MARK BRNOVICH
Attorney General
(Firm State Bar No. 14000)
John C. Gray (State Bar No. 028454)
Office of the Attorney General
2005 North Central Avenue
Phoenix, AZ 85004
Telephone: (602) 542-7753
Facsimile: (602) 542-4377
Email: john.gray@azag.gov

Attorneys for Plaintiff

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

STATE OF ARIZONA, *ex rel.* MARK BRNOVICH, Attorney General, Plaintiff, vs. PREMERA BLUE CROSS, Defendant.	Case No. **COMPLAINT**

Plaintiff State of Arizona, *ex rel.* Mark Brnovich, Attorney General (hereinafter "Plaintiff"), brings this action against defendant Premera Blue Cross ("Defendant" or "Premera"), and alleges as follows:

PARTIES

1. Plaintiff brings this action pursuant to 42 U.S.C. 1320d-5(d)(1) and the Arizona Consumer Fraud Act, A.R.S. § 44-1521 *et seq*.

2. Defendant 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 it is required to comply with the federal standards governing the privacy and security of electronic protected health information ("ePHI") under the Health Insurance Portability and Accountability Act ("HIPAA"), 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 protected health information ("PHI") and ePHI (collectively, "sensitive data").

JURISDICTION AND VENUE

5. Jurisdiction is proper because Defendant has, at all relevant times, maintained sufficient contacts with Arizona to make the exercise of jurisdiction in this Court reasonable and just with respect to the claims asserted herein.

6. Venue is proper in this Court pursuant to A.R.S. § 12-401(17).

FACTS

7. On January 29, 2015, Premera discovered that an unauthorized party may have gained unauthorized access to sensitive information. The unauthorized party had access to Premera's computer network from May 5, 2014, through March 6, 2015.

8. Premera publicly announced the breach on March 17, 2015, indicating that the sensitive information of 11 million individuals had been exposed. Upon further investigation, Premera revised the number of affected consumers to 10.466 million, approximately 171,455 of whom were Arizona residents.

9. The unauthorized party had taken advantage of multiple weaknesses in Premera's data security, in which Premera failed to appropriately and adequately address known cybersecurity risks. 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 its own internal IT auditors and cybersecurity assessors.

10. Furthermore, Premera failed to provide adequate resources to protect personal 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.

11. Premera's security failures occurred in spite of state and federal privacy laws, including HIPAA, which require reasonable security, cybersecurity, and other safeguards to protect sensitive information. For example, HIPAA sets forth strict rules and standards to adequately safeguard and protect data from unauthorized access. These include requirements to map ePHI on its networks, ensure appropriate access privileges to ePHI based on job function, include appropriate safeguards to secure physical access to data centers, regularly monitoring log in attempts, regularly and accurately assessing risks to ePHI, updating its security program to protect against known cybersecurity threats, and adequately mitigating identified risks.

12. Thus, Premera's failures to adequately safeguard personal data, which permitted unauthorized access to the sensitive information of more than 10 million individuals for nearly a year, violated HIPAA and the Arizona Consumer Fraud Act.

13. Prior to and during the breach, Premera also misrepresented in its privacy notices that it protects consumer privacy and safeguards sensitive data. For example, Premera claimed: "[w]e take steps to secure our buildings and electronic systems from unauthorized access"; "[w]e are committed to maintaining the confidentiality of your personal financial and health information"; and "[w]e 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."

14. In addition, even after Premera announced the breach, the company continued to misrepresent its purported security measures, and it also misrepresented the scope and severity of the problem. For example, Premera provided its call-center agents with a script that claimed: "[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." Such assertions are contradicted by Premera's numerous security failures and HIPAA violations.

CLAIMS FOR RELIEF

COUNT I: Violation of HIPAA

15. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

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

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

18. As a Covered Entity and Business Associate, Premera is required to comply with HIPAA regulations pertaining to ePHI, including the Privacy Rule and the Security Rule, 45 C.F.R. Part 164, Subparts A, C, & E.

19. 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).

20. 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 state authorized to enforce HIPAA. 42 U.S.C § 1320d-5(d)(2); 45 C.F.R. § 160.406.

21. Each state is separately and independently entitled to statutory damages pursuant to 42 U.S.C. § 1320d-5(d)(2) and attorney fees pursuant to 42 U.S.C. § 1320d-5(d)(3).

COUNT II: VIOLATION OF ARIZONA CONSUMER FRAUD ACT

22. Plaintiff realleges and incorporates by reference the allegations set forth in each of the preceding paragraphs of this Complaint.

23. Premera, in the course of conducting its business, engaged in deceptive and unfair acts and practices in violation of the Arizona Consumer Fraud Act, A.R.S. § 44-1521 *et seq.*, by, among other things, failing to implement and maintain reasonable security procedures and practices appropriate to protect the sensitive information of Arizona residents, as alleged above.

24. At all relevant times, Premera knew or should have known that its actions were of the nature prohibited by the Arizona Consumer Fraud Act, such that Premera acted willfully as defined in A.R.S. § 44-1531(B).

PRAYER FOR RELIEF

WHEREFORE, PLAINTIFF prays for judgment as follows.

25. A judgment determining that Defendant has violated the Arizona Consumer Fraud Act, A.R.S. § 44-1521 *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.A. § 160 *et seq*.;

26. A permanent injunction prohibiting Defendant from further acts and practices in violation of the Arizona Consumer Fraud Act and HIPAA;

27. Civil penalties of up to $10,000 for each violation of the Arizona Consumer Fraud Act pursuant to A.R.S. § 44-1531;

28. 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;

29. The award of investigative and litigation costs and reasonable attorney fees to Plaintiff; and

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

RESPECTFULLY SUBMITTED this 11th day of July 2019.

MARK BRNOVICH
Attorney General

By: _____
John C. Gray
Assistant Attorney General
Attorneys for Plaintiff