STATE OF RHODE ISLAND

PROVIDENCE, sc.	SUPERIOR COURT
ALEXANDRA MORELLI 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.

INTRODUCTION

1. Alexandra Morelli (hereafter also referred to as "Morelli") and Diane M. Cappalli (hereafter referred to as "Cappalli") (hereafter Morelli and Cappalli collectively referred to as "Plaintiffs"), individually and on behalf of others similarly situated (hereafter also referred to as "Class" or "Class Members") bring this action 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 actions and inactions of 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") in their failure 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 approximately 22,000 individuals. The PHI and the PII were gathered and maintained as part of self-insured healthcare plans provided to employees and retirees of RIPTA and the State of Rhode Island. As a result of the Breach,

Plaintiffs and Class Members have been harmed as they have been exposed to an imminent and ongoing risk of fraud and identity theft which requires continued monitoring of their financial accounts, future financial footprints, their credit profiles, and their very identities.

2. Plaintiffs and Class 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.

3. In addition, Plaintiffs and Class Members have incurred and may incur direct damages related to various forms of identity theft and fraud. Plaintiffs and Class 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, and the reimbursement of out-of-pocket damages and the payment of compensatory damages.

4. Plaintiffs and Class 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.; and c) violations of the Confidentiality of Healthcare Communications and Information Act, R.I. Gen. Laws § 5-37-3.1.

PARTIES

5. Plaintiff Alexandra Morelli is an individual who resides in Coventry, Rhode Island, and who has worked at the University of Rhode Island since 2016.

6. 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.

7. 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.

8. 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

9. 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

10. The State of Rhode Island provides health insurance to state employees through a self-insured health 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.

11. The State of Rhode Island currently uses Blue Cross Blue Shield of Rhode Island (hereafter also referred to as "BCBS") as its self-insured healthcare plan administrator. Prior to using BCBS, the State of Rhode Island had a contract with UHC to administer the State Plan.

12. 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").

13. 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.

14. 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. 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.

15. 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.

16. The Data Files provided by UHC to RIPTA included information not only for individuals insured under RIPTA's healthcare plan 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.

17. 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.

18. 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.

19. Whether or not Current Procedural Terminology codes (hereafter also referred to as "CPT Codes") (which identify the service and procedure) or "ICD-10" codes (which identify a diagnosis), both of which are often contained in billing records, were downloaded has not yet been ascertained.

20. 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.

21. 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.

22. 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.

23. 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.

24. At a State of Rhode Island State Senate oversight hearing held on January 24, 2022, RIPTA revealed that roughly five thousand (5,000) out-of-state residents had also had their information breached.

25. As participants in the State Plan and the RIPTA Plan, Plaintiffs and Class 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 and the Class Members and given the substantial increase in national data breaches preceding the date of the Breach.

Federal Regulatory Data Security Standards

26. Federal statutes and regulations have put the Defendants on direct notice of the confidential nature of the information it maintained on the Plaintiffs and the Class Members and the requirement to securely maintain the Class 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.

27. 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.

28. 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.

29. RIPTA and UHC were aware of HIPAA's requirements and were subject to HIPAA's mandates to protect the PHI and PII of Plaintiffs and Class 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).

30. 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).

31. The notices sent by RIPTA failed to comply with HIPAA's sixty (60) day notice rule and thereby exposed the Plaintiffs and the Class Members 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

32. 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 and Class 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)).

33. 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).

34. 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).

35. 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.

36. 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.

37. 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).

38. 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.

39. 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.

Plaintiff Alexandra Morelli

40. 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.

41. Thereafter, 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 $29,999.00 (February 15th for $5,000.00, February 23rd for $10,000.00, and March 8 for $14,999.00).

42. 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.

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

44. 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.

Plaintiff Diane M. Cappalli

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

CLASS ALLEGATIONS

46. 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 definition, subject to amendment as appropriate:

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

47. The Plaintiffs also propose the following Subclass:

a. 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 seeks to represent the Subclass.

48. 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.

49. **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.

50. **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.

51. **Typicality.** 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.

52. **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.

53. **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.

54. **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.

55. 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 Identify Theft Protection Act, Gen. Laws § 11-49-3-1, et seq.
(As to RIPTA and UHC)

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

57. 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, was administered by UHC.

58. 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.

59. 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.

60. 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."

61. 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).

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

63. 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).

64. 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.

65. 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.

66. 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).

67. 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.

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

69. 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.

70. 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.

71. 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)

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

73. 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, was administered by UHC.

74. 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.

75. 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 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.

76. 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.

77. 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.

78. 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).

79. 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.

80. As a direct and proximate result of UHC's 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 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, the Class, and the Subclass; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

81. In addition, as a direct and proximate result of UHC's negligence and negligence per se, 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, loss of privacy, and other economic and non-economic losses.

82. Moreover, as a direct and proximate result of UHC's statutory violations, 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 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)

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

84. 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, was administered by UHC.

85. 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.

86. 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.

87. 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.

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

89. 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.

90. 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.

91. 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.

92. 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.

93. 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.

94. 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)

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

96. 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, was administered by UHC.

97. 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.

98. 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, 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.

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

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

101. Therefore, UHC owed a duty of reasonable care to the Plaintiffs, the Class, and the Subclass to safeguard, maintain, store, purge, and destroy the data securely as required by federal and state law and industry standards.

102. UHC breached the duty of care it owed to the Plaintiffs, the Class, 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 non-RIPTA state and quasi-state employee data from its files, thereby enabling an unauthorized person or entity to access and download the data.

103. As a direct and proximate result of UHC'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 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, the Class, and the Subclass; and (xi) the loss and invasion of their privacy with respect to their PHI and PII.

104. As a direct and proximate result of UHC's negligence and negligence per se, 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.

105. Additionally, as a direct and proximate result of UHC'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 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.

106. 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.

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

PRAYER FOR RELIEF

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

a. 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;

b. 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;

c. 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;

d. 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.

e. 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:

1. 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;

2. 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;

3. 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.

4. 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;

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

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

7. 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;

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

9. 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;

10. 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;

11. 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

12. 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

f. 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: 10-25-2022

By their attorneys,

/s/ Peter N. Wasylyk
Peter N. Wasylyk Esq., #3351
Law Offices of Peter N. Wasylyk
1307 Chalkstone Ave
Providence, RI 02908
401-831-7730
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