

COPY

FILED

JUL 11 2019

ANGIE SPARKS, Clerk of District Court
By: AMBER M. MULLEN Deputy Clerk

TIMOTHY C. FOX
Montana Attorney General
KELLEY L. HUBBARD
Assistant Attorney General
P.O. Box 200151
555 Fuller Ave.
Helena, MT 59620-0151
(406) 444-2026
khubbard@mt.gov

MONTANA FIRST JUDICIAL DISTRICT COURT
LEWIS AND CLARK COUNTY

STATE OF MONTANA,

Plaintiff,

v.

PREMERA BLUE CROSS,

Defendant.

Cause No. ADV-2019-9360

COMPLAINT

Plaintiff, the State of Montana, by and through its Attorney General, brings this action against Defendant Premera Blue Cross (“Defendant” or “Premera”) for violation the Montana Unfair Trade Practices and Consumer Protection Act (“Consumer Protection Act”), the Montana Impediment of Identity Theft Act, and HIPAA, and alleges the following upon information and belief:

PARTIES

1. Plaintiff is the State of Montana (the “State” or the “Plaintiff”), represented by Attorney General, Timothy C. Fox, bringing suit in his or her official capacity pursuant to 42 U.S.C. 1320d-5(d)(1) and Mont. Code Ann. § 30-14-111(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 the Montana Impediment of Identity Theft Act, Mont. Code Ann. § 30-14-1702(7) and -1704(4)(b), e.g. personally identifiable information (“PII”), medical record 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 or has engaged in conduct impacting Montana or its residents at all times relevant to this complaint.

6. Venue is proper pursuant to Mont. Code Ann. § 30-14-111(3).

FACTS

7. On March 17, 2015, Premera publicly announced that it had discovered unauthorized access to its networks, which exposed the sensitive information of eleven (11) million individuals. Upon further investigation, Premera revised the number of affected consumer to 10.466 million, approximately 111,222 of whom were Montana residents.

8. 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.

9. The unauthorized party took 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 took place 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 monitor log in attempts, regularly and accurately assess risks to ePHI, updating its security program to protect against known cybersecurity threats, and adequately mitigate identified risks.

12. 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 publicly 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 that “[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 constitute deceptive statements in violation of the Montana Consumer Protection Act.

13. Premera’s failure to adequately safeguard personal data permitted unauthorized access to the sensitive information of 10,466,000 individuals for nearly a year in violation of HIPAA, the Montana Consumer Protection Act, and the Montana Impediment of Identity Theft Act.

CLAIMS FOR RELIEF

COUNT I: Violation of HIPAA

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

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

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

17. 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.

18. 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 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)(1).

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).

19. 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. Each Plaintiff State separately alleges each and every HIPAA violation identified in paragraph 5.5(a)-(q) herein.

20. Each and every Plaintiff State 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: VIOLATION OF THE MONTANA CONSUMER PROTECTION ACT
AND IMPEDIMENT OF IDENTITY THEFT ACT**

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

22. Premera, in the course of conducting its business, willfully engaged in acts or practices that were unfair or deceptive, and therefore violated Mont. Code Ann. § 30-14-103, by making deceptive statements regarding the safety and confidentiality of its customers' Personal Information and by failing to implement and maintain reasonable security procedures and practices appropriate to protect the Personal Information of Montana residents that Premera owned, licensed, or maintained, and thus did not protect that Personal Information from unauthorized access, use, destruction, modification, or disclosure.

PRAYER FOR RELIEF

Plaintiff prays for judgment as follows.

1. A Judgment determining that Defendant has violated the Montana Consumer Protection Act and the Impediment of Identity Theft Act, Mont. Code Ann. §§ 30-14-101 *et seq.* and -1701 *et seq.*, and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1938, 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.*;
2. A permanent injunction prohibiting Defendant from further acts and practices in violation of the Montana Consumer Protection Act, Impediment of Identity Theft Act, and HIPAA;
3. Civil penalties of up to \$10,000 for each violation of the Montana Consumer Protection Act pursuant to Mont. Code Ann. § 30-14-142(2);

4. 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;
5. The award of investigative and litigation costs and reasonable attorney fees to the State pursuant to Mont. Code Ann. § 30-14-131(2); and
6. All such other and further relief as the Court may deem appropriate.

DATED this 11th day of July, 2019.

Respectfully submitted,

TIMOTHY C. FOX
Montana Attorney General



KELLEY L. HUBBARD
Assistant Attorney General