STATE OF RHODE ISLAND

PROVIDENCE, sc. SUPERIOR COURT

ALEXANDRA MORELLI, DAVID NOVSAM, AUDREY SNOW, BETTY J. POTENZA, NORMAN R. PLANTE, EILEEN BOTELHO, GARY RUO, DAVID A. ROSA, ROBIN KULIK, CARONAH CASSELL-JOHNSON, SHEILA M. GALAMAGA, CAITLYN LAMARRE, and DIANE M. CAPPALLI, individually and on behalf of all others similarly situated, Plaintiffs, v. RHODE ISLAND PUBLIC TRANSIT AUTHORITY and UNITEDHEALTHCARE OF NEW ENGLAND, INC., Defendants.	C.A. NO. PC-2022-6145

PLAINTIFFS' FIRST AMENDED COMPLAINT

INTRODUCTION

1. Alexander Morelli (hereafter also referred to as "Morelli"), David Novsam (hereafter also referred to as "Novsam"), Audrey Snow (hereafter also referred to as "Snow"), Betty J. Potenza (hereafter also referred to as "Potenza"), Norman R. Plante (hereafter also referred to as "Plante"), Eileen Botelho (hereafter also referred to as "Botelho"), Gary Ruo (hereafter also referred to as "Ruo"), David A. Rosa (hereafter also referred to as "Rosa"), Robin Kulik (hereafter also referred to as "Kulik"), Caronah Cassell-Johnson (hereafter also referred to as Cassell-Johnson), Sheila M. Galamaga (hereafter also referred to as "Galamaga"), Cailyn Lamarre (hereafter also referred to as "Lamarre") and Diane M. Cappalli (hereafter also referred to as "Cappalli") (hereafter Morelli, Novsam, Snow, Potenza, Plante, Botelho, Ruo, Rosa, Kulik,

Cassell-Johnson, Galamaga, Lamarre, and Cappalli collectively referred to as "Plaintiffs"), individually and on behalf of others similarly situated (hereafter also referred to as "Class" or "Class Members" or "Subclass" or "Subclass Members") bring this putative class action lawsuit against the Rhode Island Public Transit Authority (hereafter also referred to as "RIPTA") and UnitedHealthcare of New England (hereafter also referred to as "UHC") (hereafter RIPTA and UHC collectively referred to as "Defendants").

2. Plaintiffs make the following factual, as well as legal, allegations based upon personal knowledge as to all matters related to themselves, and upon information and belief, obtained in part from an investigation by their attorneys, as to all other matters:

3. Plaintiffs seek to remedy the damage caused by a data breach that occurred between August 3, 2021, and August 5, 2021 (hereafter also referred to as "Data Breach" or "Breach") resulting from the Defendants' actions and inactions.

4. Defendants failed to protect and secure highly sensitive confidential personal healthcare information (hereafter also referred to as "PHI") and highly sensitive confidential personally identifiable information (hereafter also referred to as "PII") of Plaintiffs and approximately 22,000 individuals that consist of employees and retirees of RIPTA as well as employees and retirees of the State of Rhode Island, who have had health insurance plans through RIPTA and the State of Rhode Island that UHC administered.

5. The PHI and the PII were gathered and maintained as part of self-insured healthcare insurance plans that UHC administered for employees and retirees of RIPTA and the State of Rhode Island.

6. The PHI containing data files that UHC wrongfully transmitted to RIPTA on behalf of State of Rhode Island employees without the employee's written consent included healthcare

plan member identification numbers, claim amounts, and dates of service for claims filed. Since such PHI data files contained healthcare information that revealed the history, diagnosis, condition, and treatment of State of Rhode Island employees, such PHI data is considered "confidential healthcare information."

7. The PII containing data files that UHC wrongfully transmitted to RIPTA on behalf of State of Rhode Island employees also included names, social security numbers, and dates of birth which, when accessed by unauthorized third parties, can be used to create financial havoc in the form of fraudulent financial activity and identity theft for the State of Rhode Island employees. Once an unauthorized third party has an individual's social security number, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name and get access to the individual's checking and savings accounts.

8. RIPTA unreasonably delayed notification of the Breach to Plaintiff and the Class and Subclass Members.

9. Had the Plaintiffs and the Class and Subclass Members received timely notice of the Breach, many would have been able to mitigate the harm caused by the delayed notification.

10. As a direct and indirect consequence of RIPTA's delay in notification of the Breach to the Plaintiffs, the Class, and the Subclass, several Plaintiffs have already been harmed by suffering fraud and identity theft from the Breach and are now exposed to imminent substantial ongoing risks of future fraud and identity theft since the threatened future injuries are certainly impending.

11. All Plaintiffs, the Class, and Subclass Members require continued monitoring of their financial accounts, future financial footprints, credit profiles, and identities as direct and indirect consequences of the Breach.

12. Plaintiffs, Class Members, and Subclass Members have incurred, will continue to incur, and may have to incur in the future out-of-pocket expenses for credit monitoring, credit freezes, or other protective products and services, along with expending time and resources to contact financial entities to cancel bank and credit card accounts, deactivate debit and credit cards, and request new debit and credit cards.

13. Also, Plaintiffs, Class Members, and Subclass Members have incurred and may incur direct damages related to various forms of identity theft and fraud. Plaintiffs, Class Members, and Subclass Members seek to remedy the damage caused by the Breach through injunctive relief for credit monitoring, the purging and destruction of their PHI and PII, the establishment of adequate security protocols, the reimbursement of out-of-pocket damages and the payment of compensatory damages.

14. Plaintiffs, Class Members, and Subclass Members bring the following claims: a) negligence; b) violations of the Identify Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-1, et seq.; c) violations of the Confidentiality of Healthcare Communications and Information Act, R.I. Gen. Laws § 5-37-3.1, d) breach of contract; e) breach of implied contract; f) violations of the Rhode Island Deceptive Trade Practices Act; and g) third-party beneficiary breach of contract.

PARTIES

15. Plaintiff Alexandra Morelli is an individual who resides in Coventry, Rhode Island, and who has worked at the University of Rhode Island since 2016. Plaintiff David Novsam is an individual who resides in Cranston, Rhode Island, and works for RIPTA. Plaintiff Audrey Snow is an individual who resides in Warwick and works for the State of Rhode Island. Plaintiff Betty J. Potenza is an individual who resides in Warwick and works for the State of Rhode Island.

16. Plaintiff Norman R. Plante is an individual who resides in West Warwick and works for Rhode Island Department of Corrections. Plaintiff Eileen Botelho is an individual who resides in Seekonk, Massachusetts, and works for the Rhode Island Department of Elementary and Secondary Education. Plaintiff Gary Ruo is an individual who resides in Coventry and is a retired State of Rhode Island who worked for the Rhode Island Department of Corrections. Plaintiff David A. Rosa is an individual who resides in Providence and works at Rhode Island College. Plaintiff Robin Kulik is an individual who resides in Cranston and is a retired State of Rhode Island employee who worked for the Rhode Island Department of Corrections.

17. Plaintiff Caronah Cassell-Johnson is an individual who resides in Providence and works for the State of Rhode Island. Plaintiff Sheila M. Galamaga is an individual who resides in Warwick and works for the Rhode Island Department of Education. Plaintiff Caitlyn Lamarre is an individual who resides in Cranston and works for the Rhode Island Department of Human Services. Plaintiff Diane M. Cappalli is an individual who previously resided in Rhode Island, currently resides in Sarasota, Florida, has worked at RIPTA, and is currently a RIPTA retiree.

18. Defendant, the Rhode Island Public Transit Authority, is a quasi-governmental entity located in Providence empowered by R.I. Gen. Laws § 39-18-4(a)(4) to sue and be sued in its own name.

19. Defendant, UnitedHealthcare of New England, Inc., is a Rhode Island corporation with its principal office address of 475 Kilvert Street, Warwick, Rhode Island.

JURISDICTION AND VENUE

20. This Court has subject jurisdiction over this case pursuant to R.I. Gen. Laws §§ 8-2-13 (equity), 8-2-14 (general jurisdiction where the amount exceeds $10,000), and 9-30-1

(declaratory judgment) as it seeks equitable and declaratory relief in addition to damages. The venue is proper as the Defendants are located in the State of Rhode Island; the Plaintiffs, the Class, and the Subclass are or were employed within the State of Rhode Island; UHC had a contract with the State of Rhode Island and with RIPTA to administer and process healthcare claims; and the claims at issue arose from services provided by UHC pursuant to its contract with RIPTA.

RELEVANT FACTS

21. The State of Rhode Island provides health insurance to state employees through a self-insured healthcare insurance plan (hereafter also referred to as the "State Plan"). Over the years, the State of Rhode Island has contracted with different health insurance entities to administer healthcare benefits and process medical care claims under the State Plan.

22. The State of Rhode Island currently has a contract with and uses Blue Cross Blue Shield of Rhode Island (hereafter also referred to as "BCBS") as its self-insured healthcare insurance plan administrator. Before using BCBS, the State of Rhode Island had a contract with and used UHC as its self-insured healthcare insurance plan administrator.

23. RIPTA is a quasi-public entity that provides public transportation, primarily bus service, in Rhode Island. RIPTA provides health insurance to its employees through its own self-insured health insurance plan (hereafter also referred to as the "RIPTA Plan").

24. RIPTA uses the same third-party administrators as the State to administer its plan. Accordingly, it, likewise, had replaced UHC with BCBS as its healthcare plan administrator approximately two years ago.

25. On Monday, January 31, 2022, at 5:30 PM, a State of Rhode Island Legislative committee, the Rhode Island Senate Committee on Rules, Government Ethics, and Oversight

(hereafter also referred to as "Senate Oversight Committee"), held a public hearing and took testimony, under oath, from witnesses on the topic of the RIPTA Cyber Data Breach (hereafter also referred to as "Senate Oversight Hearing"). The entire Senate Oversight Hearing is available at (https://ritv.devosvideo.com/show?video=9b38d2a2b1bc&apg=46373b64).

26. Representatives from RIPTA did appear and testified under oath at the Senate Oversight Hearing on the RIPTA Cyber Data Breach.

27. Notably, however, no representatives from UHC appeared or testified at the Senate Oversight Hearing.

28. Senator Louis P. DiPalma, Chairperson of the Senate Oversight Committee, noted his disappointment that UnitedHealthcare, who had accepted an invitation to appear before the Committee, had withdrawn its appearance as "there is a set of facts and some data that we are not going to hear."

29. As indicated in Committee testimony, on or about August 5, 2021, RIPTA identified the Breach, the unauthorized access to and a hack of its computer systems that occurred between August 3, 2021, and August 5, 2021.

30. Scott Avedisian, RIPTA's Executive Director, testified under oath at the Senate Oversight Hearing that "So on August 5, 2021, we identified a security incident that resulted in unauthorized access to some of our computer systems."

31. Scott Avedisian went on to testify at the Senate Oversight Hearing that "We immediately began investigation and took measures to address the incident and secure the systems that were involved. A third-party computer forensic firm was engaged as part of that investigation. The investigation determined that an unauthorized third-party acquired certain files stored on RIPTA's systems between August 3rd, 2021, and August 5th of 2021."

32. The Data Breach resulted in the unauthorized downloading of approximately forty-four thousand (44,000) data files (hereafter also referred to as "Data Files" or "Exfiltrated Data Files"), which contained PHI and PII of RIPTA employees and retirees as well as State of Rhode Island employees and retirees.

33. The Data Files had previously been sent to RIPTA by UHC, its prior healthcare plan administrator, and pertained to healthcare plan medical billing claims. The Data Files were not adequately encrypted and secured from unauthorized access by third parties.

34. At the Senate Oversight Hearing, Gary Jarvis, RIPTA's Chief Technology Officer, admitted, "Nothing was encrypted up to the point of the breach, and we are working on getting the proper software in place."

35. Senator Stephen R. Archambault, a member of the Senate Oversight Committee, asked the following question at the Senate Oversight Hearing: "The State employee data was incorrectly shared with RIPTA by a prior healthcare provider. Who was that healthcare provider?" Under oath, Gary Jarvis, RIPTA's Chief Technology Officer, responded: "UnitedHealthcare."

36. Scott Avedisian testified at the Senate Oversight Hearing, "We conducted a careful review of all the files that were identified pertaining to RIPTA's healthcare plan and the healthcare plan administrator." Scott Avedisian testified, "Among the files determined to be illegally acquired by the unauthorized third party were reports provided by RIPTA's former health plan administrator."

37. After conducting an internal investigation, it was not until October 28, 2021 – eighty-four (84) days after the discovery of the Breach – that RIPTA claimed that it determined

that the Breach had involved PHI and PII of current and former RIPTA and State of Rhode Island health insurance plan members and their families.

38. The Data Files provided by UHC to RIPTA included information not only for individuals insured under RIPTA's healthcare plan, which totaled roughly 5015 RIPTA insured individuals but also for approximately 17,000 individuals insured under the State of Rhode Island's healthcare plan who were not past or current RIPTA employees which totaled roughly 22,000 individuals affected by the Breach.

39. Scott Avedisian testified at the Senate Oversight Hearing, "In addition to containing information about our health plan participants, the reports also included information about individuals under the State organized health plan who were never insured under RIPTA's health plan. RIPTA no longer uses this health plan administrator, and RIPTA has communicated with them."

40. The PHI and PII downloaded by the hackers, which pertained to healthcare plan medical billing, contained the following information: plan member names, Social Security numbers, addresses, dates of birth, Medicare identification numbers and qualification information, health plan member identification numbers, healthcare claim amounts and dates of service for which claims were filed.

41. Senator Louis P. DiPalma asked the following question at the Senate Oversight Hearing: "What constitutes the kinds of data that would have been in that personally identifiable health information, PHI?" Steven Colantuono, RIPTA's Chief Legal Counsel, responded that "A combination, in some cases, of all or some of the following information, the person's name, date of birth, social security number, perhaps in some situations a Medicare identification number, in some situations a PCP or provider's name, and in some situations, the date of service along with

the cost relative to that service, meaning what the health care company paid for that service and we needed to reimburse."

42. Such data as Medicare identification numbers, providers' names, and dates of service expose an individual's healthcare history, diagnosis, condition, and treatment.

43. The data files that UHC gathered and wrongfully transmitted to RIPTA on behalf of State of Rhode Island employees included "confidential healthcare information," which consisted of State of Rhode Island employees' "healthcare history, diagnosis, condition, and treatment."

44. Since the data files that UHC wrongfully transmitted to RIPTA included health plan member identification numbers, healthcare claim amounts, and dates of service for which claims were filed, such data is considered "confidential healthcare information."

45. UHC released the "confidential healthcare information" to RIPTA without the written consent of the State of Rhode Island employees.

46. In a letter dated December 21, 2021 (attached as Exhibit "A" to this Complaint) – 138 days after first discovering the Breach, RIPTA notified 17,378 Rhode Island residents of the Breach pursuant to the State of Rhode Island laws. The exact scope of the Breach was initially believed to be limited to records from 2013 to 2015 but was later expanded to an undetermined point in 2020.

47. The letter of December 21, 2021, was generic, stating that that the Exfiltrated Data Files included "one or more of the following: address, date of birth, Medicare identification number and qualification information, health plan member identification number and claims information," and failed to identify whether the breached data of any particular individual was limited to PII or included PHI as well.

48. On or about December 21, 2021, RIPTA posted a notice about the breach on its website stating that the Exfiltrated Data Files were limited to the "personal information of our health plan beneficiaries," when RIPTA knew that the PHI and PII of non-RIPTA employees had been hacked as well.

49. On or about December 21, 2021, RIPTA provided information to the U.S. Department of Health and Human Services that five thousand fifteen (5,015) people were affected by the Breach even though the letter that individual victims received indicated that the incident involved seventeen thousand three hundred seventy-eight (17,378) individuals in the State of Rhode Island.

50. At the Senate Oversight Committee hearing, RIPTA revealed that roughly five thousand (5,000) out-of-state residents also had their information breached.

51. In response to the Senate Oversight Committee's request for information relating to the Breach, RIPTA prepared a document outlining the timeline of the Breach and actions taken after the Breach. See Exhibit "B" attached to this Complaint.

52. As participants in the State Plan and the RIPTA Plan, Plaintiffs, Class Members, and Subclass Members provided their PHI and PII to UHC or RIPTA with the reasonable expectation and the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access. Defendants' data security obligations were particularly important given the confidential nature of the healthcare information of the Plaintiffs, Class Members, and Subclass Members and given the substantial increase in national data breaches preceding the date of the Breach.

Federal Regulatory Data Security Standards

53. Federal statutes and regulations have put the Defendants on direct notice of the confidential nature of the information it maintained on the Plaintiffs, Class Members, and Subclass Members and the requirement to securely maintain the Class and Subclass Members' PHI and PII. The Health Insurance Portability and Accountability Act (hereafter also known as "HIPAA") was specifically enacted to protect sensitive patient PHI and PII from being disclosed without the patient's consent or knowledge.

54. HIPAA's "Privacy Rule" has long established national standards to protect individuals' medical records and other individually identifiable PHI and PII and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.

55. HIPAA's "Security Rule" also establishes national standards to protect individuals' electronic PHI created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI and PII.

56. RIPTA and UHC were aware of HIPAA's requirements and were subject to HIPAA's mandates to protect the PHI and PII of Plaintiffs, Class, and Subclass Members. The Security Rule specifies that electronic PHI and PII are subject to a series of "Implementation Specifications," one of which is encryption, to prevent unauthorized access. 45 CFR §164.312 (a)-(e).

57. In addition, according to HIPAA, a notice of a data breach must be made individually by first-class mail or e-mail (if authorized by the affected individual) without unreasonable delay and in no case later than sixty (60) days following the discovery of the data breach. In addition, if more than 500 residents of a state are affected, media notice must also be

provided within sixty (60) days of discovery. Moreover, if the covered entity has insufficient or out-of-date contact information for ten (10) or more individuals, the covered entity must provide individual substitute notice by either posting the notice on the home page of its website for at least ninety (90) days or by providing the notice in major print or broadcast media where the affected individuals likely reside. 45 CFR §164.404 (d)(2).

58. The notices sent by RIPTA failed to comply with HIPAA's sixty (60) day notice rule and thereby exposed the Plaintiffs, Class, and Subclass to a higher probability of identity theft or compromised financial accounts, as the time for them to take mitigating measures was delayed due to Defendants' lack of timely notice.

State Healthcare Data Security

59. In addition to HIPAA's requirements, the State of Rhode Island has enacted a privacy statute that also protects the PHI and PII of Plaintiffs, Class, and Subclass Members. The Identity Theft Protection Act of 2015 requires the Defendants to comply with the following:

a. implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information, and the purpose for which the information was collected in order to protect PHI and PII from unauthorized access, use, modification, destruction or disclosure and to preserve the confidentiality, integrity, and availability of such information (R.I. Gen. Laws § 11-49.3-2(a));

b. not retain PHI and PII for a period longer than is reasonably required to provide the services requested, to meet the purpose for which it was collected, or in accordance with a written retention policy or as may be required by law (R.I. Gen. Laws § 11-49.3-2(a));

c. destroy all PHI and PII, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure (R.I. Gen. Laws § 11-49.3-2(a)).

60. Under the statute, a data breach is defined as the "unauthorized access or acquisition of unencrypted computerized data information that compromises the security, confidentiality, or integrity of personal information maintained by the municipal agency, state agency or person." R.I. Gen. Laws § 11-49.3-3(a). The statute defines encryption as "the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and that "[d]ata shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would permit access to the encrypted data." R.I. Gen. Laws § 11-49.3-3(a).

61. That statute further requires that the Defendants notify the affected plan members ". . . in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d) of this section, . . ." Gen. Laws 1956, § 11-49.3-4(a)(2).

62. RIPTA, in its capacity as a self-insured plan, and UHC, as a third-party administrator of health insurance plans, were on direct notice of the applicable state and federal statutory and regulatory schemes mandating the protection of PHI and PII.

63. RIPTA and UHC, as active players in the healthcare industry, were acutely aware of the potential for a data breach and the foreseeable harm a data breach would cause to members.

64. Their level of awareness and need for compliance was heightened by the nature of the confidential information in their possession, which included the gold standard for hackers such as Social Security numbers, Medicare numbers, and dates of birth and the fact that there had been numerous publicized healthcare industry data hacks dating back to at least 2018. See, *Healthcare Data New Gold Standard for Hackers; Agencies Need to Be Ready for More Cyber Attacks*, https://www.accountsrecovery.net/ 2020/02/06/healthcare-data-new-gold-standard-for-hackers-agencies-need-to-be-ready-for-more-cyber-attacks/; *AMCA Healthcare Data Breach Could Set a New Precedent for Health IT Security*, CPO Magazine, Nicole Lindsey, June 26, 2019; *2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020*, HIPAA Journal, Steve Alder (January 19, 2021).

65. Despite this knowledge, the Defendants failed to adequately secure the Data Files in keeping with federal and state statutory and regulatory standards and requirements and standard healthcare industry data security requirements, resulting in unauthorized access and the subsequent Data Breach.

66. In addition, the Defendants failed to timely and adequately notify the affected plan members as required by federal and state law, thereby adding insult to injury and preventing the affected members from immediately attempting to mitigate potential losses and identify theft.

Sale of PHI and PII on the Dark Web

67. PHI and PII obtained by hackers are sold on the Dark Web. The Dark Web refers to a non-public portion of the Internet that cannot be accessed through the use of standard web browsers. Because of its anonymity, the Dark Web is used for criminal activity, such as the sale of confidential information to engage in identity theft.

68. Stolen PHI and PII data are listed for sale on the Dark Web. The stolen PHI and PII are then purchased by cyber criminals who use the information for identity theft and other illegal activity, such as accessing and withdrawing money from bank accounts, applying for fraudulent credit cards, and filing false requests for tax refunds, among other illegal activities.

69. The type of PHI and PII exfiltrated in the Data Breach is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

70. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name and get access to the individual's checking and savings accounts.

71. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

72. As described below, several of the named Plaintiffs have suffered some form of identity theft after and proximately caused by the Data Breach, as their PHI and/or PII has appeared and been purchased on the Dark Web and/or, more likely than not, based on the timing of their identity theft, was acquired on the Dark Web.

73. Given the type of PHI and PII obtained in the data breach and the fact that numerous Class and Subclass Members have already experienced incidents of identity theft or

attempted identity theft, all the named Plaintiffs, the Class, and the Subclass are at imminent risk of becoming victims of identity theft or unknown crimes as a result of the data breach.

Plaintiff Alexandra Morelli

74. Alexandra Morelli has worked at the University of Rhode Island since 2016. Alexandra Morelli is enrolled in the State Plan. In January of 2022, Alexandra Morelli received a notice from RIPTA regarding the Breach and signed up for the Equifax credit monitoring offered in the letter.

75. An unauthorized third-party purposefully obtained Morelli's PHI and PII.

76. Morelli's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

77. As a direct or indirect consequence of the Breach, Morelli has already been the victim of fraudulent activity.

78. Alexandra Morelli incurred the following as a direct and proximate result of the Breach:

a. January of 2022 – fraudulent transactions on her Kohl's credit card

b. February 2022 – suspicious activity on her Target and GAP credit cards

c. February 15th, February 23rd and March 8th – six withdrawals from her Citizen's bank savings account totaling $29,999.000 (February 15th for $5,000.00, February 23rd for $10,000.00, and March 8 for $14,999.00).

79. Alexandra Morelli was forced to cancel her debit and credit cards and put a stop on all withdrawals from her Citizen's bank account, which disrupted her ability to timely pay her bills, some of which were paid by electronic withdrawals from her Citizen's account.

80. Alexandra Morelli reported these incidents to RIPTA, the Attorney General's Office, the State Police, the Federal Trade Commission, and Citizen's Bank.

81. Alexandra Morelli has spent a great deal of time and effort canceling credit cards; and debit cards, contacting her banks, monitoring their financial accounts, reviewing and monitoring her credit reports, disputing unauthorized access, disputing unauthorized purchases, and battling identify theft, all as a direct and proximate result of the Data Breach.

82. An unauthorized third party purposely obtained Morelli's PHI and PII.

83. As a direct or indirect consequence of the Breach, further misuse of Morelli's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing his PHI and PII in the Breach would surely be for purposes of misusing his PHI and PII for fraud, identity theft, or other unknown crimes.

84. As a direct or indirect consequence of the Breach, Morelli has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

85. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of tangible harm from fraudulent activity.

86. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Morelli's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

87. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Morelli should not have to wait until an unauthorized third party commits further harm for Morelli to have the standing to sue.

Plaintiff David Novsam

88. David Novsam is a current RIPTA employee who has had a health insurance plan through RIPTA that UHC administered.

89. At some point during the end of December 2021, Novsam received a letter from RIPTA notifying him of the Breach and informing him that his PHI and PII had been accessed as part of the Breach.

90. An unauthorized third-party purposefully obtained Novsam's PHI and PII.

91. Novsam's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

92. As a direct or indirect consequence of the Breach, Novsam has already been the victim of fraudulent activity.

93. As a direct or indirect consequence of the Breach, in October of 2022, Discover Credit Card informed Novsam that as a result of a scan of thousands of Dark Websites, his personal information was found on the Dark Web. The Discover alert stated: "We found your personal info on a Dark Web site."

94. Novsam has received over thirty (30) text messages from his credit card security division alerting him that his PII was found on the Dark Web.

95. Additionally, as a direct or indirect consequence of the Breach, Novsam's wife has had credit card accounts opened in her name.

96. As a direct or indirect consequence of the Breach, further misuse of Novsam's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing his PHI and PII in the Breach would surely be for purposes of misusing his PHI and PII for fraud, identity theft, or other unknown crimes.

97. As a direct or indirect consequence of the Breach, Novsam has been harmed since he has already been subject to fraudulent activity and will be harmed further since he is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

98. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of tangible harm from fraudulent activity.

99. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Novsam's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

100. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Novsam should not have to wait until an unauthorized third party commits further harm for Novsam to have the standing to sue.

Plaintiff Audrey Snow

101. Audrey Snow is a State of Rhode Island employee who had a health insurance plan through the State of Rhode Island that UHC administered.

102. UHC unlawfully transferred Snow's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential

healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

103. UHC unlawfully transferred Snow's PHI to RIPTA, which contained confidential healthcare information which consisted of her healthcare history, diagnosis, condition, and treatment.

104. UHC unlawfully transferred Snow's PII to RIPTA, which contained her name, social security number, address, and date of birth.

105. An unauthorized third-party purposefully obtained Snow's PHI and PII.

106. As a direct or indirect consequence of the Breach, Snow has already been the victim of fraudulent activity. Snow had an unknown person attempting to steal her identity by filing for a change of address, opening a credit card in her name, and changing her address with one of her doctors. It can be inferred that her confidential information has already been posted for sale on the Dark Web, has been purchased, and resulted in identity theft.

107. Snow's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web." This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

108. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

109. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

110. As a direct or indirect consequence of the Breach, Snow has already been the victim of fraudulent activity.

111. As a direct or indirect consequence of the Breach, someone tried to steal Snow's identity, file a change of her address, open a credit card in her name, and change her address with one of her doctors.

112. The change of address with one of her doctors is evidence that her PHI was illegally accessed and used for fraudulent activity.

113. As a direct or indirect consequence of the Breach, further misuse of Snow's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

114. As a direct or indirect consequence of the Breach, Snow has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

115. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

116. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Snow's risk of future harm moves from mere speculation to sufficiently imminent.

The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

117. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Snow should not have to wait until an unauthorized third party commits further harm for Snow to have the standing to sue.

Plaintiff Betty J. Potenza

118. Betty J. Potenza is a current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island that UHC administered.

119. At some point during the end of December 2021, Potenza received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

120. An unauthorized third-party purposefully obtained Potenza's PHI and PII.

121. Betty J. Potenza has had her Citizens checking account hacked for eleven thousand six hundred and fifty-eight dollars and forty-three cents ($11,658.43) between October 14, 2022, and October 20, 2022, via a series of nine withdrawals from her account, which ranged from 5 cents to $5,000. The first unauthorized withdrawals on October 14, 2022, were for 5 cents, 17 cents, and 22 cents, where it appears the perpetrator was testing to determine if he could access her account funds. After the October 14, 2022, withdrawals, the perpetrator escalates to $657.99, $500.00, $5,000.00, $500.00, $2,000.00, and $3,000.00.

122. Potenza's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

123. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security

numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

124. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

125. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

126. UHC unlawfully transferred Potenza's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

127. UHC unlawfully transferred Potenza's PII to RIPTA, which contained her name, social security number, address, and date of birth.

128. As a direct or indirect consequence of the Breach, she has already been the victim of fraudulent activity.

129. As a direct or indirect consequence of the Breach, further misuse of Potenza's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

130. As a direct or indirect consequence of the Breach, Potenza has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

131. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

132. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Potenza's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

133. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Potenza should not have to wait until an unauthorized third party commits further harm for Potenza to have the standing to sue.

Plaintiff Norman R. Plante

134. Norman R. Plante is a current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island that UHC administered.

135. At some point during the end of December 2021, Plante received a letter from RIPTA notifying him of the Breach and informing him that his PHI and PII had been accessed as part of the Breach.

136. An unauthorized third-party purposefully obtained Plante's PHI and PII.

137. Plante's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

138. The Dark Web refers to websites where stolen data is exchanged.

139. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

140. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

141. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

142. UHC unlawfully transferred Plante's PHI to RIPTA, which included his health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include his healthcare history, diagnosis, condition, and treatment.

143. UHC unlawfully transferred Plante's PHI to RIPTA, which contained confidential healthcare information which consisted of his healthcare history, diagnosis, condition, and treatment.

144. UHC unlawfully transferred Plante's PII to RIPTA, which contained his name, social security number, address, and date of birth.

145. As a direct or indirect consequence of the Breach, Plante has already been the victim of fraudulent activity.

146. In September of 2022, Plante noticed a hard inquiry on his credit report for a credit card from Premier Bank of Vegas.

147. Plante had not applied for a credit card from Premier Bank of Vegas. He contacted Premier Bank of Vegas and was able to stop the issuance of a credit card in his name.

148. Hard inquiries negatively affect credit scores. Plante requested that the hard inquiry be removed. To consider removing the hard inquiry, Premier Bank required Plante to first submit: a) a copy of a police report or an FTC Theft Report; b) a copy of a paystub or W-2; c) a signed and dated letter from your employer on company letterhead; d) his birth certificate or a copy of a government-issued identification card.

149. On November 7, 2022, Plante mailed Premier Bank the required paperwork and awaits to see if his credit will be restored.

150. As a direct or indirect consequence of the Breach, further misuse of Plante's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing his PHI and PII in the Breach would surely be for purposes of misusing his PHI and PII for fraud, identity theft, or other unknown crimes.

151. As a direct or indirect consequence of the Breach, Plante has been harmed since he has already been subject to fraudulent activity and will be harmed further since he is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

152. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

153. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Plante's risk of future harm moves from mere speculation to sufficiently

imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

154. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Plante should not have to wait until an unauthorized third party commits further harm for Plante to have the standing to sue.

Plaintiff Eileen Botelho

155. Eileen Botelho is a current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island that UHC administered.

156. At some point during the end of December 2021, Botelho received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

157. An unauthorized third-party purposefully obtained Botelho's PHI and PII.

158. On or about July 19-20, 2022, Botelho was notified by Citizens Bank of unusual activity on her and her husband's checking account. Her personal checking account showed an $18,000.00 payment from her checking account to a Chase credit card. Botelho had not made the $18,000.00 payment, and she did not have a Chase credit card.

159. In the Fall of 2022, Botelho experienced suspicious activity in her Discover Credit Card and Mastercard hacked and canceled both accounts. Both accounts had to be closed out with new cards being issued.

160. Botelho's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

161. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security

numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

162. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

163. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

164. UHC unlawfully transferred Botelho's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

165. UHC unlawfully transferred Botelho's PII to RIPTA, which contained her name, social security number, address, and date of birth.

166. As a direct or indirect consequence of the Breach, Botelho has already been the victim of fraudulent activity.

167. As a direct or indirect consequence of the Breach, further misuse of Botelho's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

168. As a direct or indirect consequence of the Breach, Botelho has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

169. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

170. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Botelho's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

171. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Botelho should not have to wait until an unauthorized third party commits further harm for Botelho to have the standing to sue.

Plaintiff Gary Ruo

172. Gary Ruo is a State of Rhode Island retiree who has had a health insurance plan through the State of Rhode Island that UHC administered.

173. At some point during the end of December 2021, Ruo received a letter from RIPTA notifying him of the Breach and informing him that his PHI and PII had been accessed as part of the Breach.

174. An unauthorized third-party purposefully obtained Ruo's PHI and PII.

175. On or about January 26, 2022, Equifax notified Ruo that "Your Social Security number was found on a fraudulent internet trading site." Equifax had conducted a search of "fraudulent internet trading sites" and found Ruo's Social Security number for sale.

176. After receiving notice from Equifax, Ruo paid $180 to purchase an identify protection plan from Aura to prevent identity theft.

177. Ruo's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

178. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

179. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

180. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

181. UHC unlawfully transferred Ruo's PHI to RIPTA, which included his health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include his healthcare history, diagnosis, condition, and treatment.

182. UHC unlawfully transferred Ruo's PII to RIPTA, which contained his name, social security number, address, and date of birth.

183. As a direct or indirect consequence of the Breach, further misuse of Ruo's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing his PHI and PII in the Breach would surely be for purposes of misusing his PHI and PII for fraud, identity theft, or other unknown crimes.

184. As a direct or indirect consequence of the Breach, Ruo has been harmed since he has already been subject to fraudulent activity and will be harmed further since he is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

185. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

186. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Ruo's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

187. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Ruo should not have to wait until an unauthorized third party commits further harm for Ruo to have the standing to sue.

Plaintiff David A. Rosa

188. David A. Rosa is a current State of Rhode Island employee who has had a health insurance plan through the

189. State of Rhode Island that UHC administered.

190. At some point during the end of December 2021, Rosa received a letter from RIPTA notifying him of the Breach and informing him that his PHI and PII had ben accessed as part of the Breach.

191. An unauthorized third-party purposefully obtained Rosa's PHI and PII.

192. Rosa's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

193. The Dark Web refers to websites where stolen data is exchanged.

194. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

195. UHC unlawfully transferred Rosa's PHI to RIPTA, which included his health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include his healthcare history, diagnosis, condition, and treatment.

196. UHC unlawfully transferred Rosa's PII to RIPTA, which contained his name, social security number, address, and date of birth.

197. As a direct or indirect consequence of the Breach, further misuse of Rosa's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing his PHI and PII in the Breach would surely be for purposes of misusing his PHI and PII for fraud, identity theft, or other unknown crimes.

198. As a direct or indirect consequence of the Breach, Rosa will be harmed since he is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

199. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

200. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Rosa's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

201. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Rosa should not have to wait until an unauthorized third party commits further harm for Rosa to have the standing to sue.

202. Due to the fear of identity theft after the Data Breach, Rosa purchased an "Identity Guard" monitoring service for $160 per year. His plan was renewed in January 2023, which required another $160 payment.

Plaintiff Robin Kulik

203. Robin Kulik is a State of Rhode Island retiree who has had a health insurance plan through the State of Rhode Island that UHC administered.

204. At some point during the end of December 2021, Kulik received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

205. An unauthorized third-party purposefully obtained Kulik's PHI and PII.

206. After the Data Breach, Credit Karma and McAfee informed Kulik that her PII was on the dark web.

207. Kulik's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

208. The Dark Web refers to websites where stolen data is exchanged.

209. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

210. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

211. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

212. UHC unlawfully transferred Kulik's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

213. UHC unlawfully transferred Kulik's PII to RIPTA, which contained her name, social security number, address, and date of birth.

214. As a direct or indirect consequence of the Breach, further misuse of Kulik's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

215. As a direct or indirect consequence of the Breach, Kulik has been harmed since her PII is on the Dark Web, and she will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

216. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

217. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Kulik's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

218. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Kulik should not have to wait until an unauthorized third party commits further harm for Kulik to have the standing to sue.

219. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Kulik should not have to wait until an unauthorized third party commits further harm for Kulik to have the standing to sue.

Plaintiff Caronah Cassell-Johnson

220. Caronah Cassell-Johnson is a Current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island UHC administered.

221. At some point during the end of December 2021, Cassell-Johnson received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

222. An unauthorized third-party purposefully obtained Cassell-Johnson's PHI and PII.

223. Cassell-Johnson's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

224. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

225. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

226. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

227. UHC unlawfully transferred Cassell-Johnson's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

228. UHC unlawfully transferred Cassell-Johnson's PII to RIPTA, which contained her name, social security number, address, and date of birth.

229. As a direct or indirect consequence of the Breach, Cassell-Johnson has already been the victim of fraudulent activity.

230. After the Data Breach, Cassell-Johnson could not file her Federal and State taxes electronically because a third party fraudulently filed tax returns in her name.

231. As a direct or indirect consequence of the Breach, further misuse of Cassell-Johnson's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

232. As a direct or indirect consequence of the Breach, Cassell-Johnson has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

233. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

234. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Cassell-Johnson's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

235. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Cassell-Johnson should not have to wait until an unauthorized third party commits further harm for Casell-Johnson to have the standing to sue.

Plaintiff Sheila M. Galamaga

236. Sheila M. Galamaga is a current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island that UHC administered.

237. At some point during the end of December 2021, Galamaga received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

238. An unauthorized third-party purposefully obtained Galamaga's PHI and PII.

239. After the Breach, false accounts were set up in Galamaga's name through Stash. There were several attempts to do wire transfers from her checking account. In addition to having access to her bank account number, the cyber criminal had access to Galamaga's Social Security number and date of birth.

240. She had to close her bank account and open an account at a different bank. She had to discard five hundred newly purchased checks from the closed account since they were no longer valid.

241. Galamaga's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

242. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

243. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply

for loans in the individual's name, and get access to the individual's checking and savings accounts.

244. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

245. UHC unlawfully transferred Galamaga's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

246. UHC unlawfully transferred Galamaga's PII to RIPTA, which contained her name, social security number, address, and date of birth.

247. As a direct or indirect consequence of the Breach, Galamaga has already been the victim of fraudulent activity.

248. As a direct or indirect consequence of the Breach, further misuse of Galamaga's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

249. As a direct or indirect consequence of the Breach, Galamaga has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

250. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

251. Since other Plaintiffs have already suffered tangible harm due to the Breach, the imminence of Galamaga's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

252. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Galamaga should not have to wait until an unauthorized third party commits further harm for Galamaga to have the standing to sue.

Plaintiff Caitlyn Lamarre

253. Caitlyn Lamarre is a current State of Rhode Island employee who has had a health insurance plan through the State of Rhode Island that UHC administered.

254. At some point during the end of December 2021, Lamarre received a letter from RIPTA notifying her of the Breach and informing her that her PHI and PII had been accessed as part of the Breach.

255. An unauthorized third-party purposefully obtained Lamarre's PHI and PII.

256. Lamarre's bank account was accessed, and the cybercriminal attempted to wire money out of her account. Lamarre was able to get to the bank in time to stop the withdrawals. However, she had to close her bank account and open a new bank account. Due to the opening of a new bank account, all her automatic bill payments were terminated when the old account was closed. Accordingly, some of her automatic payments were denied resulting in monetary penalties on some returned payments.

257. Lamarre's sensitive PHI and PII are the type of information that are highly sought after on the "Dark Web."

258. This type of PHI and PII is the type of data that likely subjects individuals to a perpetual risk of identity theft or fraud. Particularly sensitive forms of data like social security numbers and dates of birth make it more likely that individuals will be subject to future identity theft or fraud.

259. Social Security numbers and dates of birth can be used to create financial havoc for individuals. Once an unauthorized third party has an individual's social security number and other pieces of PII, they can open credit cards and bank accounts in the individual's name, apply for loans in the individual's name, and get access to the individual's checking and savings accounts.

260. Obtaining an individual's social security number and then associating the social security number with other pieces of PII that may exist on the Dark Web can indirectly result in an individual suffering fraudulent activity and identity theft.

261. As a direct or indirect consequence of the Breach, Lamarre has already been the victim of fraudulent activity.

262. UHC unlawfully transferred Lamarre's PHI to RIPTA, which included her health plan member identification number and claims information, which is considered confidential healthcare information since it necessarily would have to include her healthcare history, diagnosis, condition, and treatment.

263. UHC unlawfully transferred Lamarre's PII to RIPTA, which contained her name, social security number, address, and date of birth.

264. As a direct or indirect consequence of the Breach, further misuse of Lamarre's PHI and PII for fraudulent and identity theft purposes is "imminent" since the purpose of the

intentional act of accessing her PHI and PII in the Breach would surely be for purposes of misusing her PHI and PII for fraud, identity theft, or other unknown crimes.

265. As a direct or indirect consequence of the Breach, Lamarre has been harmed since she has already been subject to fraudulent activity and will be harmed further since she is now exposed to an actual, imminent, and substantial ongoing risk of future fraud and identity theft since the threatened future injury is certainly impending.

266. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of fraudulent activity.

267. Since other Plaintiffs have already suffered tangible harm as a result of the Breach, the imminence of Lamarre's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

268. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Lamarre should not have to wait until an unauthorized third party commits further harm for Lamarre to have the standing to sue.

Plaintiff Diane M. Cappalli

269. Diane M. Cappalli was a RIPTA employee enrolled in RIPTA's healthcare insurance plan at the time of the Breach. Cappalli has since retired from RIPTA. At retirement, Cappalli held the position of scheduling coordinator. At some point in time during the last couple of weeks in December of 2021, Cappalli received notice from RIPTA regarding the Branch.

270. As a direct or indirect consequence of the Breach, Cappalli has been harmed as her confidential information, like the other names Plaintiffs' confidential information, has been

exposed to the Dark Web. Other Plaintiffs in this lawsuit have already had their PHI and PII misused, as evidenced by the specific allegations of tangible harm from fraudulent activity.

271. Since other Plaintiffs have already suffered tangible harm due to the Breach and the exfiltrated data is for sale on the Dark Web, the imminence of Cappalli's risk of future harm moves from mere speculation to sufficiently imminent. The increased risk of future harm should be sufficient to establish injury-in-fact for standing purposes.

272. Since there is an imminent risk of future harm from fraudulent activity and identity theft, Cappelli should not have to wait until an unauthorized third party commits further harm for Cappelli to have the standing to sue.

CLASS ALLEGATIONS

273. Plaintiffs bring this putative class action lawsuit on behalf of themselves and on behalf of all other persons similarly situated. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

274. All persons whose PHI and/or PII was maintained in or on RIPTA's system or in Data Files in possession of RIPTA that were accessed in the Data Breach (hereafter also referred to as "RIPTA Plan Class" or "Class" or "Class Members"). David Novsam and Diane M. Cappalli seek to represent the Class.

275. The Plaintiffs also propose the following Subclass:

276. All persons who were not members or beneficiaries of the RIPTA Plan whose PHI and/or PII were sent or transferred to RIPTA by UHC and accessed in the Data Breach (hereafter also referred to as "United Non-RIPTA Plan Subclass" or "Subclass" or "Subclass Members"). Alexandra Morelli, Audrey Snow, Betty J. Potenza, Norman R. Plante, Eileen Botelho, Gary

Ruo, David A. Rosa, Robin Kulik, Caronah Cassell-Johnson, Sheila M. Galamaga, Caitlyn Lamarre seek to represent the Subclass.

277. Excluded from the Class and Subclass are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Also excluded from the Class and Subclass are members of the judiciary to whom this case is assigned, their families, and their staff members.

278. **Numerosity**. The Class Members and Subclass Members are so numerous that joinder of all of them is impracticable. While the exact number of Class Members and Subclass Members is unknown to Plaintiffs at this time, based on information and belief, the Class and Subclass consists of over 17,000 individuals whose PHI and PII were compromised in the Data Breach.

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

a. Whether the Defendants unlawfully maintained, stored, or disclosed the PHI and PII of Class Members and Subclass Members;

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

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

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

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

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

g. Whether computer hackers obtained Class Members' and Subclass Members' PHI and PII in the Data Breach;

h. Whether the Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs, Class Members, and Subclass Members suffered legally cognizable injuries as a result of the Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants failed to provide notice of the Data Breach in an adequate and timely manner; and

l. Whether Plaintiffs, Class Members, and Subclass Members are entitled to damages, civil penalties, and injunctive relief.

280. **Typicality.** The Plaintiffs' claims are typical of those of other Class Members and Subclass Members because the Plaintiffs' information, like that of every other Class Member and Subclass Member, was compromised in the Data Breach.

281. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members and Subclass Members. Plaintiffs' attorneys are competent and experienced in class action litigation.

282. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiffs, the Class Members, and the Subclass Members, in that all of Plaintiffs', Class members', and Subclass Members' PHI and PII were stored on the same computer system or in the same Data Files and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members and Subclass Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has significant and desirable advantages for judicial economy.

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

284. Defendants have acted on grounds that generally apply to the Class Members and Subclass Members as a whole so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a classwide basis.

COUNT 1
Violations of the Identity Theft Protection Act, Gen. Laws § 11-49-3-1, et seq.
(As to RIPTA and UHC)

285. Plaintiffs allege and incorporate the allegations in all of this complaint's preceding paragraphs as though fully set forth therein.

286. The Plaintiffs, the Class, and the Subclass enrolled in health insurance plans offered by RIPTA or the State of Rhode Island, both of which, at all times relevant hereto, were administered by UHC.

287. In enrolling in their plans, obtaining covered medical services under the plans, and paying for their share of medical bills, the Plaintiffs, the Class, and the Subclass were required to provide PHI and PII to UHC and their respective plans. Such information included, but was not limited to, names, addresses, dates of birth, health information, and Social Security numbers for plan members and plan beneficiaries.

288. At some point, UHC sent or otherwise transferred Data Files to RIPTA, which contained PHI and PII of the Plaintiffs, the Class, and the Subclass. The Data Files included PHI and PII for current RIPTA employees, RIPTA retirees, and RIPTA family members of RIPTA employees and retirees, as well as PHI and PII for State of Rhode Island current employees, State of Rhode Island retirees, and family members of State of Rhode Island employees and retirees who had no affiliation with RIPTA and were not members of the RIPTA Plan.

289. R.I. Gen. Laws § 11-49.3-2(a) requires that any agency or business "that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program which contains reasonable security procedures and practices appropriate to the size and scope of the organization, the nature of the information and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction or disclosure and to preserve the confidentiality, integrity, and

availability of such information." Moreover, any agency or business "shall not retain personal information for a period longer than is reasonably required to provide the services requested, to meet the purpose for which it was collected, or in accordance with a written retention policy or as may be required by law."

290. Pursuant to the statute, "'encrypted' means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key." R. I. Gen. Laws § 11-49.3-3(a).

291. UHC sent or otherwise transferred information protected by State statute to RIPTA, which was not adequately secured or encrypted as required by State statute.

292. As part of this transfer, UHC sent RIPTA the PHI and PII of State Plan members and beneficiaries without authorization, as they were not members or beneficiaries of the RIPTA Plan, ignored or failed to notice its error, and also failed to recall the unauthorized data and information it had sent. In addition, the information that UHC transferred was not adequately secured or encrypted. Therefore, UHC's acts and omissions constituted violations of R. I. Gen. Laws § 11-49.3-4(a)(1).

293. RIPTA received the PHI and PII of the Plaintiffs, the Class, and the Subclass and failed to adequately secure the Data Files. In addition, RIPTA and UHC retained all or part of the data in their systems for longer than reasonably required by statute to effectuate the requested or necessary services.

294. In August of 2021, RIPTA's systems were hacked, and the data provided by UHC to RIPTA was accessed and downloaded by hackers. The hackers obtained approximately

44,000 files on approximately 5,000 RIPTA Plan members and beneficiaries and 17,000 State Plan members and beneficiaries.

295. The Identity Theft Prevention Act also requires that an entity that is the subject of a data breach notify affected persons "in the most expedient time possible but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements in subsection (d) . . ." R.I. Gen. Laws § 11-49.3-4(a)(2).

296. RIPTA discovered the data breach on or about August 5, 2021, but did not send notice until December 21, 2021 – 138 days after first discovering the Data Breach. As a result, the notice was sent well beyond the statutory forty-five (45) day deadline.

297. The above-described acts and omissions constituted violations of R. I. Gen. Laws § 11-49.3-1, et seq.

298. As a direct and proximate result of the Defendants' statutory violations, the Plaintiffs, the Class, and the Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of money due to unauthorized deductions or use of their bank accounts and credit card accounts; (iii) the loss of the opportunity of how their PHI and PII is used; (iv) the compromise, publication, and/or theft of their PHI and PII; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII; (vi) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vii) costs associated with placing freezes on credit reports; (viii) damage to their credit; (ix) the

continued risk to their PHI and PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former customers' PHI and PII in their continued possession; (x) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PHI and PII as a result of the Data Breach for the remainder of the lives of Plaintiffs, the Class Members, and the Subclass Members; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

299. In addition, as a direct and proximate result of Defendants' negligence and negligence per se, Plaintiffs, the Class, and the Subclass have suffered and will continue to suffer other forms of injury or harm, including, but not limited to, anxiety, loss of privacy, and other economic and non-economic losses.

300. Moreover, as a direct and proximate result of Defendants' statutory violations, Plaintiffs, the Class, and the Subclass have suffered and will suffer the continued risks of exposure of their PHI and PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI and PII in its continued possession.

COUNT 2
Violations of the Confidentiality of Health Care Communications and Information Act, Gen. Laws § 5-37. 3-1, et seq.
(As to UHC with Respect to the State Plan)

301. Plaintiffs allege and incorporate by reference the allegations in all of this Complaint's preceding paragraphs as though fully set forth therein.

302. The Plaintiffs and the Subclass enrolled in health insurance plans offered by RIPTA or the State of Rhode Island, both of which, at all times relevant hereto, was administered by UHC.

303. In enrolling in their plans, obtaining covered medical services under the plans, and paying for their share of medical bills, the Plaintiffs and the Subclass were required to provide PHI and PII to UHC and their respective plans. Such information included, but was not limited to, names, addresses, dates of birth, health information, and Social Security numbers for plan members and plan beneficiaries.

304. At some point, UHC sent or otherwise transferred Data Files to RIPTA, which contained the PHI and PII of the Plaintiffs and the Subclass. The Data Files included PHI and PII for current and past RIPTA employees and RIPTA retirees, as well as PHI and PII for current employees, past employees, and retirees of the State of Rhode Island.

305. R.I. Gen. Laws § 5-37. 3-4(a)(1) expressly states that a patient's confidential healthcare information shall not be released or transferred without the written consent of the patient or his or her authorized representative.

306. RIPTA, as a separate and distinct entity administering a separate health insurance plan, was not authorized or otherwise entitled to receive confidential healthcare information about members and beneficiaries of the State Plan.

307. Despite this fact, UHC sent or otherwise transferred confidential healthcare information of State Plan members and beneficiaries without authorization, ignored or failed to notice its error, and also failed to recall the unauthorized data and information it had sent. In addition, the information that UHC transferred was not encrypted or properly secured. UHC's acts and omissions constituted violations of R. I. Gen. Laws § 5-37. 3-4(a)(1).

308. In August of 2021, RIPTA's systems were hacked, and the data provided by UHC to RIPTA, including the confidential healthcare information of members and beneficiaries of the State Plan, were accessed and downloaded by hackers.

309. As a direct and proximate result of UHC's statutory violations, the Plaintiffs and the Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of money due to unauthorized deductions or use of their bank accounts and credit card accounts; (iii) the loss of the opportunity of how their PHI and PII is used; (iv) the compromise, publication, and/or theft of their PHI and PII; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII; (vi) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vii) costs associated with placing freezes on credit reports; (viii) damage to their credit; (ix) the continued risk to their PHI and PII, which remains in UHC's possession and is subject to further unauthorized disclosures so long as UHC fails to undertake appropriate and adequate measures to protect the current and former customers' PHI and PII in its continued possession; (x) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PHI and PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Subclass; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

310. In addition, as a direct and proximate result of UHC's negligence and negligence per se, the Plaintiffs and the Subclass have suffered and will continue to suffer other forms of

injury and harm, including, but not limited to, anxiety, loss of privacy, and other economic and non-economic losses.

311. Moreover, as a direct and proximate result of UHC's statutory violations, the Plaintiffs and the Subclass have suffered and will suffer the continued risks of exposure of their PHI and PII, which remains in UHC's possession and is subject to further unauthorized disclosures so long as UHC fails to undertake appropriate and adequate measures to protect the PHI and PII in its continued possession.

COUNT 3
NEGLIGENCE
(As to RIPTA)

312. Plaintiffs allege and incorporate by reference the allegations in all of this Complaint's preceding paragraphs as though fully set forth therein.

313. The Plaintiffs, the Class, and the Subclass enrolled in health insurance plans offered by RIPTA or the State of Rhode Island, both of which, at all times relevant hereto, were administered by UHC.

314. In enrolling in their plans, obtaining covered medical services under the plans, and paying for their share of medical bills, the Plaintiffs, the Class, and the Subclass were required to provide PHI and PII to UHC and their respective plans. Such information included, but was not limited to, names, addresses, dates of birth, health information, and Social Security numbers for plan members and plan beneficiaries.

315. At some point, UHC sent or otherwise transferred Data Files to RIPTA, which contained PHI and PII of the Plaintiffs, the Class, and the Subclass. The Data Files included PHI and PII for current RIPTA employees, past RIPTA employees, RIPTA retirees, and their families, as well as PHI and PII for current State of Rhode Island Employees, past State of Rhode Island employees, retirees, and their families.

316. RIPTA, in its capacity as a self-insured healthcare plan, knew that the data and information provided by UHC in the Data Files were highly confidential information, which was protected by HIPAA, state law, and the general standards for the protection and security of confidential employee PHI and PII.

317. RIPTA owed a duty of reasonable care to the Plaintiffs, the Class, and the Subclass to maintain, protect, store, and then purge and destroy the data securely as required by federal and state law and industry standards.

318. RIPTA breached the duty of care it owed to the Plaintiffs, the Class, and the Subclass when it failed to safeguard, secure, and encrypt the data upon and after receipt from UHC and also failed to purge and destroy the data after receipt and use, thereby enabling an unauthorized person or entity to access and download the data.

319. As a direct and proximate result of RIPTA's breach of reasonable care, the Plaintiffs, the Class, and the Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of money due to unauthorized deductions or use of their bank accounts and credit card accounts; (iii) the loss of the opportunity of how their PHI and PII is used; (iv) the compromise, publication, and/or theft of their PHI and PII; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII; (vi) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vii) costs associated with placing freezes on credit reports; (viii) damage to their credit; (ix) the continued risk to their PHI and PII, which remains in RIPTA's possession and is subject to

further unauthorized disclosures so long as RIPTA fails to undertake appropriate and adequate measures to protect the current and former customers' PHI and PII in its continued possession; (x) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PHI and PII as a result of the Data Breach for the remainder of the lives of Plaintiffs, the Class, and the Subclass; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

320. As a direct and proximate result of RIPTA's negligence and negligence per se, the Plaintiffs, the Class, and the Subclass have suffered and will continue to suffer other forms of injury and harm, including, but not limited to, anxiety, emotional distress, loss of privacy, economic, and non-economic losses.

321. Additionally, as a direct and proximate result of RIPTA's negligence and negligence per se, the Plaintiffs, the Class, and the Subclass have suffered and will suffer the continued risks of exposure of their PHI and PII, which remains in RIPTA's possession and is subject to further unauthorized disclosures so long as RIPTA fails to undertake appropriate and adequate measures to protect the PHI and PII in its continued possession.

322. As a direct and proximate result of RIPTA's negligence and negligence per se, the Plaintiffs, the Class, and the Subclass are now at an increased risk of identity theft or fraud.

323. As a direct and proximate result of RIPTA's negligence and negligence per se, the Plaintiffs, the Class, and the Subclass are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT 4
NEGLIGENCE
(As to UHC)

324. Plaintiffs allege and incorporate by reference the allegations in all of this Complaint's preceding paragraphs as though fully set forth therein.

325. The Plaintiffs and the Subclass enrolled in health insurance plans offered by RIPTA or the State of Rhode Island, both of which, at all times relevant hereto, was administered by UHC.

326. In enrolling in their plans, obtaining covered medical services under the plans, and paying for their share of medical bills, the Plaintiffs and the Subclass were required to provide PHI and PII to UHC and their respective plans. Such information included, but was not limited to, names, addresses, dates of birth, health information, and Social Security numbers for plan members and plan beneficiaries.

327. At some point, UHC sent or otherwise transferred Data Files to RIPTA, which contained the PHI and PII of the Plaintiffs and the Subclass. The Data Files included PHI and PII for current RIPTA employees, past RIPTA employees, retirees, and their families, as well as PHI and PII for current State of Rhode Island employees, past State of Rhode Island employees, retirees, and their families.

328. The Data Files presumably also included PHI and PII for plan beneficiaries who were family members of employees.

329. UHC, in its contractual role as an administrator of both plans and as an established plan administrator in the healthcare industry, knew that the data and information provided by UHC in the Data Files were highly confidential information protected by HIPAA and state law.

330. Therefore, UHC owed a duty of reasonable care to the Plaintiffs and the Subclass to safeguard, maintain, store, purge, and destroy the data securely as required by federal and state law, their contracts with the State of Rhode Island, and RIPTA, and industry standards.

331. UHC breached the duty of care it owed to the Plaintiffs and the Subclass when it failed to adequately secure and encrypt the data it sent to RIPTA, included non-RIPTA employee data in the file transfer, and failed to purge or destroy the non-RIPTA state and quasi-state employee data from its files, thereby enabling an unauthorized person or entity to access and download the data.

332. As a direct and proximate result of UHC's breach of reasonable care, the Plaintiffs and the Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of money due to unauthorized deductions or use of their bank accounts and credit card accounts; (iii) the loss of the opportunity of how their PHI and PII is used; (iv) the compromise, publication, and/or theft of their PHI and PII; (v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII; (vi) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vii) costs associated with placing freezes on credit reports; (viii) damage to their credit; (ix) the continued risk to their PHI and PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as UHC fails to undertake appropriate and adequate measures to protect the current and former customers' PHI and PII in its continued possession; (x) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PHI and PII as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Subclass; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

333. As a direct and proximate result of UHC's negligence and negligence per se, Plaintiffs and the Subclass have suffered and will continue to suffer other forms of injury and harm, including, but not limited to, anxiety, emotional distress, loss of privacy, economic, and non-economic losses.

334. Additionally, as a direct and proximate result of UHC's negligence and negligence per se, the Plaintiffs and the Subclass have suffered and will suffer the continued risks of exposure of their PHI and PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as UHC fails to undertake appropriate and adequate measures to protect the PHI and PII in its continued possession.

335. As a direct and proximate result of UHC's negligence and negligence per se, the Plaintiffs are now at an increased risk of identity theft or fraud.

336. As a direct and proximate result of UHC's negligence and negligence per se, the Plaintiffs and the Subclass are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT 5
BREACH OF CONTRACT
(As to UHC)

337. Plaintiffs incorporate the preceding paragraphs as though fully stated herein.

338. UHC, through its written privacy notices, made a uniform offer to Plaintiffs and the Subclass regarding the quality and merit of its privacy policies, including that customer health and personal financial information would remain confidential, that access to such information would be limited to certain defined purposes and that such information would not be disclosed to third parties other than those defined in the notices.

339. By enrolling as members in UHC-administered health plans, the Plaintiffs and the Subclass accepted UHC's offer, resulting in a binding contract.

340. UHC breached its promises to Plaintiffs and the Subclass Members by a) failing to maintain the promised safeguards to keep their data confidential and/or encrypt the data when it was sent to RIPTA, b) sending data on non-RIPTA employees to RIPTA, c) failing to audit its practices to prevent and/or timely discover the disclosure of unencrypted data and/or data for non-RIPTA employees to RIPTA. As a direct and proximate result of UHC's breaches of contract, the Plaintiffs and the Subclass Members, as alleged above, have suffered damages in amounts to be proven at trial.

COUNT 6
BREACH OF IMPLIED CONTRACT
(As to UHC)

341. Plaintiffs incorporate the preceding paragraphs as though fully stated herein.

342. Through their course of conduct, UHC, Plaintiffs, and Subclass Members entered into implied contracts for UHC to implement data security adequate to safeguard and protect the Plaintiffs' and Subclass Members' health and personal financial information, the privacy of role as plan administrator and through it written privacy notices, made a uniform offer to Plaintiffs and the Subclass regarding the quality and merit of its privacy policies, including that customer health and personal financial information would remain confidential, that access to such information would be limited to certain defined purposes and that such information would not be disclosed to third parties other than those defined in the notices.

343. By enrolling as members in UHC-administered health plans, the Plaintiffs and the Subclass accepted UHC's offer, resulting in an implied contract.

344. UHC breached its promises to the Plaintiffs and the Subclass Members by a) failing to maintain the promised safeguards to keep their data confidential and/or encrypt the data when it was sent to RIPTA, b) sending data on non-RIPTA employees to RIPTA, c) failing to audit its practices to prevent and/or timely discover the disclosure of unencrypted data and/or data for non-RIPTA employees to RIPTA. As a direct and proximate result of UHC's breaches of contract, the Plaintiffs and the Subclass Members, as alleged above, have suffered damages in amounts to be proven at trial.

345. As a direct and proximate cause of the said breach, the Plaintiffs and the Subclass Members have suffered damages as described above.

COUNT 7
RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT
(As to UHC)

346. UHC committed unfair or deceptive acts within the meaning of the Rhode Island Deceptive Trade Practices Act. 6 R.I. Gen. Laws Ann. § 6-13.1-1 *et seq*.

347. UHC committed acts that 1) represented that its services had characteristics, benefits, and qualities that they did not have, 6 R.I. Gen. Laws Ann. § 6-13.1-1(6)(v); and 2) represented that its services were of a particular standard, quality, or grade when they were another, 6 R.I. Gen. Laws Ann. § 6-13.1-1(6)(vii).

348. UHC committed acts that 1) represented that its services had characteristics, benefits, and qualities that they did not have, 6 R.I. Gen. Laws Ann. § 6-13.1-1(6)(v); and 2) represented that its services were of a particular standard, quality, or grade when they were another, 6 R.I. Gen. Laws Ann. § 6-13.1-1(6)(vii). These acts include, but are not limited to:

a. UHC failed to enact adequate privacy and security measures to protect the Plaintiffs and the Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. UHC failed to take proper action following known security risks and prior cybersecurity incidents;

c. UHC knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Plaintiffs and the Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft;

d. UHC omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Plaintiffs and Subclass Members' PII;

e. UHC knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Plaintiffs and Subclass Members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the GLBA, 15 U.S.C. § 6801 et seq., and Rhode Island Identity Theft Protection Act of 2015, 11 R.I. Gen. Laws Ann. § 11-49.3-1 *et seq*.

f. UHC failed to maintain the privacy and security of the Plaintiffs and Subclass Members' PII in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

349. The above deceptive trade practices directly and proximately caused ascertainable injury to Plaintiffs and Subclass Members, as discussed above.

350. Plaintiffs and Subclass Members seek all available relief under 6 R.I. Gen. Laws Ann. § 6-13.1-5.2, including, but not limited to, actual damages, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

COUNT 9
BREACH OF CONTRACT – THIRD PARTY BENEFICIARY
(As to UHC)

351. UHC entered into administrative service agreements ("Agreements") with the State of Rhode Island and RIPTA to administer the State's self-insured health plan.

352. The Agreement between the State/RIPTA and UNC contained provisions that required UHC to protect the confidential information of health plan members. The types of information to be safeguarded included, but were not limited to, information covered by 42 CFR 431.305 and HIPPA, such as names, addresses, social security numbers, physical and behavioral health services provided, and medical data including diagnosis and history of diseases or disability.

353. With respect to plan member confidential information, UHC made the following or similar promises:

a. to protect confidential information from unauthorized disclosure;

b. to safeguard the members' confidential information

c. to comply with the requirements of HIPAA and regulations promulgated thereunder

d. to not use or disclose protected health information other than permitted by law or by the parties' Agreement;

e. to use the most updated industry safeguards to prevent the use or disclosure of protected health information;

f. to mitigate any harmful effect that is known to UHC of the use or disclosure of protected health information by UHC;

g. to maintain the security of protected health information by establishing, at a minimum, measures utilized in current industry standards;

h. to implement policies and procedures to facilitate the removal, termination, and final disposal of PHI in electronic format, including storage media housing the information.

354. The above promises were for the benefit of Rhode Island employees whose insurance was administered by UHC, including the Plaintiffs and Subclass Members. Accordingly, the Plaintiffs and Subclass Members were third-party beneficiaries of the said agreement and contractual promises.

355. UHC breached its promises to the Plaintiffs and Subclass Members by a) failing to maintain the promised safeguards to keep their data confidential and/or encrypt the data when it was sent to RIPTA, b) sending data on non-RIPTA employees to RIPTA, c) failing to audit its practices to prevent and/or timely discover the disclosure of unencrypted data and/or data for non-RIPTA employees to RIPTA. As a direct and proximate result of UHC's breaches of contract, the Plaintiffs and Subclass Members, as alleged above, have suffered damages in amounts to be proven at trial.

356. As a direct and proximate cause of the said breach, the Plaintiffs and Subclass Members have suffered damages as described above.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs, the Class, and the Subclass demand the following relief:

1. For an Order certifying the Class and the Subclass as defined herein and appointing Plaintiffs and their counsel to represent the Class and the Subclass;

2. For an award of actual, compensatory, consequential, incidental, nominal, statutory, and punitive damages, civil penalties, prejudgment interest, post-judgment interest, and attorney's fees and costs as allowed by statute;

3. For equitable relief ordering the Defendants to pay for and provide adequate identity and credit monitoring service through a third-party vendor for a ten (10) year period;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and disclosure of the PHI and PII of Plaintiffs, the Class, and the Subclass, and from refusing to issue prompt, complete, and accurate disclosures of the Data Breach to the Plaintiffs, the Class, and the Subclass.

5. For injunctive relief requested by the Plaintiffs, the Class, and the Subclass and other equitable relief as is necessary to protect the interests of the Plaintiffs, the Class, and the Subclass, including but not limited to an Order:

a) requiring Defendants to protect, including through encryption, all PHI and PII of plan members and beneficiaries through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, and local laws;

b) requiring Defendants to delete, destroy, and purge the PHI and PII of the Plaintiffs, the Class, and the Subclass unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of the Plaintiffs, the Class, and the Subclass and that they have established and enacted adequate security measures;

c) requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PHI and PII of Plaintiffs, the Class, and the Subclass.

d) requiring Defendants to engage independent 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, periodically, and

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

e) requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

f) requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

g) requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other areas of Defendants' systems;

h) requiring Defendants to conduct regular database scanning, security checks, data purging, and destruction as required by and in conformance with statute;

i) requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PHI and PII of the Plaintiffs, the Class, and the Subclass;

j) requiring Defendants to routinely and continually conduct internal training and education on how to identify and contain a breach when it occurs and what to do in response to a breach;

k) requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personally identifying information; and

l) requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; and

m) an award such other relief as the Court deems necessary and proper.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all claims so triable.

DATED: 2/13/23

By their attorneys,

/s/ Peter N. Wasylyk
Peter N. Wasylyk Esq., #3351
Law Offices of Peter N. Wasylyk
1307 Chalkstone Avenue
Providence, Rhode Island 02908
Tel: 401-831-7730
Email: pnwlaw@aol.com

/s/ Carlin J. Phillips
Carlin J. Phillips (*pro hac vice* pending)
PHILLIPS & GARCIA, P.C.
13 Ventura Drive
Dartmouth, MA 02747
508-998-0800
508-998-0919 (fax)
cphillips@phillipsgarcia.com

Cooperating counsel,
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF RHODE ISLAND

Of Counsel:

Lynette Labinger #1645
128 Dorrance Street Box 710
Providence, RI 02903
401-465-9565
LL@labingerlaw.com

Cooperating counsel,
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF RHODE ISLAND