Electronically Filed
7/11/2019 7:32 AM
Steven D. Grierson
CLERK OF THE COURT

COMPB
AARON D. FORD
Attorney General
ERNEST D. FIGUEROA
Consumer Advocate
LUCAS J. TUCKER (Bar No. 010252)
Senior Deputy Attorney General
LAURA M. TUCKER (Bar No. 013268)
Senior Deputy Attorney General
State of Nevada, Office of the Attorney General
Bureau of Consumer Protection
8945 W. Russell Road, #204
Las Vegas, Nevada 89148
702-486-3256 ph
ltucker@ag.nv.gov
lmtucker@ag.nv.gov
Attorneys for Plaintiff, State of Nevada

CASE NO: A-19-798251-B
Department 11

DISTRICT COURT
CLARK COUNTY, NEVADA

STATE OF NEVADA, Plaintiff, vs. PREMERA BLUE CROSS, Defendants.	CASE NO.: DEPT NO.: **BUSINESS COURT REQUESTED** **ARBITRATION EXEMPTION—** **Action in Equity**

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff, State of Nevada, by AARON D. FORD, Attorney General, ERNEST D. FIGUEROA, Consumer Advocate, and his deputies, LUCAS J. TUCKER, Senior Deputy Attorney General, and LAURA M. TUCKER, Senior Deputy Attorney General, brings this action against Defendant Premera Blue Cross ("Defendant" or "Premera") for violation of the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903, et seq., the Nevada Security of Personal Information Act, Nev. Rev. Stat. §§ 603A.010, 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

Case Number: A-19-798251-B

Health Act, Pub. L. No. 111-5, 123 Stat. 226, as well as the Department of Health and Human Services ("HHS") Regulations, 45 C.F.R. §§ 160 *et seq.* (collectively "HIPAA").

PARTIES

1. Plaintiff State of Nevada ("State") is represented by AARON D. FORD, Attorney General of the State of Nevada, who is charged, inter alia, with the enforcement of the Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. §§ 598.0903-.0999 and Nevada Security of Personal Information Act, Nev. Rev. Stat. §§ 603A.010, et seq., and is authorized to bring this action pursuant to Nev. Rev. Stat. § 598.0963 and Nev. Rev. Stat. § 603A.290. Plaintiff asserts HIPAA claims pursuant to 42 U.S.C. 1320d-5(d)(1).

2. 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.

3. Premera is a "covered entity" and a "business associate" within the meaning of 45 C.F.R. § 160.103, and required to comply with the HIPAA federal standards governing the privacy and security of ePHI, including the Privacy and Security Rules. See 45 C.F.R. § 164.302.

4. In the course of its business, Premera collects, maintains, and/or processes sensitive personal data and health information including "personal information" as defined in Nev. Rev. Stat. § 603A.040 ("Personal Information"), protected health information ("PHI") and electronic protected health information ("ePHI") (collectively, "sensitive data").

JURISDICTION AND VENUE

5. Jurisdiction is proper because Defendant has transacted business within the State of Nevada or has engaged in conduct impacting Nevada or its residents at all times relevant to this complaint.

6. Venue is proper pursuant to Nev. Rev. Stat. § 598.0989(3).

7. The Attorney General has provided, or soon after filing will provide, written notice of this action to the Secretary of HHS as required by 42 U.S.C. § 1320d-5(d)(4).

FACTS

8. Premera is a Washington health insurance company. As a health insurance company, Premera collects and maintains sensitive consumer data, including Personal Information, ePHI and PHI. Premera has an obligation to secure such sensitive health data pursuant to state and federal laws.

9. On March 17, 2015, Premera publicly announced it had discovered that an unknown user had gained unauthorized access to its networks and that this breach exposed the sensitive information of eleven (11) million individuals. Upon further investigation, Premera revised the number of affected consumer to 10.466 million, approximately 49,529 of whom were Nevada residents. The sensitive information included private health information, Social Security numbers, member identification numbers, bank account information, names, addresses, phone numbers, dates of birth, and email addresses.

10. On January 29, 2015, Premera's cybersecurity expert confirmed the unauthorized access to its networks. Following the breach, Premera's internal investigation revealed that the unauthorized party had access to Premera's network from May 5, 2014 through March 6, 2015. The unauthorized party gained access to the Premera network by taking advantage of multiple weaknesses in Premera's data security.

11. In the years leading up to the breach, Premera's own internal IT auditors and cybersecurity assessors identified multiple network vulnerabilities – such as inadequate safeguards against phishing attempts, inadequate network segmentation, ineffective password management policies, ineffectively configured security tools, and inadequate patch management – many of which Premera accepted without adequate remediation.

12. Premera's corporate culture also failed to provide its IT security team with adequate resources to inspect and safeguard consumer data.

13. For years leading up to the breach, Premera failed to comply with the security and privacy standards of HIPAA. These deficiencies include failure to (i) properly

map ePHI on its networks, (ii) ensure appropriate access privileges to Personal Information and ePHI based on job function, (iii) enforce appropriate safeguards to secure physical access to data centers, (iv) regularly monitor log in attempts, (v) regularly and accurately assess risks to Personal Information and ePHI, (vi) update its security program to protect against known cybersecurity threats, and (vii) adequately mitigate identified risks.

14. Premera's failure to adequately safeguard personal data permitted unauthorized access to the sensitive information of 49,529 Nevada consumers for nearly a year.

15. In 2015, after the 2014 security breach became public, Premera's call center agents represented to consumers, "We have no reason to believe that any of your information was accessed or misused". Premera's call center also told consumers that "There were already significant security measures in place to protect your information." These statements did not disclose the true scope and severity of the data breach, and were misleading regarding the security measures Premera had in place at the time of the breach.

CLAIMS FOR RELIEF

COUNT I: Violation of HIPAA

16. The State realleges and incorporate by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

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

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

19. As a Covered Entity and Business Associate, Premera is required to comply with the HIPAA standards, safeguards, and implementation that govern the privacy of ePHI, including the Privacy Rule and the Security Rule. 45 C.F.R. Part 164, Subparts A, C, & E.

20. 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)(l)(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)(l)(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)(l)(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 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).

21. 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, as to each and every Plaintiff State authorized to enforce HIPAA. 42 U.S.C § 1320d-5(d)(2); 45 C.F.R. § 160.406. The State of Nevada separately alleges each and every HIPAA violation identified in paragraph 20(a)-(q) herein.

22. Plaintiff State of Nevada is separately and independently 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: VIOLATIONS OF NEVADA LAW
(Nevada Deceptive Trade Practices Act and
Nevada Security of Personal Information Act)

23. The State of Nevada realleges and incorporates by reference all preceding allegations.

24. At all times during the breach window alleged in Paragraph 10, and continuing to this day, the Nevada Attorney General has authority to enforce (i) Nevada's deceptive trade practice laws in NRS Chapter 598[1], and (ii) Nevada's laws governing security and privacy of personal information in NRS Chapter 603A[2], including the authority to seek injunctive and other appropriate relief for violations of those laws.

25. In all matters alleged herein, Premera acted in the course of its business or occupation within the meaning of Nev. Rev. Stat. §§ 598.0903 to 598.0999 by providing services to Nevada consumers, including insurance plans and other health services, and advertising, marketing and soliciting business in the State of Nevada.

26. In the course of its business, Premera collects or otherwise deals with nonpublic Personal Information and is a "data collector" as defined in Nev. Rev. Stat. §

[1] Nev. Rev. Stat. § 598.0963(3).
[2] Nev. Rev. Stat. § 603A.920 (2005), recodified as Nev. Rev. Stat. § 603A.290 (2017).

603A.030.

27. Because Premera maintains records which contain Personal Information of Nevada consumers, Nev. Rev. Stat. § 603A.210 requires Premera to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, use or disclosure.

28. By its alleged acts and omissions described in paragraph 20(a)-(q) *supra*, Premera did not comply with its obligations under Nev. Rev. Stat. § 603A.210 to the extent these deficiencies exposed Personal Information.

29. As alleged in paragraph 11 *supra*, the aforementioned deficiencies in Premera's network were consistently observed by Premera's own internal IT auditors and cybersecurity assessors in the years leading up to the breach.

30. In addition, Premera deceived Nevada consumers after the breach by:

a) Misrepresenting to consumers whether their personal information was at risk; and

b) Misrepresenting to consumers the security measures in place at Premera at the time of the breach.

31. Premera's misrepresentations to Nevada consumers constitute multiple violations of Nevada's deceptive trade practice laws:

a) Nev. Rev. Stat. § 598.0915(7), a person engages in a deceptive trade practice by representing that goods or services for sale or lease are of a particular standard, quality or grade, if he or she knows or should know that they are of another standard, quality or grade; and

b) Nev. Rev. Stat. § 598.0923(2), a person engages in a deceptive trade practice by failing to disclose a material fact in connection with the sale or lease of goods or services.

32. In addition, pursuant to Nev. Rev. Stat. § 598.0923(3), a person engages in a deceptive trade practice by violating a state or federal statute or regulation relating to the sale or lease of goods or services. Accordingly, (i) Premera's violation of Nev. Rev. Stat. §

603A.210, and (ii) each of Premera's violation of HIPAA standards, safeguards and implementation specifications alleged in paragraph 20 *supra*, each constitute an independent violation of Nev. Rev. Stat. § 598.0923(3).

33. Altogether, Premera's acts and omissions constitute violations of Nev. Rev. Stat. §§ 598.0915(7), 598.0923(2), 598.0923(3) and 603A.210.

PRAYER FOR RELIEF

WHEREFORE, PLAINTIFF prays for judgment as follows.

34. A judgment determining that Defendant has violated Nev. Rev. Stat. §§ 598.0915(7), 598.0923(2), 598.0923(3) and 603A.210, and HIPAA;

35. A permanent injunction prohibiting Defendant from further acts and practices in violation of the Nevada Deceptive Trade Practices Act, the Nevada Security of Personal Information Act, and HIPAA;

36. Civil penalties of up to $5,000 for each violation of the Nevada Deceptive Trade Practices Act, pursuant to Nev. Rev. Stat. § 598.0999(2);

37. Statutory damages under 42 U.S.C. 1320d-5(d)(1) of up to $100 per violation not to exceed $25,000 per calendar year for all violations of an identical requirement or prohibition;

38. The award of investigative and litigation costs and reasonable attorney fees to Nevada; and

39. All such other and further relief as the Court may deem appropriate.

DATED this 11th day of July, 2019.

Respectfully submitted:

AARON D. FORD
Attorney General
ERNEST D. FIGUEROA
Consumer Advocate

By: _____
LUCAS J. TUCKER (Bar No. 010252)
Senior Deputy Attorney General