of the Data Breach.

569. Plaintiff Cornwell reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Cornwell would not have allowed Defendants, or anyone in Defendants' position,

to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

570. Plaintiff Cornwell greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Cornwell is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

571. Plaintiff Cornwell stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Cornwell diligently chooses unique usernames and passwords for his various online accounts.

572. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Cornwell has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

573. Following the Data Breach, Plaintiff Cornwell received alerts that his Private Information was published on the dark web.

574. Following the Data Breach, Plaintiff Cornwell has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

575. As a result of the Data Breach, Plaintiff Cornwell has spent numerous hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, and screening spam messages, emails, and calls. This is valuable time that Plaintiff Cornwell would have spent on other activities, including but not limited to work and/or recreation.

576. The Data Breach has caused Plaintiff Cornwell to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Cornwell fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

577. As a result of the Data Breach, Plaintiff Cornwell faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

578. Plaintiff Cornwell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

579. Plaintiff Cornwell's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff to the imminent prospect of additional harm. Thus, Plaintiff Cornwell has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

L. Plaintiff Jason Frost

580. Plaintiff Jason Frost is a former policyholder of BCBSIL, who provided Conduent with his Private Information.

581. As a condition of obtaining services from Defendants, Plaintiff Frost was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

582. Conduent was in possession of Plaintiff Frost's Private Information before and during the Data Breach and continues to possess Plaintiff Frost's Private Information to the present.

583. At the time of the Data Breach, Conduent retained Plaintiff Frost's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Frost's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

584. On or around October 24, 2025, Plaintiff Frost received Notice that his Private Information, including his name, Social Security number, and address, were compromised as a result of the Data Breach.

585. Plaintiff Frost reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Frost would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

586. Plaintiff Frost greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Frost is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

587. Plaintiff Frost stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Frost diligently chooses unique usernames and passwords for his various online accounts.

588. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Frost has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

589. Following the Data Breach, Plaintiff Frost has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

590. Following the Data Breach, Plaintiff Frost experienced attempted fraud, when he received a call from Capital Lending that someone tried to take out a loan for \$62,000 in his name, evidencing misuse of his Private Information.

591. As a result of the Data Breach, Plaintiff Frost has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Frost would have spent on other activities, including but not limited to work and/or recreation.

592. The Data Breach has caused Plaintiff Frost to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Frost fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

593. As a result of the Data Breach, Plaintiff Frost faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

594. Plaintiff Frost anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

595. Plaintiff Frost's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Frost to the imminent prospect of additional harm. Thus, Plaintiff Frost has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

M. Plaintiff Andrea Rodriguez, on behalf of her minor child, A.R.

596. Plaintiff Andrea Rodriguez's minor child, A.R., is a current policyholder of BCBSTX, who provided Conduent with Plaintiff Rodriguez's minor child's Private Information.

597. As a condition of obtaining services from Defendants, Plaintiff Rodriguez's minor child was required to provide Conduent, either directly or indirectly through BCBSTX, her Private Information.

598. Conduent was in possession of Plaintiff Rodriguez's minor child's Private Information before and during the Data Breach and continues to possess Plaintiff's minor child's Private Information to the present.

599. At the time of the Data Breach, Conduent retained Plaintiff Rodriguez's minor child's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Rodriguez's minor child's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

600. On or around October 24, 2025, Plaintiff Rodriguez's minor child received Notice that her Private Information was compromised as a result of the Data Breach.

601. Plaintiff Rodriguez's minor child reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Rodriguez's minor child would not have allowed Defendants, or

anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

602. Plaintiff Rodriguez's minor child greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Rodriguez's minor child is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

603. Plaintiff Rodriguez's minor child stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Rodriguez's minor child diligently chooses unique usernames and passwords for her various online accounts.

604. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Rodriguez's minor child has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

605. Following the Data Breach, Plaintiff Rodriguez's minor child experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Rodriguez's minor child had multiple unauthorized charges made on her Cash App account. in

606. As a result of the Data Breach, Plaintiff Rodriguez's minor child has spent 10 hours researching the Data Breach, reviewing her financial accounts, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Rodriguez's minor child would have spent on other activities, including but not limited to work and/or recreation.

607. The Data Breach has caused Plaintiff Rodriguez's minor child to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Rodriguez's minor child fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

608. As a result of the Data Breach, Plaintiff Rodriguez's minor child faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

609. Plaintiff Rodriguez's minor child anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

610. Plaintiff Rodriguez's minor child's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Rodriguez's minor child to the imminent prospect of additional harm. Thus, Plaintiff Rodriguez's minor child has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

N. Plaintiff Anita Burton

611. Plaintiff Anita Burton is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Burton's Private Information.

612. As a condition of obtaining services from Defendants, Plaintiff Burton was required to provide Conduent, either directly or indirectly through BCBSIL, her Private Information.

613. Conduent was in possession of Plaintiff Burton's Private Information before and during the Data Breach and continues to possess Plaintiff Burton's Private Information to the present.

614. At the time of the Data Breach, Conduent retained Plaintiff Burton's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Burton's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

615. On or around October 24, 2025, Plaintiff Burton received Notice that her Private Information was compromised as a result of the Data Breach.

616. Plaintiff Burton reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Burton would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

617. Plaintiff Burton greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Burton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

618. Plaintiff Burton stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity.

Moreover, Plaintiff Burton diligently chooses unique usernames and passwords for her various online accounts.

619. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Burton has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

620. Following the Data Breach, Plaintiff Burton received alerts that her Private Information, including was published on the dark web.

621. Following the Data Breach, Plaintiff Burton has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

622. Following the Data Breach, Plaintiff Burton experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Burton had a Wells Fargo bank account opened in her name without her authorization. Moreover, Plaintiff Burton was the victim of fraudulent charges on her bank card.

623. As a result of the Data Breach, Plaintiff Burton has spent 10 hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Burton would have spent on other activities, including but not limited to work and/or recreation.

624. The Data Breach has caused Plaintiff Burton to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Burton fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This

goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

625. As a result of the Data Breach, Plaintiff Burton faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

626. Plaintiff Burton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

627. Plaintiff Burton's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Burton to the imminent prospect of additional harm. Thus, Plaintiff Burton has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

O. Plaintiff Andrea Oliver-Alexander

628. Plaintiff Andrea Oliver-Alexander is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Oliver-Alexander's Private Information.

629. As a condition of obtaining services from Defendants, Plaintiff Oliver-Alexander was required to provide Conduent, either directly or indirectly through BCBSIL, her Private Information.

630. Conduent was in possession of Plaintiff Oliver-Alexander's Private Information before and during the Data Breach and continues to possess Plaintiff Oliver-Alexander's Private Information to the present.

631. At the time of the Data Breach, Conduent retained Plaintiff Oliver-Alexander's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Oliver-Alexander Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

632. On or around October 24, 2025, Plaintiff Oliver-Alexander received Notice that her Private Information, including name, date of birth, address, and Social Security number were compromised as a result of the Data Breach.

633. Plaintiff Oliver-Alexander reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Oliver-Alexander would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

634. Plaintiff Oliver-Alexander greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Oliver-Alexander is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

635. Plaintiff Oliver-Alexander stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Oliver-Alexander diligently chooses unique usernames and passwords for her various online accounts.

636. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Oliver-Alexander has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

637. Following the Data Breach, Plaintiff Oliver-Alexander received alerts that her Private Information was published on the dark web.

638. Following the Data Breach, Plaintiff Oliver-Alexander has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

639. Following the Data Breach, Plaintiff Oliver-Alexander experienced actual fraud, including unauthorized charges on her debit card, evidencing misuse of her Private Information.

640. As a result of the Data Breach, Plaintiff Oliver-Alexander has spent hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Oliver-Alexander would have spent on other activities, including but not limited to work and/or recreation.

641. The Data Breach has caused Plaintiff Oliver-Alexander to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Oliver-Alexander fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

642. As a result of the Data Breach, Plaintiff Oliver-Alexander faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

643. Plaintiff Oliver-Alexander anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

644. Plaintiff Oliver-Alexander's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Oliver-Alexander to the imminent prospect of additional harm. Thus, Plaintiff Oliver-Alexander has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

P. Plaintiff Rachel Zafra

645. Plaintiff Rachel Zafra is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Zafra Private Information.

646. As a condition of obtaining services from Defendants, Plaintiff Zafra was required to provide Conduent, either directly or indirectly through BCBSIL, her Private Information.

647. Conduent was in possession of Plaintiff Zafra's Private Information before and during the Data Breach and continues to possess Plaintiff Zafra's Private Information to the present.

648. At the time of the Data Breach, Conduent retained Plaintiff Zafra's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Zafra Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

649. On or around October 24, 2025, Plaintiff Zafra received Notice that her Private Information, including name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

650. Plaintiff Zafra reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Zafra would not have allowed Defendants, or anyone in Defendants' position, to

maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

651. Plaintiff Zafra greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Zafra is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

652. Plaintiff Zafra stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Zafra diligently chooses unique usernames and passwords for her various online accounts.

653. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Zafra has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

654. Following the Data Breach, Plaintiff Zafra has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

655. Following the Data Breach, Plaintiff Zafra experienced actual fraud, including unauthorized charges made on her bank card and credit card, evidencing misuse of her Private Information.

656. As a result of the Data Breach, Plaintiff Zafra has spent numerous hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Zafra would have spent on other activities, including but not limited to work and/or recreation.

657. The Data Breach has caused Plaintiff Zafra to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Zafra fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

658. As a result of the Data Breach, Plaintiff Zafra faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

659. Plaintiff Zafra anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

660. Plaintiff Zafra sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Zafra to the imminent prospect of additional harm. Thus, Plaintiff Zafra has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

Q. Plaintiff Kerri Cromer

661. Plaintiff Kerri Cromer is a former policyholder of BCBSTX, who provided Conduent with her Private Information.

662. As a condition of obtaining services from Defendants, Plaintiff Cromer was required to provide Conduent, either directly or indirectly through BCBSTX, her Private Information.

663. Conduent was in possession of Plaintiff Cromer's Private Information before and during the Data Breach and continues to possess Plaintiff Cromer's Private Information to the present.

664. At the time of the Data Breach, Conduent retained Plaintiff Cromer's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Cromer's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

665. On or around October 24, 2025, Plaintiff Cromer received Notice that her Private Information, including her name and Social Security number, were compromised as a result of the Data Breach.

666. Plaintiff Cromer reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Cromer would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

667. Plaintiff Cromer greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Cromer is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

668. Plaintiff Cromer stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity.

Moreover, Plaintiff Cromer diligently chooses unique usernames and passwords for her various online accounts.

669. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Cromer has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

670. Following the Data Breach, Plaintiff Cromer has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

671. Following the Data Breach, Plaintiff experienced actual fraud when an unauthorized charge was made on her bank card, evidencing misuse of her Private Information. Her bank later refunded the amount after it determined that the charge was fraudulent.

672. As a result of the Data Breach, Plaintiff Cromer has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Cromer would have spent on other activities, including but not limited to work and/or recreation.

673. The Data Breach has caused Plaintiff Cromer to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Cromer fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

674. As a result of the Data Breach, Plaintiff Cromer faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

675. Plaintiff Cromer anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

676. Plaintiff Cromer's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Cromer to the imminent prospect of additional harm. Thus, Plaintiff Cromer has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

R. Plaintiff Kevin McShane

677. Plaintiff Kevin McShane is a current policyholder of BCBSIL, who provided Conduent with Plaintiff McShane's Private Information.

678. As a condition of obtaining services from Defendants, Plaintiff McShane was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

679. Conduent was in possession of Plaintiff McShane's Private Information before and during the Data Breach and continues to possess Plaintiff's Private Information to the present.

680. At the time of the Data Breach, Conduent retained Plaintiff McShane's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff McShane's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

681. On or around October 24, 2025, Plaintiff McShane received Notice that his Private Information, including his name, date of birth, Social Security number, and address were compromised as a result of the Data Breach.

682. Plaintiff McShane reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff McShane would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

683. Plaintiff McShane greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff McShane is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

684. Plaintiff McShane stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff McShane diligently chooses unique usernames and passwords for his various online accounts.

685. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff McShane has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

686. Following the Data Breach, Plaintiff McShane has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

687. As a result of the Data Breach, Plaintiff McShane has spent approximately 15 hours thus far, researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is

valuable time that Plaintiff McShane would have spent on other activities, including but not limited to work and/or recreation.

688. The Data Breach has caused Plaintiff McShane to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff McShane fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

689. As a result of the Data Breach, Plaintiff McShane faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

690. Plaintiff McShane anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

691. Plaintiff McShane's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff McShane to the imminent prospect of additional harm. Thus, Plaintiff McShane has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

S. Plaintiff Tina Gustin

692. Plaintiff Tina Gustin is a former policyholder of BCBSIL, who provided Conduent with Plaintiff Gustin's Private Information.

693. As a condition of obtaining services from Defendants, Plaintiff Gustin was required to provide Conduent, either directly or indirectly through BCBSIL, her Private Information.

694. Conduent was in possession of Plaintiff Gustin's Private Information before and during the Data Breach and continues to possess Plaintiff Gustin's Private Information to the present.

695. At the time of the Data Breach, Conduent retained Plaintiff Gustin's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Gustin Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

696. On or around October 24, 2025, Plaintiff Gustin received Notice that her Private Information, including name, date of birth, address, and Social Security number were compromised as a result of the Data Breach.

697. Plaintiff Gustin reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Gustin would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

698. Plaintiff Gustin greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Gustin is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

699. Plaintiff Gustin stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity.

Moreover, Plaintiff Gustin diligently chooses unique usernames and passwords for her various online accounts.

700. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Gustin has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

701. Following the Data Breach, Plaintiff Gustin has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

702. Following the Data Breach, Plaintiff Gustin experienced actual fraud, evidencing misuse of her Private Information. On June 5, 2025, an unauthorized individual applied for unemployment benefits under Plaintiff Gustin's name. Moreover, Plaintiff Gustin received alerts from Bank of America indicating someone was attempting to open an account in her name.

703. As a result of the Data Breach, Plaintiff Gustin has spent hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Gustin would have spent on other activities, including but not limited to work and/or recreation.

704. The Data Breach has caused Plaintiff Gustin to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Gustin fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

705. As a result of the Data Breach, Plaintiff Gustin faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

706. Plaintiff Gustin anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

707. Plaintiff Gustin's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Gustin to the imminent prospect of additional harm. Thus, Plaintiff Gustin has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

T. Plaintiff Kevin Amende

708. Plaintiff Kevin Amende is a current policyholder of BCBSMT, who provided Conduent with Plaintiff Amende's Private Information.

709. As a condition of obtaining services from Defendants, Plaintiff Amende was required to provide Conduent, either directly or indirectly through BCBSMT, his Private Information.

710. Conduent was in possession of Plaintiff Amende's Private Information before and during the Data Breach and continues to possess Plaintiff Amende's Private Information to the present.

711. At the time of the Data Breach, Conduent retained Plaintiff Amende's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Amende's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

712. On or around October 24, 2025, Plaintiff Amende received Notice that his Private Information, including his name, date of birth, Social Security number, and address were compromised as a result of the Data Breach.

713. Plaintiff Amende reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Amende would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

714. Plaintiff Amende greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Amende is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

715. Plaintiff Amende stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Amende diligently chooses unique usernames and passwords for his various online accounts.

716. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Amende has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

717. Following the Data Breach, Plaintiff Amende has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

718. Following the Data Breach, Plaintiff Amende experienced actual fraud when an unauthorized third-party made purchases on his Apple account. Moreover, Plaintiff Amende experienced attempted fraud, through phishing calls from individuals attempting to extract sensitive information from Plaintiff Amende.

719. As a result of the Data Breach, Plaintiff Amende has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Amende would have spent on other activities, including but not limited to work and/or recreation.

720. The Data Breach has caused Plaintiff Amende to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Amende fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

721. As a result of the Data Breach, Plaintiff Amende faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

722. Plaintiff Amende anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

723. Plaintiff Amende's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff

Amende to the imminent prospect of additional harm. Thus, Plaintiff Amende has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

U. Plaintiff Amanda Dunn

724. Plaintiff Amanda Dunn is a current policyholder of BCBSMT, who provided Conduent with Plaintiff Dunn's Private Information.

725. As a condition of obtaining services from Defendants, Plaintiff Dunn was required to provide Conduent, either directly or indirectly through BCBSMT, her Private Information.

726. Conduent was in possession of Plaintiff Dunn's Private Information before and during the Data Breach and continues to possess Plaintiff Dunn's Private Information to the present.

727. At the time of the Data Breach, Conduent retained Plaintiff Dunn's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Dunn's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

728. On or around October 24, 2025, Plaintiff Dunn received Notice that her Private Information, including name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

729. Plaintiff Dunn reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Dunn would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

730. Plaintiff Dunn greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Dunn is very

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

731. Plaintiff Dunn stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Dunn diligently chooses unique usernames and passwords for her various online accounts.

732. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Dunn has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

733. Following the Data Breach, Plaintiff Dunn has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

734. Following the Data Breach, Plaintiff Dunn experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Dunn had unauthorized charges made on her credit card and debit card.

735. As a result of the Data Breach, Plaintiff Dunn has spent 10 hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Dunn would have spent on other activities, including but not limited to work and/or recreation.

736. The Data Breach has caused Plaintiff Dunn to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Dunn fears for her personal financial

security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

737. As a result of the Data Breach, Plaintiff Dunn faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

738. Plaintiff Dunn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

739. Plaintiff Dunn's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Dunn to the imminent prospect of additional harm. Thus, Plaintiff Dunn has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

V. Plaintiff Brian Marshall

740. Plaintiff Brian Marshall is a current policyholder of BCBSIL, who provided Conduent with his Private Information.

741. As a condition of obtaining services from Defendants, Plaintiff Marshall was required to provide Conduent, either directly or indirectly through BCBIL, his Private Information.

742. Conduent was in possession of Plaintiff Marshall's Private Information before and during the Data Breach and continues to possess Plaintiff Marshall's Private Information to the present.

743. At the time of the Data Breach, Conduent retained Plaintiff Marshall's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

744. On or around October 24, 2025, Plaintiff Marshall received Notice that his Private Information, including his name, date of birth, Social Security number, and address were compromised as a result of the Data Breach.

745. Plaintiff Marshall reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Marshall would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

746. Plaintiff Marshall greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Marshall is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

747. Plaintiff Marshall stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Marshall diligently chooses unique usernames and passwords for his various online accounts.

748. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Marshall has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

749. Following the Data Breach, Plaintiff Marshall received alerts that his Private Information was published on the dark web.

750. Following the Data Breach, Plaintiff Marshall has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

751. As a result of the Data Breach, Plaintiff Marshall has spent time researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Marshall would have spent on other activities, including but not limited to work and/or recreation.

752. The Data Breach has caused Plaintiff Marshall to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Marshall fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

753. As a result of the Data Breach, Plaintiff Marshall faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

754. Plaintiff Marshall anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

755. Plaintiff Marshall's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Marshall to the imminent prospect of additional harm. Thus, Plaintiff Marshall has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

W. Plaintiff Michelle Dupuis-Nilsen

756. Plaintiff Michelle Dupuis-Nilsen is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Dupuis-Nilsen's Private Information.

757. As a condition of obtaining services from Defendants, Plaintiff Dupuis-Nilsen was required to provide Conduent, either directly or indirectly through BCBSIL, her Private Information.

758. Conduent was in possession of Plaintiff Dupuis-Nilsen's Private Information before and during the Data Breach and continues to possess Plaintiff Dupuis-Nilsen's Private Information to the present.

759. At the time of the Data Breach, Conduent retained Plaintiff Dupuis-Nilsen's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Dupuis-Nilsen's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

760. On or around October 24, 2025, Plaintiff Dupuis-Nilsen received Notice that her Private Information was compromised as a result of the Data Breach.

761. Plaintiff Dupuis-Nilsen reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Dupuis-Nilsen would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

762. Plaintiff Dupuis-Nilsen greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Dupuis-

Nilsen is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

763. Plaintiff Dupuis-Nilsen stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Dupuis-Nilsen diligently chooses unique usernames and passwords for her various online accounts.

764. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Dupuis-Nilsen has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

765. Following the Data Breach, Plaintiff Dupuis-Nilsen received alerts that her Private Information, including was published on the dark web.

766. Following the Data Breach, Plaintiff Dupuis-Nilsen has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

767. Following the Data Breach, Plaintiff Dupuis-Nilsen experienced attempted fraud, through a phishing call with an individual purporting to work for Verizon, evidencing misuse of her Private Information.

768. As a result of the Data Breach, Plaintiff Dupuis-Nilsen has spent time researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Dupuis-Nilsen would have spent on other activities, including but not limited to work and/or recreation.

769. The Data Breach has caused Plaintiff Dupuis-Nilsen to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been

compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Dupuis-Nilsen fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

770. As a result of the Data Breach, Plaintiff Dupuis-Nilsen faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

771. Plaintiff Dupuis-Nilsen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

772. Plaintiff Dupuis-Nilsen's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Dupuis-Nilsen to the imminent prospect of additional harm. Thus, Plaintiff Dupuis-Nilsen has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

X. Plaintiff Andrew Cook

773. Plaintiff Andrew Cook is a current policyholder of BCBSIL, who provided Conduent with Plaintiff Cook's Private Information.

774. As a condition of obtaining services from Defendants, Plaintiff Cook was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

775. Conduent was in possession of Plaintiff Cook's Private Information before and during the Data Breach and continues to possess Plaintiff Cook's Private Information to the present.

776. At the time of the Data Breach, Conduent retained Plaintiff Cook's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Cook's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

777. On or around October 24, 2025, Plaintiff Cook received Notice that his Private Information, including his name and Social Security number, were compromised as a result of the Data Breach.

778. Plaintiff Cook reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Cook would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

779. Plaintiff Cook greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Cook is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

780. Plaintiff Cook stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Cook diligently chooses unique usernames and passwords for his various online accounts.

781. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Cook has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

782. Following the Data Breach, Plaintiff Cook has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

783. Following the Data Breach, Plaintiff Cook experienced actual fraud when unauthorized charges were made on his credit card, evidencing misuse of his Private Information.

784. As a result of Data Breach, Plaintiff Cook has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Cook would have spent on other activities, including but not limited to work and/or recreation.

785. The Data Breach has caused Plaintiff Cook to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Cook fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law. Moreover, Plaintiff Cook has experienced added fear, stress, and anxiety, due to the fact his minor children were also impacted by the Data Breach, and he now worries about their Private Information being misused.

786. As a result of the Data Breach, Plaintiff Cook faces a lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

787. Plaintiff Cook anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

788. Plaintiff Cook's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Cook to the imminent prospect of additional harm. Thus, Plaintiff Cook has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

Y. Plaintiff Emily Gresh

789. Plaintiff Emily Gresh is a current policyholder of BCBSOK, who provided Conduent with Plaintiff Gresh's Private Information.

790. As a condition of obtaining services from Defendants, Plaintiff Gresh was required to provide Conduent, either directly or indirectly through BCBSOK, her Private Information.

791. Conduent was in possession of Plaintiff Gresh's Private Information before and during the Data Breach and continues to possess Plaintiff Gresh's Private Information to the present.

792. At the time of the Data Breach, Conduent retained Plaintiff Gresh's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Gresh's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

793. On or around October 24, 2025, Plaintiff Gresh received Notice that her Private Information, including name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

794. Plaintiff Gresh reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Gresh would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

795. Plaintiff Gresh greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Gresh is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

796. Plaintiff Gresh stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Gresh diligently chooses unique usernames and passwords for her various online accounts.

797. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Gresh has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

798. Following the Data Breach, Plaintiff Gresh has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

799. As a result of the Data Breach, Plaintiff Gresh has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Gresh would have spent on other activities, including but not limited to work and/or recreation.

800. The Data Breach has caused Plaintiff Gresh to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Gresh fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

801. As a result of the Data Breach, Plaintiff Gresh faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed. Gresh Plaintiff Gresh anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

802. Plaintiff Gresh's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Gresh to the imminent prospect of additional harm. Thus, Plaintiff Gresh has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

Z. Plaintiff Richard Acosta

803. Plaintiff Richard Acosta is a current policyholder of BCBSTX, who provided Conduent with Plaintiff Acosta's Private Information.

804. As a condition of obtaining services from Defendants, Plaintiff Acosta was required to provide Conduent, either directly or indirectly through BCBSTX, his Private Information.

805. Conduent was in possession of Plaintiff Acosta's Private Information before and during the Data Breach and continues to possess Plaintiff Acosta's Private Information to the present.

806. At the time of the Data Breach, Conduent retained Plaintiff Acosta's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Acosta's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

807. On or around October 24, 2025, Plaintiff Acosta received Notice that his Private Information, including his name, date of birth, Social Security number, and address were compromised as a result of the Data Breach.

808. Plaintiff Acosta reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Acosta would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

809. Plaintiff Acosta greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Acosta is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

810. Plaintiff Acosta stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Acosta diligently chooses unique usernames and passwords for his various online accounts.

811. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Acosta has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

812. Following the Data Breach, Plaintiff Acosta received alerts that his Private Information was published on the dark web.

813. Following the Data Breach, Plaintiff Acosta has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

814. Following the Data Breach, Plaintiff Acosta experienced actual fraud when an unauthorized third-party made a charge to his credit account, evidencing misuse of his Private Information.

815. As a result of the Data Breach, Plaintiff Acosta has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Acosta would have spent on other activities, including but not limited to work and/or recreation.

816. The Data Breach has caused Plaintiff Acosta to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Acosta fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

817. As a result of the Data Breach, Plaintiff Acosta faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

818. Plaintiff Acosta anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

819. Plaintiff Acosta's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Acosta to the imminent prospect of additional harm. Thus, Plaintiff Acosta has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

AA. Plaintiff Ricardo Alamilla

820. Plaintiff Ricardo Alamilla is a current policyholder of BCBSTX, who provided Conduent with Plaintiff Alamilla's Private Information.

821. As a condition of obtaining services from Defendants, Plaintiff Alamilla was required to provide Conduent, either directly or indirectly through BCBSTX, his Private Information.

822. Conduent was in possession of Plaintiff Alamilla's Private Information before and during the Data Breach and continues to possess Plaintiff Alamilla's Private Information to the present.

823. At the time of the Data Breach, Conduent retained Plaintiff Alamilla's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Alamilla's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

824. On or around October 24, 2025, Plaintiff Alamilla received Notice that his Private Information, including his name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

825. Plaintiff Alamilla reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Alamilla would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

826. Plaintiff Alamilla greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Alamilla is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

827. Plaintiff Alamilla stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Alamilla diligently chooses unique usernames and passwords for his various online accounts.

828. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Alamilla has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

829. Following the Data Breach, Plaintiff Alamilla has received alerts that his Private Information was published on the dark web.

830. Following the Data Breach, Plaintiff Alamilla has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

831. Following the Data Breach, Plaintiff Alamilla experienced attempted fraud, evidencing misuse of his Private Information. Plaintiff Alamilla received phishing emails informing him that bank accounts and an account with the Internal Revenue Service were being opened under his name.

832. As a result of the Data Breach, Plaintiff Alamilla has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Alamilla would have spent on other activities, including but not limited to work and/or recreation.

833. The Data Breach has caused Plaintiff Alamilla to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Alamilla fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

834. As a result of the Data Breach, Plaintiff Alamilla faces a lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

835. Plaintiff Alamilla anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

836. Plaintiff Alamilla's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Alamilla to the imminent prospect of additional harm. Thus, Plaintiff Alamilla has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

BB. Plaintiff Phillip Groll Jr.

837. Plaintiff Phillip Groll Jr. is a former policyholder of BCBSTX, who provided Conduent with his Private Information.

838. As a condition of obtaining services from Defendants, Plaintiff Groll was required to provide Conduent, either directly or indirectly through BCBSTX, his Private Information.

839. Conduent was in possession of Plaintiff Groll's Private Information before and during the Data Breach and continues to possess Plaintiff Groll's Private Information to the present.

840. At the time of the Data Breach, Conduent retained Plaintiff Groll's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Groll's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

841. On or around October 24, 2025, Plaintiff Groll received Notice that his Private Information, including name, address, date of birth, and Social Security number were exposed as a result of the Data Breach.

842. Plaintiff Groll reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Groll would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

843. Plaintiff Groll greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Groll is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

844. Plaintiff Groll stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Groll diligently chooses unique usernames and passwords for his various online accounts.

845. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Groll has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

846. Following the Data Breach, Plaintiff Groll has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

847. Following the Data Breach, Plaintiff Groll experienced actual fraud, including six unauthorized transactions between his bank card and credit card, evidencing misuse of his Private Information.

848. As a result of the Data Breach, Plaintiff Groll has spent several hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Groll would have spent on other activities, including but not limited to work and/or recreation.

849. The Data Breach has caused Plaintiff Groll to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Groll fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

850. As a result of the Data Breach, Plaintiff Groll faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

851. Plaintiff Groll anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

852. Plaintiff Groll's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Groll to the imminent prospect of additional harm. Thus, Plaintiff Groll has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

CC. Plaintiff Alexis Jackson

853. Plaintiff Alexis Jackson is a current policyholder of BCBSMT, who provided Conduent with Plaintiff Jackson's Private Information.

854. As a condition of obtaining services from Defendants, Plaintiff Jackson was required to provide Conduent, either directly or indirectly through BCBSMT, her Private Information.

855. Conduent was in possession of Plaintiff Jackson's Private Information before and during the Data Breach and continues to possess Plaintiff Jackson's Private Information to the present.

856. At the time of the Data Breach, Conduent retained Plaintiff Jackson's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Jackson's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

857. On or around October 24, 2025, Plaintiff Jackson received Notice that her Private Information, including name, address, data of birth, and Social Security number were compromised as a result of the Data Breach.

858. Plaintiff Jackson reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Jackson would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

859. Plaintiff Jackson greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Jackson is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

860. Plaintiff Jackson stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Jackson diligently chooses unique usernames and passwords for her various online accounts.

861. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Jackson has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

862. Following the Data Breach, Plaintiff Jackson has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

863. Following the Data Breach, Plaintiff Jackson experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Jackson had unauthorized charges made on her credit card.

864. As a result of the Data Breach, Plaintiff Jackson has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Jackson would have spent on other activities, including but not limited to work and/or recreation.

865. The Data Breach has caused Plaintiff Jackson to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Jackson fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

866. As a result of the Data Breach, Plaintiff Jackson faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

867. Plaintiff Jackson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

868. Plaintiff Jackson's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Jackson to the imminent prospect of additional harm. Thus, Plaintiff Jackson has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

DD. Plaintiff Teresa Jones

869. Plaintiff Teresa Jones is a current policyholder of BCBSTX, who provided Conduent with Plaintiff Jones Private Information.

870. As a condition of obtaining services from Defendants, Plaintiff Jones was required to provide Conduent, either directly or indirectly through BCBSTX, her Private Information.

871. Conduent was in possession of Plaintiff Jones' Private Information before and during the Data Breach and continues to possess Plaintiff Jones' Private Information to the present.

872. At the time of the Data Breach, Conduent retained Plaintiff Jones' Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Jones Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

873. On or around October 24, 2025, Plaintiff Jones received Notice that her Private Information, including name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

874. Plaintiff Jones reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Jones would not have allowed Defendants, or anyone in Defendants' position, to

maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

875. Plaintiff Jones greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Jones is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

876. Plaintiff Jones stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Jones diligently chooses unique usernames and passwords for her various online accounts.

877. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Jones has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

878. Following the Data Breach, Plaintiff Jones received alerts that her Private Information, including was published on the dark web.

879. Following the Data Breach, Plaintiff Jones has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

880. Following the Data Breach, Plaintiff Jones experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Jones had unauthorized charges made on her bank account which was the same account Plaintiff Jones used to pay for her health insurance. Additionally, Plaintiff has received multiple notifications from her other credit card accounts regarding attempted fraudulent charges which were rejected by the charge card companies. Last,

Plaintiff has recently been notified the IRS of an attempt by an unknown third party to obtain her Private Information.

881. As a result of the Data Breach, Plaintiff Jones has spent numerous hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Jones would have spent on other activities, including but not limited to work and/or recreation.

882. The Data Breach has caused Plaintiff Jones to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Jones fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

883. As a result of the Data Breach, Plaintiff Jones faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

884. Plaintiff Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

885. Plaintiff Jones sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Jones to the imminent prospect of additional harm. Thus, Plaintiff Jones has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

EE. Plaintiff Jared Poli

886. Plaintiff Jared Poli is a current policyholder of BCBSIL, who provided Conduent with his Private Information.

887. As a condition of obtaining services from Defendants, Plaintiff Poli was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

888. Conduent was in possession of Plaintiff Poli's Private Information before and during the Data Breach and continues to possess Plaintiff Poli's Private Information to the present.

889. At the time of the Data Breach, Conduent retained Plaintiff Poli's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Poli's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

890. On or around October 24, 2025, Plaintiff Poli received Notice that his Private Information, including his name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

891. Plaintiff Poli reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Poli would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he known that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

892. Plaintiff Poli greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Poli is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

893. Plaintiff Poli stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Poli diligently chooses unique usernames and passwords for his various online accounts.

894. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Poli has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the Data Breach, has already been used for criminal, fraudulent purposes.

895. Following the Data Breach, Plaintiff Poli received an alert that his Private Information was published on the dark web.

896. Following the Data Breach, Plaintiff Poli has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

897. Following the Data Breach, Plaintiff Poli experienced actual fraud, evidencing misuse of his Private Information. Plaintiff Poli was the victim of fraudulent charges of his credit card, as well as a fraudulent credit inquiry.

898. As a result of the Data Breach, Plaintiff Poli has spent 20 hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his password and other necessary mitigation efforts. This is valuable time that Plaintiff Poli would have spent on other activities, including but not limited to work and/or recreation.

899. The Data Breach has caused Plaintiff Poli to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been

compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Poli fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

900. As a result of the Data Breach, Plaintiff Poli faces a lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

901. Plaintiff Poli anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

902. Plaintiff Poli's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff to the imminent prospect of additional harm. Thus, Plaintiff Poli has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

FF. Plaintiff Paul Snow

903. Plaintiff Paul Snow is a current policyholder of BCBSTX, who provided Conduent with his Private Information.

904. As a condition of obtaining services from Defendants, Plaintiff Snow was required to provide Conduent, either directly or indirectly through BCBSTX, his Private Information.

905. Conduent was in possession of Plaintiff Snow's Private Information before and during the Data Breach and continues to possess Plaintiff Snow's Private Information to the present.

906. At the time of the Data Breach, Conduent retained Plaintiff Snow's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

907. On or around October 24, 2025, Plaintiff Snow received Notice that his Private Information was compromised as a result of the Data Breach.

908. Plaintiff Snow reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Snow would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

909. Plaintiff Snow greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Snow is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

910. Plaintiff Snow stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Snow diligently chooses unique usernames and passwords for his various online accounts.

911. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Snow has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

912. Following the Data Breach, Plaintiff Snow has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

913. Following the Data Breach, Plaintiff Snow experienced actual fraud when an unauthorized third-party made charges on his credit account, evidencing misuse of his Private Information.

914. As a result of the Data Breach, Plaintiff Snow has spent 30 hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report, changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Snow would have spent on other activities, including but not limited to work and/or recreation.

915. The Data Breach has caused Plaintiff Snow to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Snow fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

916. As a result of the Data Breach, Plaintiff Snow faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

917. Plaintiff Snow anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

918. Plaintiff Snow's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Snow to the

imminent prospect of additional harm. Thus, Plaintiff Snow has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

GG. Plaintiff Wesley Triphahn

919. Plaintiff Wesley Triphahn is a former policyholder of BCBSIL, who provided Conduent with Plaintiff Triphahn's Private Information.

920. As a condition of obtaining services from Defendants, Plaintiff Triphahn was required to provide Conduent, either directly or indirectly through BCBSIL, his Private Information.

921. Conduent was in possession of Plaintiff Triphahn's Private Information before and during the Data Breach and continues to possess Plaintiff Triphahn's Private Information to the present.

922. At the time of the Data Breach, Conduent retained Plaintiff Triphahn's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Triphahn's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

923. On or around October 24, 2025, Plaintiff Triphahn received Notice that his Private Information, including his name, date of birth, Social Security number, and address were compromised as a result of the Data Breach.

924. Plaintiff Triphahn reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Triphahn would not have allowed Defendants, or anyone in Defendants' position, to maintain his Private Information if he knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

925. Plaintiff Triphahn greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Triphahn is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

926. Plaintiff Triphahn stores documents containing his Private Information in a secure location and destroys any documents he receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise his identity. Moreover, Plaintiff Triphahn diligently chooses unique usernames and passwords for his various online accounts.

927. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Triphahn has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

928. Following the Data Breach, Plaintiff Triphahn has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of his Private Information.

929. Following the Data Breach, Plaintiff Triphahn experienced actual fraud when an unauthorized third-party submitted an unemployment claim in Plaintiff Triphahn's name to the Illinois Department of Employment Security or around June 2025, evidencing misuse of his Private Information. Once notified, Plaintiff Triphahn contacted his employer's human resources personnel and the Illinois Department of Employment Security to notify of them of the fraudulent claim. Moreover, on or around June 16, 2025, Plaintiff Triphahn filed a police report and registered with IdentityTheft.gov.

930. As a result of the Data Breach, Plaintiff Triphahn has spent more than 10 hours researching the Data Breach, reviewing his financial accounts, monitoring his credit report,

changing his passwords online, and remediating the fraud perpetrated against him. This is valuable time that Plaintiff Triphahn would have spent on other activities, including but not limited to work and/or recreation.

931. The Data Breach has caused Plaintiff Triphahn to suffer fear, anxiety, and stress regarding the disclosure of his Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying him of the fact that his Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Triphahn fears for his personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of his Private Information.

932. As a result of the Data Breach, Plaintiff Triphahn faces a present and continuing lifetime risk of identity theft and fraud, as his Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

933. Plaintiff Triphahn anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

934. Plaintiff Triphahn's sensitive Private Information remains unencrypted in Defendants' possession without adequate protections against known threats, exposing Plaintiff Triphahn to the imminent prospect of additional harm. Thus, Plaintiff Triphahn has a continuing interest in ensuring that his Private Information is protected and safeguarded from future breaches.

HH. Plaintiff Andrea Young

935. Plaintiff Andrea Young is a former policyholder of BCBSTX, who provided Conduent with Plaintiff Young's Private Information.

936. As a condition of obtaining services from Defendants, Plaintiff Young was required to provide Conduent, either directly or indirectly through BCBSTX, her Private Information.

937. Conduent was in possession of Plaintiff Young's Private Information before and during the Data Breach and continues to possess Plaintiff Young's Private Information to the present.

938. At the time of the Data Breach, Conduent retained Plaintiff Young's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Young's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

939. On or around October 24, 2025, Plaintiff Young received Notice that her Private Information, including name, address, date of birth, and Social Security number were compromised as a result of the Data Breach.

940. Plaintiff Young reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Young would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

941. Plaintiff Young greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Young is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

942. Plaintiff Young stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity.

Moreover, Plaintiff Young diligently chooses unique usernames and passwords for his various online accounts.

943. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Young has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

944. Following the Data Breach, Plaintiff Young has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

945. Following the Data Breach, Plaintiff Young experienced attempted fraud, evidencing misuse of her Private Information, when an unauthorized party used Plaintiff Young's Private Information to request unemployment benefits on her behalf with the Texas Workforce Commission.

946. As a result of the Data Breach, Plaintiff Young has spent several hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Young would have spent on other activities, including but not limited to work and/or recreation.

947. The Data Breach has caused Plaintiff Young to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Young fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

948. As a result of the Data Breach, Plaintiff Young faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

949. Plaintiff Young anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

950. Plaintiff Young sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Young to the imminent prospect of additional harm. Thus, Plaintiff Young has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

Humana Plaintiff

II. Plaintiff Peggi Bordelon

951. Plaintiff Peggi Bordelon is a current policyholder of Humana who provided Conduent with Plaintiff Bordelon's Private Information.

952. As a condition of obtaining services from Defendants, Plaintiff Bordelon was required to provide Conduent, either directly or indirectly through Humana, her Private Information.

953. Conduent was in possession of Plaintiff Bordelon's Private Information before and during the Data Breach and continues to possess Plaintiff Bordelon's Private Information to the present.

954. At the time of the Data Breach, Conduent retained Plaintiff Bordelon's Private Information on its network with inadequate data security and in unencrypted form, causing Plaintiff Bordelon's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

955. On or around October 8, 2025, Plaintiff Bordelon received Notice that her Private Information, including name, treatment cost information, treatment date information, and health insurance number, were compromised as a result of the Data Breach.

956. Plaintiff Bordelon reasonably understood and expected that Defendants would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Bordelon would not have allowed Defendants, or anyone in Defendants' position, to maintain her Private Information if she knew that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

957. Plaintiff Bordelon greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Bordelon is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

958. Plaintiff Bordelon stores documents containing her Private Information in a secure location and destroys any documents she receives in the mail that contains any Private Information or that may contain any information that could otherwise be used to compromise her identity. Moreover, Plaintiff Bordelon diligently chooses unique usernames and passwords for her various online accounts.

959. As a direct and proximate result of the Data Breach that Defendants caused and allowed to occur, Plaintiff Bordelon has suffered, and will imminently suffer, injuries-in-fact and damages, including the unauthorized disclosure of the Private Information itself.

960. Following the Data Breach, Plaintiff Bordelon has experienced a significant increase in spam calls, text messages, and emails, evidencing misuse of her Private Information.

961. Following the Data Breach, Plaintiff Bordelon experienced actual fraud, evidencing misuse of her Private Information. Plaintiff Bordelon had a fraudulent charge made on her American Express card.

962. As a result of the Data Breach, Plaintiff Bordelon has spent more than 20 hours researching the Data Breach, reviewing her financial accounts, monitoring her credit report, changing her passwords and other necessary mitigation efforts. This is valuable time that Plaintiff Bordelon would have spent on other activities, including but not limited to work and/or recreation.

963. The Data Breach has caused Plaintiff Bordelon to suffer fear, anxiety, and stress regarding the disclosure of her Private Information in the Data Breach, which has been compounded by Defendants' delay in notifying her of the fact that her Private Information was acquired by criminals as a result of the Data Breach. Plaintiff Bordelon fears for her personal financial security and uncertainty over the information disclosed in the Data Breach and is experiencing emotional distress over the unauthorized disclosure of her Private Information. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that is contemplated and addressed by law.

964. As a result of the Data Breach, Plaintiff Bordelon faces a lifetime risk of identity theft and fraud, as her Private Information compromised in the Data Breach includes sensitive data that cannot be changed.

965. Plaintiff Bordelon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

966. Plaintiff Bordelon's sensitive Private Information remains in Defendants' possession without adequate protections against known threats, exposing Plaintiff Bordelon to the

imminent prospect of additional harm. Thus, Plaintiff Bordelon has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

967. Plaintiffs bring this action individually and on behalf of all other persons similarly situated pursuant to Federal Rule of Civil Procedure 23.

968. The Class Plaintiffs seek to represent is defined as follows:

Nationwide Class: All individuals residing in the United States whose Private Information was compromised in the Data Breach, including all those individuals who receive notice of the Data Breach.

969. In addition, Plaintiffs seek to represent Subclasses of persons defined as follows:

State Subclasses: All individuals residing in the State identified in the applicable Count whose Private Information was compromised in the Data Breach, including all those individuals who receive notice of the Data Breach.

970. Collectively, the Class and Subclasses are referred to as the “Class” or “Class Members.”

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

972. The proposed Class is based on the information available to Plaintiffs at this time. Plaintiffs reserve the right to modify the Class definition before the Court determines whether class certification is appropriate, as may be necessary to account for any newly-learned or changed facts as the litigation progresses.

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

974. Numerosity. Upon information and belief, there are over 44.4 million Class Members. Thus, the Class Members are so numerous that joinder of all Class Members is impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of Class Members are ascertainable through Defendants' records, including but not limited to the files implicated in the Data Breach.

975. Commonality. There are questions of law and fact common to the Class. These common questions of law and fact include, without limitation:

- a. Whether Defendants engaged in the conduct alleged herein;
- b. When Defendants learned of the Data Breach;
- c. Whether Defendants' response to the Data Breach was adequate;
- d. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- f. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- g. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
- h. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

- i. Whether Defendants breached their duty to Plaintiffs and Class Members to safeguard their Private Information;
- j. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- k. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- l. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- m. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;
- n. Whether Defendants' conduct was negligent;
- o. Whether Defendants' conduct was *per se* negligent;
- p. Whether Defendants were unjustly enriched;
- q. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages as a result of Defendants' wrongful conduct;
- r. Whether Plaintiffs and Class Members are entitled to equitable relief as a result of Defendants' wrongful conduct, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

976. Typicality. Plaintiffs' claims are typical of the claims of Class Members. The claims of the named Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories. Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

977. Adequacy of Representation. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members. Plaintiffs will fairly and adequately represent and protect the interests of Class Members and have no interests antagonistic to Class Members. Further, Plaintiffs have retained counsel who are competent and experienced in litigating class actions, particularly data privacy litigation of this kind.

978. Predominance. Common questions of law and fact predominate over any questions affecting only individual Class Members. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that Plaintiffs' and Class Members' Private Information was stored 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.

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

980. Injunctive Relief. Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

981. Ascertainability. Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Conduent***

982. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

983. Conduent 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 Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

984. Conduent's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

985. Conduent knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Conduent knew or should have known it would be an attractive target for cyberattacks.

986. Conduent owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Conduent'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 design, maintain, oversee, and test its security systems to ensure that the Private Information in its possession was adequately secured and protected;
- c. To protect the Private Information in its possession by using reasonable and adequate security procedures and systems compliant with industry standards;
- d. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;
- e. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;
- f. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- g. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

987. Conduent's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measure to protect confidential data.

988. Conduent's duty also arose because it was bound by industry standards to protect the Private Information entrusted to it.

989. Plaintiffs and Class Members were foreseeable victims of any inadequate data security practices on the part of Conduent, and Conduent owed Plaintiffs and Class Members a duty of care to prevent the foreseeable risk of harm its insufficient data security measures created.

990. Conduent also had independent duties under state laws that required it to reasonably safeguard Plaintiffs and Class Members' Private Information and promptly notify them of the Data Breach.

991. Conduent, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

992. Conduent, by its actions and/or omissions, breached its duty of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

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

994. The specific negligent acts and omissions committed by Conduent include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information from being accessed and exfiltrated in the Data Breach;
- b. Failing to adequately monitor the security of their networks and systems, including failing to implement processes to quickly detect a data breach,

resulting in Defendants' failure to detect the Data Breach for nearly three months;

- c. Failing to periodically ensure that its systems maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;
- e. Failing to comply with the FTCA and HIPAA;
- f. Failing to adopt, implement, and maintain adequate practices and protocols to promptly determine that Plaintiffs' and Class Members' Private Information had been compromised in the Data Breach; and
- g. Failing to adopt, implement, and maintain adequate practices and protocols to timely notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

995. By failing to provide prompt and adequate individual notice of the Data Breach to Plaintiffs and Class Members, Conduent acted with reckless disregard for the rights of Plaintiffs and Class Members, depriving Plaintiffs and Class Members of the ability to take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

996. Conduent had the ability to protect its systems (and the Private Information that it stored on them) from attack, whereas Plaintiffs and Class Members did not.

997. Conduent's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

998. As a direct and proximate result of Conduent's inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misuse of Private Information and misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort, and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

999. Plaintiffs and the Class remain at heightened risk of future injury because their Private Information resides with Conduent and, further, because Conduent continues to gather new data on Plaintiffs and the Class. Without the use of adequate data security, Plaintiffs and the Class remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

1000. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees.

1001. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Conduent to, among other things, 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 Class Members.

COUNT II – NEGLIGENCE

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Insurer Defendants***

1002. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1003. Insurer Defendants 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 disclosed, compromised, lost, stolen, and misused by unauthorized parties.

1004. Insurer Defendants' duty also included a responsibility to implement processes by which they could detect and analyze a breach of their third-party vendors' security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

1005. Insurer Defendants knew or should have known of the risks inherent in sharing the Private Information of Plaintiffs and Class Members with Conduent and the importance of adequate security by their vendor. Insurer Defendants knew or should have known Conduent would be an attractive target for and was susceptible to cyberattacks.

1006. Insurer Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Insurer Defendants' duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their and their vendors' possession;

- b. To design, maintain, oversee, and test Conduent's security systems to ensure that the Private Information in Conduent's possession was adequately secured and protected;
- c. To require and ensure Conduent adequately safeguarded the Private Information in its possession by using reasonable and adequate security procedures and systems compliant with industry standards;
- d. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information shared with Conduent;
- e. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;
- f. To require and continuously verify Conduent implemented processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- g. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

1007. Insurer Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measure to protect confidential data.

1008. Insurer Defendants' duty also arose because Insurer Defendants were bound by industry standards to protect the Private Information entrusted to them.

1009. Plaintiffs and Class Members were foreseeable victims of any inadequate data security practices on the part of Insurer Defendants and their vendor, and Insurer Defendants owed them a duty of care not to subject them to an unreasonable risk of harm.

1010. Insurer Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiffs and Class Members' Private Information and promptly notify them of the Data Breach.

1011. Insurer Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information shared with Conduent.

1012. Insurer Defendants, by their actions and/or omissions, breached their duty of care by failing to require and verify that Conduent provided fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

1013. Insurer Defendants, by their actions and/or omissions, breached their duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

1014. The specific negligent acts and omissions committed by Insurer Defendants include, but are not limited to the following:

- a. Failing to exercise adequate oversight of Conduent by ensuring it adopted reasonable data security measures, practices, and protocols to protect Plaintiffs' and Class Members' Private Information from being accessed and exfiltrated in the Data Breach;

- b. Sharing their customers' Private Information with a company that Insurer Defendants should have known did not have adequate systems, practices, and protocols in place to protect it from unauthorized disclosure;
- c. Failing to implement data security systems, practices, and protocols sufficient to protect customers' Private Information;
- d. Failing to comply, or require and verify Conduent complied, with industry-standard data security measures;
- e. Failing to require and verify that Conduent adopt, implement, and maintain adequate practices and protocols to promptly determine that Plaintiffs' and Class Members' Private Information had been compromised in the Data Breach; and
- f. Failing to require and verify that Conduent adopt, implement, and maintain adequate practices and protocols to timely notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

1015. By failing to provide prompt and adequate individual notice of the Data Breach to Plaintiffs and Class Members, Insurer Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members, depriving Plaintiffs and Class Members of the ability to take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

1016. Insurer Defendants had special relationships with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Insurer Defendants with their Private Information was predicated on the understanding that Insurer Defendants would take adequate

security precautions, including with respect to their third-party vendors like Conduent. Only Insurer Defendants and Conduent had the ability to protect Conduent's systems (and the Private Information that it stored on them) from attack.

1017. Insurer Defendants were in an exclusive position to protect Plaintiffs' and Class Members' Private Information from the unauthorized access and exfiltration that resulted from the Data Breach. Plaintiffs and Class Members relied on Insurer Defendants to implement reasonable and industry standard data security protections and had no way to audit or influence the integrity of Insurer Defendants' or their vendors' data security practices.

1018. Insurer Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

1019. As a direct and proximate result of Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misuse of Private Information misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort, and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1020. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages;

enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees.

1021. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Insurer Defendants to, among other things, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III – NEGLIGENCE *PER SE*
***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Conduent***

1022. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1023. Pursuant to Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, Conduent had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs’ and Class Members’ Private Information.

1024. Section 5 of the FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Conduent, of failing to use reasonable measures to protect Private Information. 15 U.S.C. § 45(a)(1).

1025. The harms that occurred as a result of the Data Breach are the types of harms the FTCA was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiffs and Class Members here.

1026. Plaintiffs and Class Members are within the class of persons these federal laws were designed to protect.

1027. Insurer Defendants are “covered entities” under HIPAA and have a duty to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Insurer Defendants likewise had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.” *See* 45 C.F.R. § 164.304 (definition of “encryption”).

1028. As entities that receive patient information, Conduent is a “business associate” under HIPAA. Business associates also have legal obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into business associate agreements (“BAAs” between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.

1029. Conduent implemented inadequate data security measures and violated the FTCA and HIPAA by:

- a. Failing to adopt, implement, and maintain adequate security systems and data security practices to safeguard Plaintiffs’ and Class Members’ Private Information from being accessed and exfiltrated in the Data Breach;

- b. Failing to adequately monitor the security of their networks and systems, including failing to implement processes to quickly detect a data breach, resulting in Defendants' failure to detect the Data Breach for nearly three months;
- c. Failing to periodically ensure that its systems maintained reasonable data security safeguards;
- d. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;
- e. Failing to adopt, implement, and maintain adequate practices and protocols to promptly determine that Plaintiffs' and Class Members' Private Information had been compromised in the Data Breach; and
- f. Failing to adopt, implement, and maintain adequate practices and protocols to timely notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

1030. Conduent's violations of the FTCA and HIPAA constitute negligence *per se*.

1031. As a direct and proximate result of Conduent's inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misuse of Private Information misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort, and expense responding to and preventing

the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1032. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees.

1033. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Conduent to, among other things, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT IV – NEGLIGENCE *PER SE*
On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Insurer Defendants

1034. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1035. Pursuant to Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, Insurer Defendants each had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs’ and Class Members’ Private Information.

1036. Section 5 of the FTCA prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Insurer Defendants, of failing to use reasonable measures to protect Private Information. 15 U.S.C. § 45(a)(1).

1037. The harms that occurred as a result of the Data Breach are the types of harms the FTCA was intended to protect against. The FTC has pursued enforcement actions against

businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiffs and Class Members here.

1038. Plaintiffs and Class Members are within the class of persons these federal laws were designed to protect.

1039. Insurer Defendants are “covered entities” under HIPAA and have a duty to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Insurer Defendants likewise had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.” *See* 45 C.F.R. § 164.304 (definition of “encryption”).

1040. As entities that receive patient information, Conduent is a “business associate” under HIPAA. Business associates also have legal obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into business associate agreements (“BAAs” between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.

1041. Insurer Defendants implemented inadequate data security measures and violated the FTCA and HIPAA by:

- a. Failing to exercise adequate oversight of Conduent by ensuring it adopted reasonable data security measures, practices, and protocols to protect Plaintiffs' and Class Members' Private Information from being accessed and exfiltrated in the Data Breach;
- b. Sharing their customers' Private Information with a company that Insurer Defendants should have known did not have adequate systems, practices, and protocols in place to protect it from unauthorized disclosure;
- c. Failing to implement data security systems, practices, and protocols sufficient to protect customers' Private Information;
- d. Failing to comply, or require and verify Conduent complied, with industry-standard data security measures;
- e. Failing to require and verify that Conduent adopt, implement, and maintain adequate practices and protocols to promptly determine that Plaintiffs' and Class Members' Private Information had been compromised in the Data Breach; and
- f. Failing to require and verify that Conduent adopt, implement, and maintain adequate practices and protocols to timely notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

1042. Insurer Defendants' violations of the FTCA and HIPAA constitute negligence *per se*.

1043. As a direct and proximate result of Insurer Defendants' inadequate security and the resulting Data Breach, Plaintiffs suffered and will continue to suffer significant injuries, including,

but not limited to (a) loss of privacy; (b) misuse of Private Information misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort, and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1044. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees.

1045. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Insurer Defendants to, among other things, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT V – BREACH OF IMPLIED CONTRACT

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Insurer Defendants***

1046. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1047. Plaintiffs and Class Members were required to provide sensitive Private Information to Insurer Defendants as a precondition for receiving employment and/or services.

1048. Insurer Defendants solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Insurer Defendants' regular business practices. Plaintiffs and Class Members accepted Insurer Defendants' offers and provided their Private Information to Insurer Defendants.

1049. When Plaintiffs and Class Members agreed to provide their Private Information and/or payment to Insurer Defendants, they entered into valid and enforceable implied contracts with Insurer Defendants pursuant to which Insurer Defendants agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

1050. Additionally, Insurer Defendants implicitly promised and agreed to retain this Private Information only under conditions that kept such information secure and confidential and only as long as reasonably necessary to perform essential business functions. As such, Insurer Defendants had a duty to reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or access.

1051. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Insurer Defendants' data security practices and policies were reasonable and consistent with industry standards, and Insurer Defendants' own representations.

1052. Insurer Defendants' implied promises to safeguard Plaintiffs' and Class Members' Private Information are evidenced by representations on Insurer Defendants' websites and in their applicable privacy policies, described herein. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Insurer Defendants on the other, is further demonstrated by their conduct and course of dealing.

1053. Plaintiffs and Class Members reasonably believed that Insurer Defendants would use part of the monies obtained from the benefits derived from the Private Information they provided, or payments made directly or indirectly on their behalf, to fund proper and reasonable data security practices.

1054. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Insurer Defendants in the absence of the implied contract or implied terms between them and Insurer Defendants. The safeguarding of the Private Information of Plaintiffs and Class Members was material to realize the intent of the parties.

1055. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Insurer Defendants when they provided their Private Information and/or payment to Insurer Defendants.

1056. Insurer Defendants materially breached their implied contracts with Plaintiffs and Class Members to protect their Private Information by failing to implement adequate data security precautions to protect Plaintiffs' and Class Members' Private Information from disclosure to unauthorized parties, and failing to notify Plaintiffs and Class Members of the specific data breached in a reasonably timely manner.

1057. The Data Breach was a reasonably foreseeable consequence of Insurer Defendants' conduct in breach of these implied contracts with Plaintiffs and Class Members.

1058. As a direct and proximate result of Insurer Defendants' breach of implied contract, Plaintiffs and Class Members did not receive the benefit of their bargains with Insurer Defendants and instead received services of diminished value compared to those contemplated in the implied contracts. Plaintiffs and Class Members were therefore damaged in an amount equal to at least the

difference in the value of the services with data security protection they paid for and that which they received.

1059. Had Insurer Defendants disclosed that their data security practices were inadequate, Plaintiffs and Class Members would not have contracted with Insurer Defendants, nor would any reasonable person.

1060. As a direct and proximate result of Insurer Defendants' breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages. Plaintiffs and Class Members seek all available damages, including compensatory, consequential, general, and/or nominal damages, in an amount to be proven at trial.

COUNT VI – BREACH OF THIRD PARTY BENEFICIARY CONTRACT

*On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Conduent*

1061. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1062. Under HIPAA, 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 provider of certain services to, a covered entity that involve access by the business associate to PHI. HIPAA rules require that a covered entity and any business associate enter into business associate agreements (“BAAs”) requiring the business associate to appropriately safeguard PHI.

1063. Pursuant to HIPAA, a “business associate must comply with the applicable standards, implementation specifications, and requirements of [HIPAA] with respect to electronic protected health information of a covered entity.” 45 C.F.R. § 164.302. Those safeguards include obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements

into BAAs between business associates and covered entities); see also 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902. These requirements are uniform and exist in every BAA.

1064. Because Conduent uses, analyzes, collects, obtains, and accesses personal health information of patients through the normal course of its business, including Plaintiffs' and Class Members' Private Information, upon information and belief, Conduent entered into BAAs with Insurer Defendants.

1065. Those BAAs must each contain identical requirements obligating signatories (*i.e.*, here, Defendants) to comply with HIPAA. The requirements in the BAA are intended to protect patients like Plaintiffs' and the Class against the disclosure, theft, unauthorized access, or other harms stemming from the use of their medical information.

1066. Thus, these contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Conduent and Insurer Defendants. Conduent knew that if it were to breach these contracts with Insurer Defendants, Plaintiffs and Class Members would be harmed.

1067. Although Conduent was subject to a BAA and, therefore, HIPAA's requirements to implement adequate safeguards to protect PHI, Conduent failed to comply.

1068. Conduent breached the contracts it entered into with Insurer Defendants by, among other things, (a) failing to use reasonably data security measures and protocols sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized access and exfiltration during the Data Breach, including by failing to adequately segregate Plaintiffs' and Class Members' Private Information and permitting access to Conduent's network containing Plaintiffs'

and the Class's unencrypted Private Information without the use of MFA; (b) failing to use reasonably data security measures and protocols sufficient to detect the Data Breach, including failing to adequately monitor activity on the network containing Plaintiffs' and the Class's Private Information; and (c) failing to promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

1069. As a direct and proximate result of Conduent's violation of HIPAA and breach of its required BAAs, Plaintiffs and the Class suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misuse and misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1070. Plaintiffs and the Class remain at heightened risk of future injury because their Private Information resides with Conduent and, further, because Conduent continues to gather new medical information on Plaintiffs and the Class via the direct or indirect contracts with providers. Absent compliance to those contracts' data security requirements, Plaintiffs and the Class remain at a heightened and substantial risk that their Private Information will be subject to another data breach. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

1071. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT VII – UNJUST ENRICHMENT

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Conduent***

1072. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1073. This claim is alleged in the alternative to the breach of third-party beneficiary claim.

1074. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, used by, and maintained by Conduent and that was ultimately stolen in the Data Breach.

1075. Conduent received a substantial monetary benefit from Plaintiffs and the Class by collecting, using, processing, storing, analyzing, and maintaining (for its own benefit and revenue) Plaintiffs' and Class Members' Private Information. Conduent has made substantial gains through the collection, processing, use, storage, and analysis of Plaintiffs' and the Class's Private Information, and was contracted in part for the specific purpose of processing and analyzing the customer data.

1076. Conduent obtained Plaintiffs' and Class Members' Private Information under the promise of securing patient data from unauthorized access and complying with HIPAA and other state and federal requirements to implement reasonable measures to protect that Private Information.

1077. Thus, Plaintiffs and Class Members conferred a benefit on Conduent by providing their Private Information to the Conduent.

1078. Moreover, upon information and belief, payments made by Insurer Defendants to Conduent included payments for cybersecurity protection to protect Plaintiffs and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated premiums charged by Insurer Defendants. Plaintiffs and Class Members did not receive such protection.

1079. Upon information and belief, Conduent funds its data security measures entirely from their general revenue, including from payments made to Conduent by Plaintiffs and Class Members, through Insurer Defendants.

1080. As such, a portion of the payments made by Plaintiffs and Class Members to Conduent, and of the revenue Conduent generates from providing services with respect to their Private Information, should have been used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards.

1081. Had Plaintiffs and Class Members known Conduent would not adequately secure their Private Information, they would not have provided such Private Information to Insurer Defendants or permitted Insurer Defendants to provide such information to Conduent.

1082. Further, if Conduent had disclosed that its data security measures were inadequate, Conduent would not have been permitted to continue in operation by regulators or its clients.

1083. Conduent has unjustly retained the benefits of its unlawful conduct, including (a) the amounts of payment received indirectly from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices, which Conduent failed to provide, and (b) Plaintiffs' Private Information, which Conduent profits from and is specifically contracted to use

and manage, while failing to use the payments and revenue it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

1084. Conduent also benefitted through its unjust conduct by retaining money Conduent should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

1085. Conduent knew Plaintiffs and Class Members conferred these benefits upon it, which Conduent accepted.

1086. As a result of Conduent's wrongful conduct as alleged in this Complaint, Conduent has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

1087. The benefits conferred upon, received, and enjoyed by Conduent were not conferred gratuitously, and it would be inequitable, unfair, and unjust for Conduent to retain the benefit. Conduent's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

1088. Plaintiffs and Class Members have no adequate remedy at law because of Conduent's continuing inadequate security practices, and because their injuries include an imminent and ongoing risk of identity theft and fraud.

1089. Plaintiffs and the Class remain at heightened risk of future injury because their Private Information resides with Conduent and, further, because Conduent continues to gather new medical information on Plaintiffs and the Class. Without the use of adequate data security requirements, Plaintiffs and the Class remain at a heightened and substantial risk that their Private Information will be subject to another data breach.

1090. Conduent is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Conduent as a result of its wrongful conduct, including specifically: the value to Conduent of the Private Information that Plaintiffs and Class Members provided; the revenue Conduent received and is receiving from the use of that Private Information; and the amounts that Conduent should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT VIII – UNJUST ENRICHMENT

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against Insurer Defendants***

1091. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1092. This claim is alleged in the alternative to the breach of implied contract claim.

1093. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, used by, and maintained by Insurer Defendants and that was ultimately stolen in the Data Breach.

1094. Insurer Defendants received a substantial monetary benefit from Plaintiffs and the Class by the collection, maintenance, and use (for their own benefit) of Plaintiffs' Private Information. Insurer Defendants have made substantial gains through the collection and analysis of Plaintiffs' and the Class's Private Information, which Insurer Defendants obtained under the promise of securing patient data from unauthorized access and complying with HIPAA and other state and federal requirements to implement reasonable measures to protect that Private Information.

1095. Plaintiffs and Class Members conferred a benefit on Insurer Defendants by providing their Private Information to Insurer Defendants.

1096. Plaintiffs and Class Members conferred a benefit on Insurer Defendants by permitting Insurer Defendants to turn over their Private Information to Conduent so that Insurer Defendants could reduce their operating costs.

1097. Moreover, upon information and belief, Plaintiffs and Class Members allege that payments made by Insurer Defendants to Conduent included payments for cybersecurity protection to protect Plaintiffs and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by Insurer Defendants for their services. Plaintiffs and Class Members did not receive such protection.

1098. Upon information and belief, Insurer Defendants fund their data security measures entirely from their general revenue, including from payments made to Insurer Defendants by Plaintiffs and Class Members.

1099. As such, a portion of the payments made by Plaintiffs and Class Members to Insurer Defendants is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Insurer Defendants.

1100. If Plaintiffs and Class Members had known that Insurer Defendants would not adequately secure their Private Information, they would not have provided such Private Information to Insurer Defendants or permitted Insurer Defendants to provide such information to Conduent.

1101. Further, if Insurer Defendants had disclosed that their data security measures were inadequate, Insurer Defendants would not have been permitted to continue in operation by regulators or their customers.

1102. Insurer Defendants have unjustly retained the benefits of their unlawful conduct, including (a) the amounts of payment received indirectly from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices, which they failed to provide and (b) Plaintiffs' Private Information, which Defendants profit from using for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs and Class Members' Private Information and prevented the Data Breach.

1103. Because of value provided by Insurer Defendants' use of Plaintiffs' and Class Members' Private Information, Insurer Defendants sold more services and products than they otherwise would have. Additionally, Insurer Defendants rely on data from Plaintiffs' and Class Members' Private Information to analyze underwriting risk and set premium rates, necessary acts to generate revenue. Thus, Insurer Defendants were unjustly enriched by profiting from the additional services and products they were able to market, sell, and create to the detriment of Plaintiffs and Class Members.

1104. Insurer Defendants also benefitted through their unjust conduct by retaining money that they should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information, or to exercise sufficient oversight over the data security practices of their contractors.

1105. Insurer Defendants knew Plaintiffs and Class Members conferred these benefits upon them, which Insurer Defendants accepted.

1106. As a result of Insurer Defendants' wrongful conduct as alleged in this Complaint, Insurer Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

1107. The benefits conferred upon, received, and enjoyed by Insurer Defendants were not conferred gratuitously, and it would be inequitable, unfair, and unjust for Insurer Defendants to retain the benefit. Insurer Defendants' retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

1108. Plaintiffs and Class Members have no adequate remedy at law because of Insurer Defendants' continuing inadequate security practices, and because their injuries include an imminent and ongoing risk of identity theft and fraud.

1109. Insurer Defendants are therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Insurer Defendants as a result of their wrongful conduct, including specifically: the value to Insurer Defendants of the Private Information that was stolen in the Data Breach; the profit Insurer Defendants received and are receiving from the use of that Private Information; the amounts that Insurer Defendants overcharged Plaintiffs and Class Members for use of their products and services; and the amounts that Insurer Defendants should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT IX – DECLARATORY AND INJUNCTIVE RELIEF

***On behalf of Plaintiffs and the Nationwide Class, or
alternatively, the State Subclasses, against all Defendants***

1110. Plaintiffs restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1111. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, which authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant necessary further relief. Furthermore, the Court has broad authority to restrain

acts, such as here, that are tortious and violate the terms of the federal statute and state common law as described in this Complaint.

1112. Defendants owe duties of care to Plaintiffs and Class Members, which required them to adequately secure Plaintiffs' and Class Members' Private Information.

1113. Defendants still possess Private Information regarding Plaintiffs and Class Members.

1114. Plaintiffs allege that Defendants' data security measures remain inadequate.

1115. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

1116. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants owed, and continue to owe, a legal duty to secure Private Information obtained from Plaintiffs and Class Members and to timely notify such individuals of a data breach under the common law, and Section 5 of the FTC Act;
- b. Defendants breached and continue to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information; and
- c. Defendants' breach of their legal duties continues to cause harm to Plaintiffs and Class Members.

1117. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols (and oversight of such protocols) consistent

with law and industry standards to protect individuals' (i.e., those of Plaintiffs and Class Members) Private Information, including the following:

- a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.
- b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:
 - i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
 - ii. engaging third-party security auditors and internal personnel to run automated security monitoring;
 - iii. auditing, testing, and training their security personnel regarding any new or modified procedures;
 - iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
 - v. conducting regular database scanning and security checks;
 - vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

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

1118. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial, a fact Conduent acknowledges in its Form 10-K. In fact, now that Conduent's insufficient data security is known to hackers, the Private Information in Conduent's possession is even more vulnerable to cyberattack. If another breach at Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

1119. The hardship to Plaintiffs and Class Members if an injunction is not issued 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 preexisting legal obligation to employ such measures.

1120. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff, Class Members, and consumers whose confidential information would be further compromised.

COUNT X – VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT

Cal. Bus. & Prof. Code § 1798.150, *et seq.* (“CCPA”)

***On behalf of the California Plaintiffs and the California Subclass against Defendant
Conduent Business Services, LLC***

1121. The California Plaintiffs identified above (“Plaintiffs” for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1122. Defendant Conduent Business Services, LLC (“Defendant” for the purposes of this Count) violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs’ and the California Subclass’ nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

1123. Defendant is a “business” under the meaning of California Civil Code § 1798.140(d) because Defendant is a “corporation[s], association[s], or other legal entit[ies] that [are] organized or operated for the profit or financial benefit of [their] shareholders or other owners” that “collect consumers’ Private Information” and are active “in the State of California” and “had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year.”

1124. Plaintiffs and the California Subclass seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiffs’ and the California Subclass’s Private Information. Plaintiffs and the California Subclass have an interest in ensuring

that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

1125. On January 15, 2026, Defendant Conduent Business Services, LLC was sent written notice of its violations pursuant to Cal. Civ. Code § 1798.150 by Plaintiff Nathan Cornwell. On January 16, 2026, Defendant Conduent Business Services, LLC was sent written notice of its violations pursuant to Cal. Civ. Code § 1798.150 by Plaintiff Marc Powell. As Defendant has failed to cure the violation within 30 days, Plaintiffs seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars (\$750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

1126. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the Private Information under the CCPA.

1127. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

COUNT XI – VIOLATION OF THE CCPA

Cal. Bus. & Prof. Code § 1798.150, *et seq.*

***On behalf of the California Plaintiffs and the California Subclass
against Defendants Elevance and HCSC***

1128. The California Plaintiffs identified above (“Plaintiffs” for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1129. Defendants Elevance and HCSC (“Defendants” for the purposes of this Count) violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs and the California Subclass. As a direct and

proximate result, Plaintiffs' and the California Subclass' nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

1130. Defendants are each a "business" under the meaning of California Civil Code § 1798.140(d) because each Defendant is a "corporation[s], association[s], or other legal entit[ies] that [are] organized or operated for the profit or financial benefit of [their] shareholders or other owners" that "collect consumers' Private Information" and are active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year."

1131. Plaintiffs and the California Subclass seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold Private Information, including Plaintiffs' and the California Subclass's Private Information. Plaintiffs and the California Subclass have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

1132. On March 18, 2026, Defendant Elevance was sent written notice of its violations pursuant to Cal. Civ. Code § 1798.150 by Plaintiff Marc Powell. On March 18, 2026, Defendant HCSC was sent written notice of its violations pursuant to Cal. Civ. Code § 1798.150 by Plaintiff Nathan Cornwell. In the event that Defendants fail to cure the violation within 30 days, Plaintiffs will request leave to amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars (\$750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

1133. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the Private Information under the CCPA.

1134. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants.

**COUNT XII – VIOLATION OF THE CALIFORNIA
CONFIDENTIALITY OF MEDICAL INFORMATION ACT**

**Cal. Civ. Code § 56 *et seq.* (“CMIA”)
*On behalf of the California Plaintiffs and the California Subclass against Defendants
Conduent, Elevance and HCSC***

1135. The California Plaintiffs identified above (“Plaintiffs” for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1136. Under California’s Confidentiality of Medical Information Act (“CMIA”), “persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved . . . [and it] is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information.” Cal. Civ. Code Div. 1, Pt. 2.6.

1137. Furthermore, “[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein.” Cal. Civ. Code § 56.101(a).

1138. And “[a]ny provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys,

or disposes of medical information shall be subject to the remedies and penalties provided.” Cal. Civ. Code § 56.101(a).

1139. As providers of health care, contractor, and/or recipient of medical information, Defendants Conduent, Elevance, and HCSC (“Defendants” for purposes of this Count) were required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated or released without patient’s authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.13, 56.245, 56.26, 56.36, and 56.101.

1140. Thus, “an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her.” Cal. Civ. Code § 56.36(b).

1141. Plaintiffs and California Subclass Members are “patients” as defined in Cal. Civ. Code § 56.05(m) (“‘Patient’ means a natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.”).

1142. Plaintiffs and Class Members are “Enrollees” under Civil Code § 56.05(e) to the extent they are a “person who is enrolled in a plan and who is a recipient of services from the plan.” *See* Cal. Health & Safety Code § 1345(c).

1143. Plaintiffs and Class Members are “Subscribers” under Civil Code § 56.05(q) to the extent they are a “person who is enrolled in a plan and who is a recipient of services from the plan.” *See* Cal. Health & Safety Code § 1345(p).

1144. Plaintiffs and California Subclass Members, as patients and customers of Defendants, had their individually identifiable “medical information,” within the meaning of Cal.

Civ. Code § 56.05(j), created, maintained, preserved, and stored on Defendants' computer networks, and were patients on or before the date of the Data Breach.

1145. Here, Defendants are subject to the CMIA because Defendants provide health care service plans, and Defendants created, maintained, preserved, stored, abandoned, destroyed, and/or disposed of medical information regarding Plaintiffs and the California Subclass.

1146. Defendants were negligent because they failed to take reasonable precautions to ensure Conduent's data systems were protected. As a result of Defendants' negligence, an unauthorized third-party viewed and obtained Plaintiffs' medical information.

1147. Defendants' negligence resulted in the release of individually identifiable medical information pertaining to Plaintiffs and California Subclass Members to unauthorized persons and the breach of the confidentiality of that information. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs and California Subclass Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

1148. Defendants also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

1149. Section 56.101(a) of the CMIA provides that "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be

subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” Section 56.101(b)(1)(A) further provides that “[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information.”

1150. Section 56.36(b) of the CMIA provides the following:

In addition to any other remedies available at law, an individual may bring an action against a person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following:

(1) Except as provided in subdivision (e), nominal damages of one thousand dollars (\$1,000). In order to recover under this paragraph, it is not necessary that the plaintiff suffered or was threatened with actual damages.

(2) The amount of actual damages, if any, sustained by the patient.

1151. As such, Defendants are liable for damages in an amount to be determined at trial, but not less than the statutorily provided nominal damages of \$1,000 for each class member.

COUNT XIII – VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code § 1798.80 *et seq.* (“CCRA”)

***On behalf of the California Plaintiffs and the California Subclass against
Defendants Conduent, Elevance, and HCSC***

1152. The California Plaintiffs identified above (“Plaintiffs” for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1153. Under the California Customer Records Act, any “person or business that conducts business in California, and that owns or licenses computerized data that includes Private Information” must “disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted Private Information was, or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82. The disclosure must “be made in the most expedient time possible and without unreasonable delay” but disclosure must occur “immediately following discovery [of the

breach], if the Private Information was, or is reasonably believed to have been, acquired by an unauthorized person.” *Id.* (emphasis added).

1154. The Data Breach constitutes a “breach of the security system” of Conduent, Insurer Defendants’ vendor.

1155. Unauthorized person(s) acquired Plaintiffs’ and the California Subclass’s personal unencrypted information.

1156. Because Defendants Conduent, Elevance, and HCSC (“Defendants” for purposes of this Count) reasonably believed that California Plaintiffs’ and the California Subclass’s Private Information was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach in “the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82.

1157. Defendants failed to provide legally compliant and timely notice under § 1798.82 to Plaintiffs and Subclass members. Conduent became aware of the Data Breach on January 13, 2025. Upon information and belief, Insurer Defendants became aware of the Data Breach in January 2025. Yet Defendants failed to provide the required written notice to impacted individuals until beginning in October 2025, a year after the Data Breach began. Plaintiffs and the Class did not and could not know they were impacted by the Data Breach until and unless they received direct notice from Defendants.

1158. Defendants’ unreasonable delay prevented Plaintiffs and California Subclass members from taking appropriate measures to protect themselves against harm.

1159. Because Plaintiffs and California Subclass members were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

1160. As a direct and proximate result of Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, California Plaintiffs and California Subclass Members suffered damages including, but not limited to (a) loss of privacy; (b) misuse of Private Information misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1161. Plaintiffs and California Subclass members are entitled to equitable relief and damages in an amount to be determined at trial.

**COUNT XIV – VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND
DECEPTIVE BUSINESS PRACTICES ACT**

815 Ill. Comp. Stat. §§ 505/1 *et seq.* ("ICFA")

On behalf of the Illinois Plaintiffs and the Illinois Subclass against Conduent and HCSC

1162. The Illinois Plaintiffs identified above ("Plaintiffs" for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1163. Plaintiffs and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e). Plaintiffs, the Illinois Subclass, Conduent, and HCSC are "persons" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

1164. Conduent and HCSC ("Defendants" for purposes of this Count) are engaged in "trade" or "commerce," including the provision of services, as defined by 815 Ill. Comp. Stat. § 505/1(f). Defendants engaged in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

1165. The Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”) makes unlawful certain acts by persons in the conduct of trade or commerce. 815 Ill. Comp. Stat. § 505/2. Violating the Illinois Personal Information Protection Act (“IPIPA”), 815 Ill. Comp. Stat. 530/1, et seq., is one such unlawful act. 815 Ill. Comp. Stat. 530/20.

1166. The IPIPA requires “[a]ny data collector that owns or licenses personal information concerning an Illinois resident” to provide notice to the resident expediently and without unreasonable delay “that there has been a breach of the security of the system data following discovery or notification of the breach.” 815 Ill. Comp. Stat. § 530/10.

1167. Defendants are data collectors that own the personal information of Illinois’s residents as defined by the IPIPA. 815 Ill. Comp. Stat. 530/5.

1168. The IPIPA requires data collectors like Defendants that own or maintain “records that contain personal information concerning an Illinois resident” to “implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.” 815 Ill. Comp. Stat. § 530/45. Defendants failed to implement and maintain reasonable security measures as required by the statute.

1169. Defendants stored the Private Information in a knowingly unsafe and unsecured manner by, among other things, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Illinois Plaintiffs’ and the Illinois Subclass’s Private Information, and failing to adequately segment the sensitive data from other parts of Conduent’s servers and networks.

1170. Similarly, Defendants deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security. For example, upon information and belief, access to the breached network was

possible using compromised VPN credentials without multi-factor authentication—a basic data security requirement necessary to prevent unauthorized access to information.

1171. As Data Collectors, under IPIPA, Defendants were required to notify Plaintiffs and Illinois Subclass members of a breach of their data security systems in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

1172. Defendants failed to disclose the Data Breach in the most expedient time possible and without unreasonable delay. Thus, Defendants violated 815 Ill. Comp. Stat. § 530/10(a).

1173. Defendants’ decision not to timely disclose the Data Breach to Plaintiffs and Illinois Subclass Members was knowing and willful.

1174. Defendants’ unfair and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, also include:

- a. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Illinois Subclass Members’ Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;
- b. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs’ and Illinois Subclass Members’ Private Information, including by implementing and maintaining reasonable security measures;

- c. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);
- d. Failing to timely and adequately notify Plaintiffs and Illinois Subclass Members of the Data Breach;
- e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Illinois Subclass Members' Private Information; and
- f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

1175. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

1176. Defendants engaged in "unfair" business practices in violation of the ICFA because their failures to implement appropriate data security and data breach notification practices offends public policy.

1177. Defendants' conduct against Plaintiffs and the Illinois Subclass is oppressive in that Plaintiffs and the Illinois Subclass had no choice but to share their Private Information with Defendants in order to obtain health insurance services and/or employment from Insurer Defendants.

1178. Defendants intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions. Plaintiffs and Illinois Subclass Members reasonably relied on Defendants to advise them if their data security and data storage systems were not adequately secure to protect their Private Information, the truth of which they could not otherwise have discovered.

1179. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1180. Defendants acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Illinois Subclass members' rights. Conduent's past data breaches as well as other industry breaches put it on notice that its security and privacy protections were inadequate.

1181. As a direct and proximate result of Defendants’ unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1182. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law.

**COUNT XV – VIOLATION OF THE MASSACHUSETTS
CONSUMER PROTECTION ACT**

Mass. Gen. Laws Ann. Ch. 93A § 1 *et seq.*

***On behalf of the Massachusetts Plaintiff and the Massachusetts Subclass against Defendant
Conduent Business Services, LLC***

1183. The Massachusetts Plaintiff identified above (“Plaintiff” for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1184. Chapter 93A of the Massachusetts Consumer Protection Act forbids “unfair or deceptive acts or practices in the conduct of any trade or commerce.” Mass. Gen. Laws ch. 93A, § 2(a). Chapter 93A expressly provides that consideration be given to interpretations by the FTC and the federal courts relating to Section 5 of the FTC Act. Mass. Gen. Laws ch. 93A, § 2(b).

1185. Massachusetts Plaintiff and members of the Massachusetts Subclass are each a “person” as defined by the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §1(a) and, as alleged herein, have “been injured by another person's use or employment of any method, act or practice declared to be unlawful” under Ch. 93A. Mass. Gen. Laws Ann. ch. 93A, § 9.

1186. Defendant Conduent Business Services, LLC (“Defendant” for the purposes of this Count) is a “person” as defined by the Massachusetts Consumer Protection Act, Mass. Gen. Laws Ann. Ch. 93A, §1(a).

1187. Defendant engaged in “trade” or “commerce” defined as advertising, the offering for sale, rent or lease, the sale, rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situated. Mass. Gen. Laws Ann. Ch. 93A, §1(b).

1188. Defendant engaged in trade or commerce that directly or indirectly affects the people of the Commonwealth of Massachusetts.

1189. Specifically, Defendant collected and stored Massachusetts Plaintiff’s and the Massachusetts Subclass’s Personal Information. Defendant stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Massachusetts Plaintiff’s and the Massachusetts Subclass’s information, and failing to adequately segment the sensitive data from other parts of Conduent’s networks.

1190. Similarly, Defendant deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security.

1191. Defendant had a duty to keep the Personal Information safe and secure under HIPAA and regulations promulgated thereunder, the FTCA and regulations promulgated thereunder, and Mass. Gen. Laws Ch. 93H, §2 and regulations promulgated thereunder.

1192. Defendant's failure to comply with basic data security necessary to protect any stored data, much less the significant Private Information Conduent stored, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to over thirty million people. That is especially true because, despite failing to reasonably protect Massachusetts Plaintiff's and the Massachusetts Subclass's highly sensitive and private Personal Information, Defendant gained significant profit from that information. While Defendant profited off of Massachusetts Plaintiff's and the Massachusetts Subclass's data, it failed to take the necessary measures to protect it, leaving Plaintiff's and the Class at significant and foreseeable risk of harm.

1193. Defendant's unfair or deceptive acts and practices complained of herein affected the public interest and consumers at large, including Massachusetts Plaintiff and the Massachusetts Subclass, who are Massachusetts residents affected by the Data Breach. Massachusetts Plaintiff and the Massachusetts Subclass each were injured in Massachusetts.

1194. As a result of those unlawful and unfair business practices, Massachusetts Plaintiff and the Massachusetts Subclass's highly sensitive and private health and medical information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Private Information over thirty million people.

1195. As a direct and proximate result of Defendant's inadequate security and the resulting Data Breach, Plaintiff and the Massachusetts Subclass suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental

distress and anguish resulting from the access, theft and posting of their Personal Information; (g) disruption of their medical care and treatment; (h) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1196. Defendant Conduent Business Services, LLC was sent notice of Plaintiff's state statutory claims under Ch. 93A on January 14, 2026, more than thirty days before the filing of this Complaint.

1197. Massachusetts Plaintiff and the Massachusetts Subclass seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT XVI – VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT

N.J. Stat. Ann. §§ 56:8-1 *et seq.*

***On behalf of the New Jersey Plaintiff and the New Jersey Subclass
against Conduent and HCSC***

1198. The New Jersey Plaintiff identified above ("Plaintiff" for purposes of this Count) restate the allegations in Paragraphs 1 – 981 above as if fully set forth herein.

1199. The New Jersey Consumer Fraud Act ("NJCFA") makes unlawful certain acts by persons in any commercial practice. N.J. Stat. § 56:8-2. Violating New Jersey's data-breach notice statute is an unlawful practice under the NJCFA. N.J. Stat. § 56:8-160.

1200. The notice statute requires "any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information" to provide notice without unreasonable delay to New Jersey residents "whose

personal information was, or is reasonably believed to have been, accessed by an unauthorized person.” N.J. Stat. § 56:8-163(a).

1201. Conduent and HCSC (for purposes of this Count, “Defendants”) are businesses that compile and maintain computerized records that contain personal information as defined in N.J. Stat. § 56:8-161.

1202. Defendants therefore were required to disclose to New Jersey Plaintiff and New Jersey Subclass members the existence of the Data Breach without unreasonable delay.

1203. Although the Data Breach occurred in from October 2024 – January 2025 and Defendants became aware of the Data Breach in January 2025, Defendants failed to begin providing written notice to many victims until October 2025.

1204. As a direct and proximate result of Defendants’ inadequate security and the resulting Data Breach, Plaintiff and the New Jersey Subclass suffered and will continue to suffer significant injuries, including, but not limited to (a) loss of privacy; (b) misappropriation of their identity, name and likeness; (c) fraud and identity theft from the misuse of their stolen Private Information; (d) diminution in the value of their Private Information due to the loss of security, confidentiality, and privacy; (e) lost value of their Private Information; (f) emotional and mental distress and anguish resulting from the access, theft and posting of their Private Information; (g) disruption of their medical care and treatment; (h) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (i) a continued substantial and imminent risk of the misuse of their Private Information.

1205. New Jersey Plaintiff and the New Jersey Subclass seek all relief available by law including monetary damages and injunctive relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of those similarly situated, respectfully request the following relief:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Federal Rule of Civil Procedure 23; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

5. That Plaintiffs be granted the declaratory relief sought herein;

6. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: June 12, 2026

/s/ James E. Cecchi

James E. Cecchi
**CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.**
5 Becker Farm Road
Roseland, NJ 07068
Tel.: (973) 994-1700
Fax: (973) 994-1744
Email: jcecchi@carellabyrne.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Law Oas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel.: (954) 332-4200
Fax: (954) 525-4300
Email: ostrow@kolawyers.com

Co-Lead Counsel

Norman E. Seigel*
STUEVE SIEGEL HANSON LLP
460 Nichols Rd., Suite 200
Kansas City, MO 64112
Tel.: (816) 714-7112
Fax: (816) 714-7101
Email: siegel@stuevesiegel.com

Conduent Settlement Counsel

Gary M. Klinger*
MILLBERG, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

Conduent Client Settlement Counsel

Shauna Brie Itri
SEEGER WEISS LLP
325 Chestnut Street, Suite 917
Philadelphia, PA 19106
Tel.: (267) 973-4265
Email: sitri@seegerweiss.com

Ashley Crooks
HAUSFELD LLP
33 Whitehall Street, 14th Floor
New York, NY 10004
Tel.: (646) 357-1100
Fax: (212) 202-4322
Email: acrooks@hausfeld.com

Corban S. Rhodes*
DICELLO LEVITT LLP
485 Lexington Avenue, Suite 1001
New York, NY 10017
Tel.: (646) 933-1000
Email: crhodes@dicellolevitt.com

Connor P. Hayes*
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel.: (412) 322-9243
Email: connorh@lcllp.com

Raph Graybill*
GRAYBILL LAW FIRM, P.C.
300 4th Street North
P.O. Box 3586
Great Falls, MT 59403
Tel.: (406) 452-8566
Email: raph@graybilllawfirm.com

Thomas E. Loeser*
COTCHETT, PITRE & MCCARTHY, LLP
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel.: (206) 802-1272
Email: tloeser@cpmlegal.com

Linda P. Nussbaum*
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Tel.: (917) 438-9189
Email: lnussbaum@nussbaumpc.com

Brian C. Gudmundson*
ZIMMERMAN REED LLP

1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel.: (612) 341-0400
Email: brian.gudmundson@zimmreed.com

Plaintiffs' Steering Committee

Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Ste 1201
Newark, NJ 07102
Tel.: (973) 623-3000
Fax: 973-623-0858
Email: cderenze@litedepalma.com

Liaison Counsel

Attorneys for Plaintiffs and the Proposed Class

**Pro Hac Vice*