IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

CHANTAL ATTIAS AND ANDREAS KOTZUR, *Individually and on behalf of all others similarly situated*
1220 N St., NW
Washington, DC 20005

- AND -

RICHARD AND LATANYA BAILEY
Individually and on behalf of all others Similarly Situated
2 Broomfield Dr.
Stafford, VA 22554

- AND –

CURT AND CONNIE TRINGLER,
Individually and on behalf of all other Similarly Situated
12222 Carlos Rd.
Frostburg, Maryland 21532

- AND –

LISA HUBER
Individually and on behalf of all others similarly situated
1824 Weyburn Rd.
Baltimore, MD 21237

Plaintiffs,

v.

CAREFIRST, INC. d/b/a Group Hospitalization Medical Services, Inc., Carefirst of Maryland, Inc., Carefirst BlueCross Blueshield, Carefirst BlueChoice
1501 S. Clinton St.
Baltimore, MD 21224

Serve:
CT Corporation System
1015 15th St., NW
Suite 1000
Washington, DC 20005

Case No.: 1:15-cv-00882-CRC

SECOND AMENDED CLASS ACTION COMPLAINT

JURY DEMAND

- AND -

GROUP HOSPITALIZATION AND MEDICAL SERVICES, INC.
d/b/a Carefirst, Inc., Carefirst BlueCross Blueshield, Carefirst BlueChoice

Serve:
The Corporation Trust Inc.
300 E. Lombard St.
Baltimore, MD 21202

- AND -

CAREFIRST OF MARYLAND, INC
d/b/a Carefirst, Inc.. BlueCross and BlueShield of Maryland Inc., Carefirst BlueCross BlueShield, Carefirst BlueChoice

Serve:
The Corporation Trust, Inc.
351 West Camden St.
Baltimore, MD 21201

- AND -

CAREFIRST BLUECHOICE
d/b/a Carefirst, Inc., Carefirst BlueCross BlueShield, Group Hospitalization and Medical Services Inc., Carefirst of Maryland, Inc.

Serve:
CT Corporation System
1025 Vermont Ave., NW
Washington, DC 20005

Defendants.

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Chantal Attias, Andreas Kotzur, Richard Bailey, Latanya Bailey, and Lisa Huber make this class action complaint against Defendants Carefirst, Inc., D/B/A Group Hospitalization Medical Services, Inc., Carefirst of Maryland, Inc., Carefirst BlueCross Blueshield, Carefirst

BlueChoice (hereinafter "Carefirst"); Group Hospitalization and Medical Services, Inc, D/B/A Carefirst BlueCross BlueShield and Carefirst BlueChoice (hereinafter "GHMS"); Carefirst Of Maryland, Inc., D/B/A BlueCross and BlueShield of Maryland, Inc., Carefirst BlueCross BlueShield, Carefirst BlueChoice (hereinafter "Carefirst of Maryland"); and Carefirst BlueChoice D/B/A Carefirst BlueCross BlueShield, Group Hospitalization and Medical Services, Inc., Carefirst of Maryland, Inc. (hereinafter referred to as "BlueChoice")[1] and for their claims state the following:

PARTIES

1. Plaintiffs Chantal Attias and Andreas Kotzur are adult residents of the District of Columbia.
2. Plaintiffs Richard and Latanya Bailey are adult residents of the Commonwealth of Virginia.
3. Plaintiffs Curt and Connie Tringler are residents of the State of Maryland.
4. Plaintiff Lisa Huber is an adult resident of the State of Maryland.
5. Defendant Carefirst, Inc. d/b/a Group Hospitalization Medical Services, Inc., Carefirst BlueCross Blueshield, Carefirst BlueChoice is a foreign corporation doing business in the District of Columbia.
6. Defendant GHMS is a domestic corporation doing business in the District of Columbia and the Commonwealth of Virginia.
7. Defendant Carefirst of Maryland is a foreign corporation doing business in the State of Maryland and the District of Columbia.
8. Defendant BlueChoice is a foreign corporation doing business in the District of Columbia, Maryland and the Commonwealth of Virginia.

JURISDICTION

9. Each of the preceding paragraphs is incorporated by reference herein.

[1] Each of the named Defendants may be referred to collectively as "Defendants" throughout this Complaint.

10. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) in that Plaintiffs file their claims as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and that in the aggregate the claims and claims of the other members of the Class exceed $5,000,000 exclusive of interests and costs, and there are numerous class members who are citizens of states other than the Defendants.

11. This Court has personal jurisdiction over the Defendants because the Defendants are authorized to do business in the District of Columbia, and offer and or sell health insurance policies to citizens of the District of Columbia.

12. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because the acts and transactions giving rise to this action occurred in this District and because the Defendants are subject to personal jurisdiction in this District.

SUMMARY OF THE CASE

13. Each of the preceding paragraphs is incorporated by reference herein.

14. This is a class action lawsuit brought by Plaintiffs, individually and on behalf of all others similarly situated, due to the failure of Defendants to safeguard and secure the medical information, and other personally identifiable information, including names, addresses, birthdates, subscriber identification numbers, telephone numbers, and, possibly other information including patient credit card, medical or clinical information, and highly confidential health information and personal health related information[2] of Plaintiffs and Class Members.

[2] (collectively, "Personally Identifiable Information" or "PII;" "Personal Health Information" or "PHI" and "Sensitive Information"

15. Defendants announced to the public this massive loss of information on or about May 20, 2015 wherein the Plaintiffs personal "PII", "PHI" and "Sensitive Information", considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") entrusted to Defendants was stolen and/or made accessible to hackers and identity thieves.

16. As a result of Defendants' failure to implement and follow basic security procedures, the PII/PHI/Sensitive Information of a multitude of residents of the District of Columbia, the State of Maryland, and the Commonwealth of Virginia, including the Plaintiffs and the class they seek to represent are now in the hands of thieves.

17. The Plaintiffs and Class Members now face an increased risk of identity theft, and also actual identity theft and resulting losses, and need to take immediate action to protect themselves from identity theft, which have already and will continue to result in real and actual loss regardless of whether identity theft actually occurs.

18. Plaintiffs and Class Members are immediately and imminently in danger of sustaining some or further direct injury/injuries as a result of the identity theft they suffered when Defendants did not protect and secure their PII/PHI/Sensitive Information and disclosed their PII/PHI/Sensitive Information to hackers. These further instances of identity theft are certainly impending and imminent. The PII/PHI/Sensitive Information access, copied and transferred from Defendants have all of the information wrongdoers need, and the American government and financial systems requires, to completely and absolutely misuse Plaintiffs' and Class Members' identity to their detriment.

19. Consequently, the Plaintiffs and Class Members have or will have to spend significant time and money to protect themselves; including, but not limited to: the cost of responding to the data breach, the cost of acquiring identity theft protection and monitoring, cost of conducting a damage assessment, mitigation costs, costs to rehabilitate Plaintiffs' and Class

Members' PII/PHI/Sensitive Information, and costs to reimburse from losses incurred as a proximate result of the breach.

20. Many Plaintiffs and Class Members suffered from actual economic injury resulting in tax-refund fraud, identify theft, credit card fraud, and other conduct causing direct economic injury as a result of the identity theft they suffered when Defendants did not protect and secure their PII/PHI/Sensitive Information and disclosed their PII/PHI/Sensitive Information to hackers.

21. Plaintiffs contracted for services that included a guarantee by Defendants to safeguard their personal information and, instead, Plaintiffs received services devoid of these very important protections. Accordingly, Plaintiffs allege claims for breach of contract, unlawful trade practices, unjust enrichment, negligence, and negligence *per se*.

FACTS COMMON TO ALL CLAIMS

22. Each of the preceding paragraphs is incorporated by reference herein.

23. Defendants are a network of for-profit health insurers which provide health insurance coverage to individuals in the District of Columbia, the State of Maryland and the Commonwealth of Virginia. Collectively, Defendants insure in excess of One Million individuals with health coverage.

24. Defendants are "covered entities" as defined by the Health Insurance Portability and Accountability Act (hereinafter "HIPAA") and therefore must comply with HIPAA its accompanying rules and regulations, and also must comply with the Health Information Technology for Economic and Clinical Health Act (hereinafter "HITECH") and its accompanying rules and regulations.

25. Plaintiffs are customers and the insureds of Defendants and provided payment to Defendants for certain services, including health insurance coverage, part of which was intended to pay administrative costs of securing their PII/PHI/Sensitive Information.

26. The Plaintiffs contracted for services that included a promise by Defendants to safeguard, protect, and not disclosure their personal information and, instead, Plaintiffs received services devoid of these very important protections.

27. In the regular course of business, Defendants collect and maintain possession, custody, and control of a wide variety of Plaintiffs' PII/PHI/Sensitive Information, including, but not limited to patient credit card, medical or clinical information and history, patient names, addresses, birthdates, telephone numbers, email addresses, account numbers, and social security numbers.

28. Defendants issued an "Internet Privacy Policy" intended to convey how PII/PHI and other Sensitive Information would be secured and protected. Specifically, Defendants Internet Privacy Policy stated:

> CareFirst BlueCross BlueShield respects the need for security regarding your personal information. Whenever you provide personal information, your information will be protected using Secure Sockets Layer (SSL) technology. SSL is an industry standard that encrypts the information you provide, to avoid the decoding of that information by anyone other than CareFirst BlueCross BlueShield. This technology, however, does not absolutely guarantee the total privacy of information that has been provided to this site.
>
> Information you submit directly to us will remain on our servers or those of our affiliates, secured by various industry approved technologies to prevent unauthorized access to your personal information.

29. In September 2013, Defendants issued an amended Privacy Policy which stated:

> We maintain physical, electronic and procedural safeguards in accordance with federal and state standards to protect your health information. All of our associates receive training on these standards at the time they are hired and thereafter receive annual refresher training. Access to your protected health information is restricted to appropriate business purposes and requires pass codes to access our computer

systems and badges to access our facilities. Associates who violate our standards are subject to disciplinary actions.

30. Personal Information is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

31. Despite Defendants' stated Internet Privacy Policy, Defendants, individually and collectively, did not provide encryption for all of the personal information whether in transit or at rest, which the Plaintiffs and class members provided to Defendants. Instead, only a portion of the Personal Information was encrypted, while other information was not given the protections of encryption, and was subsequently able to be obtained unlawfully.

32. Despite Defendants' statements to the contrary, the combination of members' names, birth dates, email addresses and subscriber identification number alone qualifies as personal information, and the unauthorized access to said combination of information creates a material risk of identity theft and access to other personal information including Personal Health Information ("PHI"), Electronic Personal Health Information ("ePHI"), Personal Identification Information ("PII"), financial information, medical information and other Sensitive Information.

33. In June of 2014, Defendants suffered a cyberattack on its servers.

34. By failing to provide the encryption technology and other technology safeguards that Defendants' Internet Privacy Policy and General Privacy Policy indicated, the cyberattack allowed access to PII, PHI, ePHI, and other personal and sensitive information of Plaintiffs and The Class members.

35. Defendants then failed to recognize that a cyberattack occurred until April of 2015 after obtaining an outside consulting firm to perform a scan and search of its servers.

36. Finally, on May 20, 2015 – nearly a year after the cyberattack occurred – Defendants notified Plaintiffs and the class members that a cyberattack had occurred and that some of their personal information may have been gathered by individuals with ulterior motives.

37. Defendants suggested that Plaintiffs and each class member protect themselves with identity theft protection and monitoring to combat Defendants' failures to adequately and appropriately safeguard personal information, to identify a cyberattack in a timely fashion, and to provide the privacy security and safeguards promised in Defendants' Internet Privacy Policy.

38. Plaintiffs and members of The Class have suffered economic and non-economic loss in the form of mental and emotional pain and suffering and aguish as a result of Defendants' failures.

HIPAA AND HITECH ACT REQUIREMENTS

39. Each of the preceding paragraphs is incorporated by reference herein.

40. Under HIPAA and the HITECH Act, Defendants must implement policies and procedures to limit administrative, technical and physical access to their electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. *See* 45 C.F.R. § 164.302, *et seq.*

41. Specifically, Defendants must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmit; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted. *See* 45 C.F.R. § 164.306.

42. Defendants must also implement technical policies and procedures for electronic information systems that maintain electronic PII/PHI to allow access only to those persons

or software programs that have been granted access rights as specified in 45 C.F. R. §164.308(a)(4). A few of these policies and procedures include, but are not limited to: implementing a mechanism to encrypt and decrypt electronic PII/PHI; implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PII/PHI; implementing procedures to verify that a person or entity seeking access to electronic PII/PHI is the one claimed; implementing technical security measures to guard against unauthorized access to electronic PH/PHI that is being transmitted over an electronic communications network; implementing security measures to ensure that electronically transmitted electronic PH/PHI is not improperly modified without detection until disposed of. See 45 C.F.R. §164.312.

43. When Defendants permit business associates to create, receive, maintain, or transmit electronic PH/PHI, it must ensure that those business associates comply with HIPAA and the HITECH Act. See 45 C.F.R. § 164.314.

44. Defendants must also conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate; implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and implement procedures for guarding against, detecting, and reporting malicious software. See 45 C.F.R. § 164.308.

45. Defendants did not comply with any of the foregoing requirements.

CONSEQUENCES OF DEFENDANTS' CONDUCT

46. Each of the preceding paragraphs is incorporated herein.

47. The ramifications of Defendants' failure to keep class members' PII, PHI, ePHI and other personal and sensitive information secure are severe.

48. The information Defendants lost, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). FTC, *About Identity Theft*, available at <http://www.vanderbilt.edu/PersonalIdentityTheftProtection.pdf> (last visited Feb. 5, 2015). Identity theft occurs when someone uses another's PII and/or PHI, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. *Id.* The FTC estimates that as many as 9 million Americans have their identities stolen each year. *Id.*

49. Identity thieves can use identifying data – including that accessed on Defendants' servers - to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. *Id.*

50. Identity thieves can use personal information such as that pertaining to the Class, which Defendants failed to keep secure to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

51. In addition, identity thieves may get medical services using the Plaintiff's PII and PHI or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

52. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008:

> In addition to the losses that result when identity thieves fraudulently

> open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, at p.11 (April 2007), available at: <http://www.ftc.gov/sites/default/files/documents/reports/combating-dentitytheft-strategic-plan/strategicplan.pdf> (last visited Feb. 5, 2015).

53. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

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

GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Feb. 5, 2015).

54. "In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health endangered by inaccurate entries in their medical records. This inaccurate information can potentially cause victims to receive improper medical care, have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that a theft has

occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits." *Id.* at 30.

55. With the advent of the prescription drug benefit of Medicare Part D, the Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft." Identity thieves can use such information "fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase . . . sales commissions" or commit other types of fraud. "The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal." *Id.* at 31.

56. Plaintiffs and the Class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

57. Plaintiffs Curt and Connie Tringler, residents of Frostburg, Maryland, had their PII/PHI/Sensitive Information disclosed as a result of the Defendant's failures to protect their information. Carefirst promised that their information would be protected in accordance with industry standards and as mandated by law. The Tringlers' Sensitive Information was compromised in and as a result of the data breach at issue in this case and they suffered a cognizable injury. Since the data breach, the Tringlers have experienced tax-refund fraud and have still has not received their federal or state tax refund. The Tringlers have spent significant hours to prevent further fraud and in dealing with the ramifications of the data breach at issue in this case. The Tringlers were harmed by having their Sensitive Information compromised, suffered monetary damages, and face an ongoing, imminent threat of future additional harm from the data breach like all members of the proposed class

58. As a result of Defendants failing to protect the Plaintiffs PII/PHI/Sensitive Information, many Plaintiffs have already suffered from direct economic injury such as tax-refund fraud, identify theft, credit card fraud, and other conduct causing direct economic injury.

CLASS ACTION ALLEGATIONS

59. Pursuant to Rule 23 – specifically Rule 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4) - of the Federal Rules of Civil Procedure, the Plaintiffs bring this action on their own behalf, and on behalf of all other persons similarly situated ("the Class").

60. The Class that Plaintiffs seek to represent the following class and subclasses:

THE CLASS

All persons who reside in the District of Columbia, the State of Maryland and the Commonwealth of Virginia and have purchased and/or possessed health insurance from Carefirst, Inc., Group Hospitalization and Medical Services, Inc., Carefirst of Maryland, Inc., and/or Carefirst BlueChoice and whose personally identifiable information, personal health information, sensitive personal information, and/or financial information was breached as a result of the data breach announced on or about May 20, 2015.[3]

THE SUBCLASSES

1. All persons who reside in the District of Columbia, and have purchased and/or possessed health insurance from Carefirst, Inc., Group Hospitalization and Medical Services, Inc., Carefirst of Maryland, Inc., and/or Carefirst BlueChoice and whose personally identifiable information, personal health information, sensitive personal information, and/or financial information was breached as a result of the data breach announced on or about May 20, 2015.[4]

2. All persons who reside in the State of Maryland, and have purchased and/or possessed health insurance from Carefirst, Inc., Group Hospitalization and Medical Services, Inc., Carefirst of Maryland, Inc., and/or Carefirst BlueChoice and whose personally identifiable information, personal health information, sensitive personal information, and/or financial information was breached as a result of the data breach announced on or about May 20, 2015.[5]

[3] Hereinafter referred to as "The Class."
[4] Hereinafter referred to as "The DC Class" or "The DC Subclass."
[5] Hereinafter referred to as "The Maryland Class" or "The Maryland Subclass."

> 3. All persons who reside in the Commonwealth of Virginia, and have purchased and/or possessed health insurance from Carefirst, Inc., Group Hospitalization and Medical Services, Inc., Carefirst of Maryland, Inc., and/or Carefirst BlueChoice and whose personally identifiable information, personal health information, sensitive personal information, and/or financial information was breached as a result of the data breach announced on or about May 20, 2015.[6]

61. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants.

62. Excluded from the Classes are (1) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current or former employees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Classes; and (iv) the legal representatives, successors, or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of the data stored by Defendants.

63. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because the members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is excess of One Million patients (including Plaintiffs and the class they seek to represent) is now in the hands of thieves.

64. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because there is a well-defined community of interest among the members of the Class, common questions of law and fact predominate, the claims are typical of the members of the Class, and the

[6] Hereinafter referred to as "The Virginia Class" or "The Virginia Subclass."

Plaintiffs can fairly and adequately represent the interests of the Class.

65. The action satisfies the requirement of Federal Rule of Civil Procedure 23(b)(1) because prosecuting separate actions by or against individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for the party opposing the class; or adjudications with respect to individual class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests

66. Plaintiffs and members of The Class also seek injunctive relief because Defendants have acted and failed to act on grounds that affect The Class as a whole. Therefore, the action satisfies the requirements of Rule 23(b)(2).

67. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to the member of the Class that predominate or any questions affecting only individual members, including, but not limited to:

a. Whether the Defendants unlawfully used, maintained, lost or disclosed Class members' PII, PHI and Sensitive Information;

b. Whether the Defendants unreasonably delayed in notifying affected customers/patients of the data breach;

c. Whether the 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;

d. Whether the Defendants' conduct was negligent;

e. Whether the Defendants' conduct was a breach of contract;

f. Whether the Defendants violated applicable consumer protection statutes;

g. Whether the Defendants violated applicable Data Breach Notification statutes;

h. Whether the Defendants committed fraud;

i. Whether the Defendants were unjustly enriched;

j. Whether the Defendants breached their duties of confidentiality;

j. Whether the Plaintiffs and the Class are entitled to damages, statutory penalties, punitive damages, and/or injunctive relief.

58. The Plaintiffs claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by the Defendants.

59. Plaintiffs will fairly and adequately represent the interests of The Class and the respective subclasses.

60. The prosecution of separate actions by individual members of the Class or separate actions of each subclass would create a risk of inconsistent or varying adjudications with respect to individual members of The Class, which would establish incompatible standards of conduct for the Defendants and would lead to repetitive adjudication of common questions of law and fact. The Class is in excess of 1 million individuals, and accordingly, class treatment is superior to any other method for adjudicating the controversy. The Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).

61. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, the Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

62. For all of the foregoing reasons, certification is proper under Rule 23(b)(1), 23(b)(2) and 23(b)(3).

63. Plaintiffs reserve the right to revise Class definitions and questions based upon facts learned in discovery.

BREACH OF CONTRACT (express and implied)
Count I

64. Each of the preceding paragraphs is incorporated herein.

65. Plaintiffs and the class members paid money to Defendants in exchange for health insurance, which included promises to protect Plaintiffs' PII, PHI and Sensitive Information.

66. In its written services contract, Defendants promised Plaintiffs and the class members that Defendants only disclose health information when required to do so by federal or state law. Defendant further promised that it would protect Plaintiffs' Sensitive Information.

67. Defendants also promised through its Internet Privacy Policy that it would encrypt all personal information given to Defendants.

68. Defendants promised to comply with all HIPAA standards and to make sure that Plaintiffs' PPI, PHI and Sensitive Information was protected.

69. Defendants' promises to comply all HIPAA standards and to make sure that Plaintiffs' health information and Sensitive Information was protected and specifically encrypted created an implied contract.

70. To the extent that it was not expressed, an implied contract was created whereby Defendants' promised to safeguard Plaintiffs' health information and Sensitive Information from being accessed, copied, and transferred by third parties.

71. Under the contract, Defendants were further obligated to provide Plaintiffs with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

72. Defendants did not safeguard Plaintiffs' health information and Sensitive Information and did not encrypt all personal information that Plaintiffs provided to Defendants, therefore, Defendants breached the contract with Plaintiffs.

73. Furthermore, Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs that were of a diminished value.

74. As a result, Plaintiffs have been harmed and/or injured and will incur economic and non-economic damages as a proximate and direct result of the breach by Defendants.

75. **WHEREFORE**, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

NEGLIGENCE
Count II

76. Each of the preceding paragraphs is incorporated herein.

77. Defendants owed the Plaintiffs a duty of care in protecting the confidentiality of the personal and private information that the Plaintiffs provided to the Defendants as consumers of the Defendants' health insurance policies.

78. Defendants came into possession of Plaintiff's PII, PHI and Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

79. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's PII, PHI and Sensitive Information.

80. Defendants had a duty to conduct audits of its electronic files and determine whether any

PII, PHI or Sensitive Information had been obtained by unauthorized parties.

81. Defendants had a duty to provide reasonable and timely notice to Plaintiffs and members of The Class regarding the data breach and the steps that can be taken by Plaintiffs and members of the Class to protect themselves from identity theft.

82. The Defendants were negligent in that it breached the duty of reasonable care that it owed to the Plaintiffs as its patients by failing to have in place reasonable and appropriate protections from unauthorized data breaches, providing a reasonable and timely notice of the breach, and failing to perform reasonable and timely audits of the data protection system.

83. As a direct and proximate result of the Defendants' negligence, the Plaintiffs have suffered damages, including pain and suffering and past and future economic loss.

84. **WHEREFORE**, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION ACT
Count III

85. Each of the preceding paragraphs is incorporated by reference herein.

86. Defendants produced an Internet Privacy Policy which informed Plaintiff Chantal Attias and members of the DC Class and the DC General Public that personal information given to Defendants would be secured by means of encryption on Defendants' electronic computers and servers.

87. Instead, Defendants did not secure all personal information that Plaintiffs Mr. Kotzur and Mrs. Attias and the DC Class produced to Defendants on encrypted servers, allowing some of that information to be secured without the security safeguards and benefits of encryption.

88. As such, Defendants violated their Internet Privacy Policy and committed and unfair and unlawful trade practice in that the services provided:

    a. Did not provide the types of characteristics and benefits which Defendants proffered when Defendants claimed to encrypt Mr. Kotzur and Mrs. Attias' and the class members personal information;

    b. Misrepresented as to a material fact which has a tendency to mislead because Defendants did not secure Mr. Kotzur and Mrs. Attias' personal information as indicated in their Internet Privacy Policy;

    c. Did not comply with federal law requirements for data security and protection, including HIPAA's requirements for administrative, physical, and technical safeguards found in 45 C.F.R. 164.302, *et seq.*;

    d. Otherwise deceives and misleads.

89. As a proximate and direct result of this unlawful and deceptive trade practice, Mr. Kotzur and Mrs. Attias and members of the DC Class were deceived in their purchase of health insurance from Defendants in that Mr. and Mrs. Attias and the members of the DC Class believed Defendants would comply with their own stated Internet Privacy Policy and encrypt personal information when in transit and at rest.

90. As a result of this unfair and deceptive trade practice, Mr. Kotzur and Mrs. Attias and members of the DC Class have been injured and seek the following for herself and on behalf of the general public and members of the class:

a. An injunction against Defendants, including that Defendants encrypt all personal information provided to it by their insureds, or that Defendants modify their Internet Privacy Policy and General Privacy Policy to accurately reflect their encryption and technological safeguard policies;

b. Additional relief to restore to the consumer money which was acquired by means of the unlawful trade practice in the District of Columbia;

c. Punitive damages;

d. $1500 per violation or treble damages, whichever is greater;

e. Reasonable Attorney's fees;

f. All other statutory relief the court determines proper under D.C. Code § 28–3905(k)(1).

91. **WHEREFORE**, Plaintiffs Andreas Kotzur and Chantal Attias on behalf of themselves as individuals and on behalf of the general public and the DC Class, make this Complaint for all damages requested above including injunctive relief and all other monetary damages allowed by law believed to be in excess of the jurisdictional amount.

VIOLATION OF THE DC DATA BREACH NOTIFICATION STATUTE
Count IV

92. Each of the preceding paragraphs is incorporated by reference herein.

93. The District of Columbia Data Breach Notification Statute (D.C. Code, Loc. Bus. Aff. § 28-3851, *et seq.*) defines "personal information" as "An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:

(ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account." D.C. Code § 28-3851(3).

94. Pursuant to Defendants' notice to its insureds, the following information of Mr. Kotzur and Mrs. Attias and the DC Class was breached: members' names, birth dates, email addresses and subscriber identification number.

95. Defendants were therefore required to notify Mr. Kotzur and Mrs. Attias and the DC Class in the "most expedient time possible" and without unreasonable delay. Defendants were further required to notify all Consumer Reporting Agencies without unreasonable delay of the breach of information of Mr. Kotzur and Mrs. Attias and the DC Class, which is in excess of 1000 individuals.

96. Defendants failed to provide notice of the data breach to Mr. Kotzur and Mrs. Attias and the DC Class in the most expedient time possible and also failed to provide notice of the breach to all required Consumer Reporting Agencies without unreasonable delay.

97. Mr. Kotzur and Mrs. Attias and the DC Class have suffered actual damages in that they and members of the DC Class have purchased and will need to continue to purchase credit monitoring and identity theft protection for life.

98. Mr. Kotzur and Mrs. Attias brings this cause of action on behalf of themselves individually and the DC Class seeking all actual damages, costs of the action and reasonable attorneys' fees.

99. **WHEREFORE**, Plaintiffs Andreas Kotzur and Chantal Attias on behalf of themselves as individuals and on behalf of the general public and the DC Class, make this Complaint for all damages requested above including injunctive relief and all other monetary damages allowed by law believed to be in excess of the jurisdictional amount.

VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT
Count V

100. Each of the preceding paragraphs is incorporated by reference herein.

101. Defendants produced an Internet Privacy Policy which informed Plaintiffs Curt and Connie Tringler, Lisa Huber and members of the Maryland Class that personal information given to Defendants would be secured by means of encryption on Defendants' electronic computers and servers. Instead, Defendants did not secure all personal information that Plaintiffs Curt and Connie Tringler, Lisa Huber and the Maryland Class produced to Defendants on encrypted servers, allowing some of that information to be secured without the security safeguards and benefits of encryption.

102. As such, Defendants violated their Internet Privacy Policy and General Privacy Policy and committed and unfair and unlawful trade practice in that the Internet Privacy Policy:

a. Contained misleading statements that had the capacity and tendency to mislead Plaintiffs Curt and Connie Tringler, Lisa Huber and the Maryland Class to believe that the personal information that they supplied to Defendants would be encrypted in transit and at rest on Defendants' servers.

b. Failed to state a material fact that tended to deceive Plaintiffs Curt and Connie Tringler, Lisa Huber and the Maryland Class to believe that their personal information would be encrypted while in transit and at rest on Defendants' servers.

103. Further, the State of Maryland defines "Personal information" as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: **(i)** A Social Security number; **(ii)** A driver's license number; or **(iii)** A financial account number...." Md. Commercial Law Code Ann. § 14-3501.

104. A "breach of the security system" occurred because Defendants permitted unauthorized access to "members' names, birth dates, email addresses and subscriber

identification number" the last of which is a "financial account number," i.e. Plaintiffs' and the Maryland Class Members' Personal Information.

105. Defendants were required to notify Plaintiffs Curt and Connie Tringle, Lisa Huber and the members of the Maryland Class of the security breach as soon as reasonably practicable after it was discovered.

106. Defendants were further required to send a notification letter which provided the following information:

> (1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;
>
> (2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;
>
> (3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and
>
> (4) (i) The toll-free telephone numbers, addresses, and Web site addresses for:
>
> - 1. The Federal Trade Commission; and
> - 2. The Office of the Attorney General; and
>
> (ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft. Md. Commercial Law Code Ann. § 14-3504.

107. Defendants failed to provide a proper notification letter in that they, collectively and individually, failed to provide toll free numbers for the major consumer reporting agencies,

toll free numbers, addresses and Web site addresses for the Federal Trade Commission and the Office of the Attorney General, and to inform the individual that information can be obtained from these sources about steps that can be taken to avoid identity theft.

108. Defendants committed an unlawful and deceptive trade practice in failing to comply with Maryland Comm. Law Code Ann. § 14-3504, *et seq.*

109. As a proximate and direct result of this failure to comply with Md. Comm. Law Code Ann. § 14-3504, Plaintiffs Curt and Connie Tringler, Lisa Huber and the Maryland Class suffered actual damages in that they were delayed in obtaining timely credit protection and identity theft monitoring, suffered actual and also imminent identity theft, and suffered mental and emotional pain and suffering.

110. Plaintiffs seek for themselves and the Maryland Class all damages allowable by law for these unlawful and deceptive trade practices including compensatory damages for economic and non-economic harm, and attorneys' fees.

111. **WHEREFORE**, Plaintiffs Curt and Connie Tringler, and Lisa Huber on behalf of themselves as individuals and on behalf of the Maryland Class, make this Complaint for all damages requested above including all monetary damages including attorneys' fees as allowed by law and believed to be in excess of the jurisdictional amount.

VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT
Count VI

112. Each of the preceding paragraphs is incorporated by reference herein.

113. Defendants committed an unlawful trade practice by failing to offer their services consistent with their own Internet Privacy Policy in that Defendants failed to encrypt Plaintiffs Richard Bailey's and Latanya Bailey's and the Virginia Class' personal information. This failure is an unlawful trade practice in that it:

a. Misrepresented the benefits of the services provided by Defendants;

b. Used deception, fraud and misrepresentation by promising that Plaintiffs Richard Bailey's and Latanya Bailey's and the Virginia Class' personal information would be encrypted on Defendants' servers;

c. Otherwise misled.

114. As a proximate and direct result of this failure to comply with Va. Code Ann. § 59.1-200, Plaintiffs Richard and Latanya Bailey and the Virginia Class suffered actual damages in that they were not given the benefit of the services for which they bargained and ultimately their PII, PHI and Sensitive Information was subject to a data breach that encryption would have prevented.

115. Plaintiffs Mr. and Mrs. Bailey seek for themselves individually and for the Virginia Class all damages allowable by law for these unlawful and deceptive trade practices including actual damages or $500, whichever is greater, and additionally for an amount equal to three times the actual damages suffered by Mr. and Mrs. Bailey and the Virginia Class or $1000 per violation whichever is greater, and attorneys' fees and court costs.

116. **WHEREFORE**, Plaintiff Richard and Latanya Bailey on behalf of himself and herself as individuals and on behalf of the Virginia Class, make this Complaint for all damages requested above including all monetary damages including attorneys' fees as allowed by law and believed to be in excess of the jurisdictional amount.

FRAUD
Count VII

117. Each of the preceding paragraphs is incorporated by reference herein.

118. Defendants made false representations of material facts to Plaintiffs and members of The Class in that Defendants proffered an Internet Privacy Policy and General Privacy Policy

which indicated that information provided by Plaintiffs and members of The Class would be encrypted. Defendants further made false representations by claiming they would use various industry technologies to prevent unauthorized access of Plaintiffs' and members of The Class' personal information.

119. Defendants made these false representations knowing them to be untrue and with reckless indifference for the truth.

120. The Defendants made these representations for the purpose of defrauding Plaintiffs and members of The Class by inducing them to purchase Defendants' services and to use Defendants' online services.

121. The Plaintiffs and members of The Class had the right to rely upon these representations and it was reasonable for them to rely upon these facts. Plaintiffs and members of The Class did in fact rely upon them.

122. The Plaintiffs and members of The Class suffered compensable injury in that their personal information was subject to an unauthorized data breach, and they each must now purchase credit monitoring and/or identity theft protection, in addition to pain and suffering, and inconvenience.

123. **WHEREFORE**, Plaintiffs on behalf of themselves as individuals and on behalf of The Class, make this Complaint for all damages allowable by law including all monetary damages including attorneys' fees and punitive damages as allowed by law and believed to be in excess of the jurisdictional amount.

NEGLIGENCE *PER SE*
Count VIII

124. Each of the preceding paragraphs is incorporated by reference herein.

125. Defendants owed the Plaintiffs a duty of care in protecting the confidentiality of

the personal and private information that the Plaintiffs provided to the Defendants as consumers of the Defendants' health insurance policies.

126. Defendants came into possession of Plaintiff's PII, PHI and Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

127. Defendants further had a duty to comply with applicable state and federal laws which were implemented to protect the Plaintiffs and members of The Class.

128. Defendants failed to comply with the duties imposed upon them by applicable federal laws in protecting Plaintiffs, The Class and the Subclasses by:

a. Failing to comply with HIPAA and HITECH to protect Plaintiffs and members of The Class, including failing to comply with the administrative and technical safeguards rules and regulations of HIPAA;

b. Failing to provide reasonable and timely notification of the data breach including by failing to comply with the DC Data Breach Notification statute and the DC Consumer Protection and Procedures Act for the benefit of Chantal Attias and members of the DC Class;

c. Failing to comply with the Maryland Consumer Protection Act and the Maryland Data Breach Notification Act (Maryland Comm. Law Code Ann. § 14-3504, *et seq.*) for the benefit of Lisa Huber and members of the Maryland Class; and

d. Failing to comply with the Virginia Consumer Protection Act and the Virginia Medical Breach Notification Act (Va. Code Ann. § 32.1-127.1:05) for the benefit of Mr. and Mrs. Bailey and members of the Virginia Class.

129. As a direct and proximate result of the Defendants' negligence, the Plaintiffs have suffered damages, including pain and suffering and past and future economic loss.

130. **WHEREFORE**, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

UNJUST ENRICHMENT
Count IX

131. Each of the preceding paragraphs is incorporated by reference herein.

132. Defendants received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.

133. Defendants did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.

134. Defendants have knowledge of said benefit.

135. Defendants have been unjustly enriched and it would be inequitable for Defendants to retain Plaintiffs' payments.

136. As a result, Plaintiffs have been proximately harmed and/or injured.

137. **WHEREFORE**, Plaintiffs individually and on behalf of the members of The Class demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

BREACH OF THE DUTY OF CONFIDENTIALITY
Count X

138. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

139. The Defendant owed the Plaintiffs and members of The Class a duty of confidentiality pursuant to its fiduciary relationship with the Plaintiffs and members of The Class as their health care providers.

140. Included in this duty owed by the Defendants is one of undivided secrecy and loyalty to the Plaintiffs as its patients, and this duty is critical to encourage the free exchange of information between patients and their healthcare providers.

141. The minimum standard of care imposed on the Defendants in maintaining the confidentiality of the Plaintiffs' Sensitive Information is expressed in multiple statutes, regulations, and judicial decisions.

142. The Defendants breached their individual and collective duty to the Plaintiffs and members of The Class through the unauthorized disclosure, breach, and/or publication of their personal and private information, and thus violated the Plaintiffs' right to have this information and their information kept confidential.

143. Indeed, such a violation breaches the trust that represents the core of the fiduciary relationship between the Plaintiffs as patients and the Defendants as their healthcare providers.

144. As a direct and proximate result of the Defendants' individual and collective breach of the duty of confidentiality, the Plaintiffs and members of The Class have suffered damages and breach of the confidential healthcare provider-patient relationship.

145. **WHEREFORE**, Plaintiffs demand judgment against Defendant jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding,

including attorney's fees.

CONSTRUCTIVE FRAUD
Count XI

146. Each of the preceding paragraphs is incorporated by reference herein.

147. Plaintiffs Curt and Connie Tringler, Lisa Huber and the Maryland Class bring this cause of action for constructive fraud.

148. At all times, Defendants were in a legal and equitable duty with Plaintiffs Curt and Connie Tringler, Lisa Huber and members of the Maryland Class arising out of the relationship that existed between Defendants and Plaintiffs and the Maryland Class in which trust and confidence exist.

149. Included in that relationship is the understanding that Defendants, each individually, will protect and safeguard the privacy of Plaintiffs Curt and Connie Tringler, Lisa Huber and the members of the Maryland Class, including by not disclosing the protected health information and sensitive information of Plaintiffs and the Maryland Class.

150. Defendants likewise owed a duty to the Plaintiffs Curt and Connie Tringler, Lisa Huber and the members of the Maryland Class to abide by the privacy policies it had incorporated and to safeguard personal health information.

151. Defendants breached that duty by deceiving the public, Curt and Connie Tringler, Lisa Huber, and the members of the Maryland Class by failing to abide by their own privacy and internet polices and disclosing personal health information and other sensitive information to third parties in violation of the Defendants' respective privacy policies and assurances.

152. As a direct and proximate cause of the fraud, Plaintiffs Curt and Connie Tringler, Lisa Huber and all members of The Maryland Class have suffered economic and non-

economic damages including damage to the physician-patient relationship that had been established, pain and suffering, mental anguish, past and future medical bills, and loss of earning capacity.

153. Plaintiffs and members of the Maryland Class rely on the doctrines of actual and apparent agency, *res ipsa loquitur*, and *respondeat superior* where applicable.

154. **WHEREFORE**, Plaintiffs Curt and Connie Tringler, and Lisa Huber individually and on behalf of the members of The Maryland Class demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiff and members of The Maryland Class for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

PRAYER FOR RELIEF

155. **WHEREFORE** Plaintiffs seek individually and on behalf of all others similarly situated, members of The Class, The DC Class and the Virginia Class, all damages allowable by law, including compensatory damages, statutory damages, punitive damages, attorneys' fees, and costs in excess of $5 million ($5,000,000.00) and further seek all injunctive relief allowed by law.

Date: July 16, 2015

Respectfully submitted,

PAULSON & NACE, PLLC

/s/ Jonathan B. Nace

Jonathan B. Nace, Esq., Bar No. 985718
1615 New Hampshire Ave, NW
Washington, DC 20009
jnace@paulsonandnace.com

202-463-1999 (Tel.)
202-223-6824 (Fax)

Troy N. Giatras Esq. (WV Bar No. 5602)
The Giatras Law Firm, PLLC
118 Capitol Street
Suite 400
Charleston, WV. 25301
304-343-2900
(*Pro Hac Vice* to follow)

DEMAND FOR JURY TRIAL

COMESNOW Plaintiffs, by and through undersigned counsel, and pursuant to Rule 38 of the Federal Rules of Civil Procedure, hereby demands trial by jury of all issues in this matter.

Respectfully submitted,

Paulson & Nace, PLLC

/s/ Jonathan B. Nace
Jonathan B. Nace, Esq., Bar No. 985718
Counsel for Plaintiffs, The Class and all Subclasses

CERTIFICATE OF SERVICE

This is to certify that on this 16th day of July, 2015, I caused a copy of the foregoing *Second Amended Class Action Complaint* to be filed via ECF upon the Court. I further certify that a copy of the foregoing will be served upon the opposing parties as soon as reasonably possible and within all requirements of Federal Rules of Civil Procedure.

Respectfully submitted,

PAULSON & NACE, PLLC

/s/ Jonathan B. Nace
Jonathan B. Nace, Esq., Bar No. 985718
1615 New Hampshire Ave, NW
Washington, DC 20009
jnace@paulsonandnace.com
202-463-1999 (Tel.)
202-223-6824 (Fax)