GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Division of Law
124 Halsey Street – 5th Floor
P.O. Box 45029
Newark, New Jersey 07101
Attorney for Plaintiffs

By: Elliott M. Siebers (033582012)
Deputy Attorney General

SUPERIOR COURT OF NEW JERSEY
CHANCERY DIVISION
MERCER COUNTY
DOCKET NO.: MER-C-_____-19

GURBIR S. GREWAL, Attorney General of the State of New Jersey, and PAUL R. RODRÍGUEZ, Acting Director of the New Jersey Division of Consumer Affairs,

Plaintiffs,

v.

PREMERA BLUE CROSS

Defendant.

COMPLAINT

Plaintiffs Gurbir S. Grewal, Attorney General of the State of New Jersey ("Attorney General") with offices located at 124 Halsey Street, Fifth Floor, Newark, New Jersey, and Paul R. Rodríguez, Acting Director of the New Jersey Division of Consumer Affairs ("Director"), with offices located at 124 Halsey Street, Seventh Floor, Newark, New Jersey, (collectively, "Plaintiffs") by way of complaint state:

PRELIMINARY STATEMENT

1. The Defendant Premera Blue Cross ("PREMERA") is a citizen of the State of Washington. PREMERA is a Washington non-profit corporation with its principal place of business at 7001 220th St. SW, Mountlake Terrace, WA, 98043.

2. In the course of its business, PREMERA collects, maintains, and/or processes sensitive personal data and health information including personal information, protected health information ("PHI"), and electronic protected health information ("ePHI") (collectively, "Sensitive Data").

3. As set forth in detail below, Plaintiffs allege that PREMERA failed to protect individuals' Sensitive Data from a data breach.

4. As a result, Plaintiffs allege that Defendant has violated the New Jersey Consumer Fraud Act, N.J.S.A., 56:8-1 et seq. ("CFA") and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the United States Department of Health and Human Services Regulations ("HHS") Regulations, 45 C.F.R. §§ 160 et seq. (collectively, "HIPAA").

5. The Attorney General and the Director commence this action to halt Defendant's unconscionable commercial practices, misrepresentations, to enforce compliance with HIPAA, and obtain other authorized relief.

PARTIES AND JURISDICTION

6. The Attorney General is charged with the responsibility of enforcing the CFA, N.J.S.A. 56:8-1 et seq. The Director is charged with the responsibility of administering the CFA, on behalf of the Attorney General.

7. The Attorney General as parens patriae for New Jersey and on behalf of the State in its sovereign capacity, may, pursuant to 42 U.S.C. § 1320d-5(d), enforce the provisions of

HIPAA. Plaintiffs provided prior written notice of this action to the Secretary of HHS, pursuant to 42 U.S.C. § 1320d-5(d)(4).

8. Jurisdiction is proper because Defendant has transacted business within New Jersey or has engaged in conduct impacting New Jersey or its residents at all times relevant to this complaint.

VENUE

9. Pursuant to R. 4:3-2, venue is proper in Mercer County because the Attorney General maintains an office there.

GENERAL ALLEGATIONS COMMON TO ALL COUNTS

10. On March 17, 2015, PREMERA publicly announced that it had discovered unauthorized access to its networks, which exposed the Sensitive Data of eleven (11) million individuals. Upon further investigation, PREMERA revised the number of affected consumers to 10.466 million, approximately 40.000 of whom were New Jersey residents.

11. On January 29, 2015, PREMERA discovered that an unauthorized party may have gained unauthorized access to Protected Health Information and Personal Information. The unauthorized party had access to PREMERA's computer network from May 5, 2014 through March 6, 2015.

12. The unauthorized party took advantage of multiple weaknesses in PREMERA's data security, including known cybersecurity risks that PREMERA failed to appropriately and adequately address. Many of these weaknesses – such as inadequate safeguards against phishing attempts, inadequate network segmentation, ineffective password management policies, ineffectively configured security tools, and inadequate patch management – had been identified as weaknesses in PREMERA's network in the years leading up to the breach by PREMERA's own internal information technology (IT) auditors and third-party cybersecurity assessors.

13. PREMERA failed to provide adequate resources to protect Sensitive Data. Additionally, PREMERA did not appropriately address or mitigate known risks, thereby failing to evaluate and adjust its security program in light of relevant circumstances.

14. PREMERA's security failures occurred in spite of state and federal privacy laws that mandate data security and other safeguards to protect Sensitive Data. For example, HIPAA sets forth strict rules and standards to protect data from unauthorized access. These include requirements to inventory ePHI, ensure appropriate access privileges to ePHI based on job function, secure physical access to data centers, regularly monitor login attempts, regularly and accurately assess risks to ePHI, update its security program to protect against known cybersecurity threats, and adequately mitigate identified risks.

15. Prior to and during the data breach, PREMERA made representations about how it protects consumer privacy and safeguards Sensitive Data in its privacy notices: "We take steps to secure our buildings and electronic systems from unauthorized access."; "We are committed to maintaining the confidentiality of your personal financial and health information."; "We authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims." After PREMERA publically announced the data breach, the company misrepresented the scope and severity of the data breach to affected consumers and misrepresented the security measures PREMERA had in place at the time of the breach. For example, PREMERA provided its call-center agents with a script that stated "[w]e have no reason to believe that any of your information was accessed or misused" and "[t]here were already significant security measures in place to protect your information." All of these assertions are contradicted by PREMERA's numerous security failures and violations of the CFA and HIPAA and post-breach analysis.

16. PREMERA's failure to adequately safeguard Sensitive Data permitted unauthorized access to the Sensitive Data of 10,466,000 individuals for nearly a year in violation of HIPAA and the CFA.

COUNT I

VIOLATIONS OF HIPAA

17. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

18. At all relevant times, PREMERA has been a Covered Entity and a Business Associate, pursuant to HIPAA, specifically 45 C.F.R. § 160.103.

19. At all relevant times, PREMERA has maintained the ePHI of millions of individuals, pursuant to HIPAA, specifically 45 C.F.R. §160.103.

20. As a Covered Entity and Business Associate, PREMERA is required to comply with the HIPAA standards, safeguards, and implementation specifications that govern the privacy of ePHI, including the Privacy Rule and the Security Rule. 45 C.F.R. Part164, Subparts. A, C, & E.

21. As described above, PREMERA failed to comply with the following standards, administrative safeguards, physical safeguards, technical safeguards, and implementation specifications as required by HIPAA, the Privacy Rule, and the Security Rule:

a. PREMERA failed to review and modify security measures as needed to continue the provision of reasonable and appropriate protection of ePHI in accordance with the implementation specifications of the Security Rule, in violation of 45 C.F.R. § 164.306(e).

b. PREMERA failed to conduct an accurate and thorough risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI it held, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(A).

c. PREMERA failed to implement adequate security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(B).

d. PREMERA failed to adequately implement and follow procedures to regularly review records of information system activity, including but not limited to audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D).

e. PREMERA failed to adequately ensure that all members of its workforce had appropriate access to ePHI in violation of 45 C.F.R. § 164.308(a)(3)(i).

f. PREMERA failed to adequately identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that were known to it; and document security incidents and their outcomes, in violation of 45 C.F.R. § 164.308(a)(6)(ii).

g. PREMERA failed to adequately update its security awareness and training program to address known deficiencies, in violation of 45 C.F.R. § 164.308(a)(5)(ii)(A).

h. PREMERA failed to adequately implement policies and procedures to guard against, detect, and report malicious software, in violation 45 C.F.R. § 164.308(a)(5)(ii)(B).

i. PREMERA failed to adequately implement policies and procedures for monitoring log in attempts and reporting discrepancies, in violation of 45 C.F.R. § 164.308 (a)(5)(ii)(C).

j. PREMERA failed to adequately implement adequate password management policies and procedures, in violation of 45 C.F.R. § 164.308(a)(5)(ii)(D).

k. PREMERA failed to adequately implement policies and procedures to safeguard its facility and the equipment therein from unauthorized physical access, tampering and theft, in violation of 45 C.F.R. § 164.310(a)(2)(ii).

l. PREMERA failed to adequately perform periodic technical and nontechnical evaluations, based initially upon the HIPAA standards, and subsequently, in response to environmental or operational changes affecting the security of ePHI, that establishes the extent to which Premera's security policies and procedures meet the requirements of 45 C.F.R. § 164.308 in violation of 45 C.F.R. § 164.308(a)(8).

m. PREMERA failed to adequately implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

n. PREMERA failed to adequately implement policies and procedures to protect ePHI from improper alteration or destruction, in violation of 45 C.F.R. § 164.312(c)(1).

o. PREMERA permitted unauthorized access to ePHI in violation of the Privacy Rule, 45 C.F.R. § 164.502 et seq.

p. PREMERA failed to adequately train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b)(l).

q. PREMERA failed to reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy Rule, in violation of 45 C.F.R. § 164.530(c)(2)(i).

22. Each violation of the above standards, administrative safeguards, physical safeguards, technical safeguards, and/or implementation specifications by PREMERA constitutes a separate violation of HIPAA on each day the violation occurred. 42 U.S.C. § 1320d-5(d)(2); 45 C.F.R. § 160.406. Plaintiffs separately allege each and every HIPAA violation identified in Paragraph 21 herein.

23. Plaintiffs are entitled to statutory damages pursuant to 42 U.S.C. § 1320d-5(d)(2) and attorneys' fees pursuant to 42 U.S.C. § 1320d-5(d)(3).

COUNT II

VIOLATION OF THE CFA (UNCONSCIONABLE COMMERCIAL PRACTICES)

24. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

25. The CFA, N.J.S.A. 56:8-2, prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing[] concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with the sale or advertisement of any merchandise...

26. The CFA defines "merchandise" as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." N.J.S.A. 56:8-1(c) (emphasis added).

27. At all relevant times, Defendants have offered for sale and sold merchandise within the meaning of the CFA, specifically health insurance plans.

28. PREMERA has engaged in unconscionable commercial practices including, but not limited to, each of the above-referenced practices described in Paragraph 21.

29. Each unconscionable commercial practice by PREMERA constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

COUNT III

VIOLATION OF THE CFA (MISREPRESENTATIONS)

30. Plaintiffs repeat and reallege the allegations in the preceding paragraphs as if more fully set forth herein.

31. PREMERA has engaged in acts or practices that constitute violations of the CFA, N.J.S.A. 56:8-2 by making or causing to be made untrue or misleading statements concerning: (1) the scope and severity of the breach to affected consumers; and (2) the privacy and security safeguards PREMERA had in place to protect Sensitive Data.

32. At the time these representations were made, PREMERA knew or should have known that these representations were untrue or misleading.

33. Each misrepresentation by PREMERA constitutes a separate violation under the CFA, N.J.S.A. 56:8-2.

PRAYER FOR RELIEF

WHEREFORE, based upon the foregoing allegations, Plaintiffs respectfully request that the Court enter judgment against PREMERA:

(a) Finding that the acts and omissions of PREMERA constitute multiple instances of unlawful practices in violation of HIPAA and the CFA;

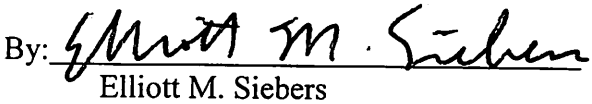
(b) Permanently enjoining PREMERA and its owners, officers, directors, employees, representatives, independent contractors, and all other persons or entities directly under its control, from engaging in, continuing to engage in, or doing any acts or practices in violation of HIPAA or the CFA, including but not limited to, the acts and practices alleged in this Complaint;

(c) Directing PREMERA to pay statutory civil penalties, in accordance, with the accompanying Final Consent Judgment for each and every violation of HIPAA, in accordance with 42 U.S.C. § 1320d-5(d)(2) and 45 C.F.R. § 160.406, and for each and every violation of the CFA, in accordance with N.J.S.A. 56:8-13;

(d) Directing PREMERA to pay costs and fees, including attorneys' fees, in accordance with the accompanying Final Consent Judgment as authorized by HIPAA, 42 U.S.C. §1320d-5(d)(3), and the CFA, N.J.S.A. 56:8-11 and N.J.S.A. 56:8-19; and

(e) Granting such other relief as the interest of justice may require.

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

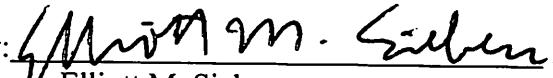
By: 
Elliott M. Siebers
Deputy Attorney General

Dated: July 11, 2019

RULE 4:5-1 CERTIFICATION

I certify, to the best of my information and belief, that the matter in controversy in this action involving the aforementioned violations of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1 et seq., and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services Regulations, 45 C.F.R. §160 et seq., is not the subject of any other action pending in any other court of this State. I further certify, to the best of my information and belief, that the matter in controversy in this action is not the subject of a pending arbitration proceeding in this State, nor is any other action or arbitration proceeding contemplated. I certify that there is no other party who should be joined in this action at this time.

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By: 
Elliott M. Siebers
Deputy Attorney General

Dated: July 11, 2019

RULE 1:38-7(c) CERTIFICATION OF COMPLIANCE

I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b).

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By: Elliott M. Siebers
Elliott M. Siebers
Deputy Attorney General

Dated: July 11, 2019

DESIGNATION OF TRIAL COUNSEL

Pursuant to R. 4:25-4, Deputy Attorney General Elliott M. Siebers is hereby designated as trial counsel for the Plaintiffs in this action.

GURBIR S. GREWAL
ATTORNEY GENERAL OF NEW JERSEY
Attorney for Plaintiffs

By: Elliott M. Siebers
Elliott M. Siebers
Deputy Attorney General

Dated: July 11, 2019