

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

STATE OF WASHINGTON  
SNOHOMISH COUNTY SUPERIOR COURT

STATE OF WASHINGTON,  
  
Plaintiff,  
  
v.  
  
PREMERA BLUE CROSS,  
  
Defendant.

NO.  
COMPLAINT **19 2 06171 31**

Plaintiff, State of Washington, by and through its attorneys Robert W. Ferguson, Attorney General, Tiffany L. Lee, and Andrea M. Alegrett, Assistant Attorneys General, brings this action against Defendant Premera Blue Cross (“Defendant” or “Premera”). The State alleges that Premera engaged in unfair and deceptive acts or practices in violation of the Consumer Protection Act, RCW 19.86, by failing to adequately safeguard consumer information, and violated 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 (“HHS”) Regulations, 45 C.F.R. Part 160 *et seq.* (collectively “HIPAA”).

Plaintiff alleges the following on information and belief:

**I. PARTIES**

1.1 Plaintiff is the Attorney General of the State of Washington.

COPY



### III. FACTS

1  
2 3.1 Premera is a Washington health insurance company. As a health insurance  
3 company, Premera collects and maintains sensitive consumer data, including ePHI and PHI.  
4 Premera has an obligation to secure such sensitive health data pursuant to state and federal laws.

5 3.2 On March 17, 2015, Premera publicly announced that it had discovered that an  
6 unknown user had gained unauthorized access to its networks and that this breach exposed the  
7 sensitive information of eleven (11) million individuals. Upon further investigation, Premera  
8 revised the number of affected consumer to 10.466 million, approximately 6.4 million of whom  
9 were Washington residents. The sensitive information included private health information,  
10 Social Security numbers, member identification numbers, bank account information, names,  
11 addresses, phone numbers, dates of birth, and email addresses.

12 3.3 On January 29, 2015, Premera's cybersecurity expert confirmed the unauthorized  
13 access to its networks. Following the breach, Premera's internal investigation revealed that the  
14 unauthorized party had access to Premera's network from May 5, 2014, through March 6, 2015.  
15 The unauthorized party gained access to the Premera network by taking advantage of multiple  
16 weaknesses in Premera's data security. In the years leading up to the breach, Premera's own  
17 internal IT auditors and cybersecurity assessors identified multiple network vulnerabilities—  
18 such as inadequate safeguards against phishing attempts, inadequate network segmentation,  
19 ineffective password management policies, ineffectively configured security tools, and  
20 inadequate patch management—many of which Premera accepted without adequate  
21 remediation.

22 3.4 Premera's corporate culture also failed to provide its IT security team with  
23 adequate resources to inspect and safeguard consumer data.

24 3.5 For years leading up to the breach, Premera failed to comply with the security  
25 and privacy standards of HIPAA. These include, failing to properly map ePHI on its networks,  
26 ensuring appropriate access privileges to ePHI based on job function, enforcing appropriate

1 safeguards to secure physical access to data centers, regularly monitoring log in attempts,  
2 regularly and accurately assessing risks to ePHI, updating its security program to protect against  
3 known cybersecurity threats, and adequately mitigating identified risks.

4 3.6 Premera's failure to adequately safeguard personal data permitted unauthorized  
5 access to the sensitive information of over 6 million Washington consumers for nearly a year.

6 3.7 Prior to and during the data breach, Premera made representations about how it  
7 protects consumer privacy and safeguards sensitive data in its privacy notices: "We take steps to  
8 secure our buildings and electronic systems from unauthorized access."; "We are committed to  
9 maintaining the confidentiality of your personal financial and health information."; "We  
10 authorize access to your personal information by our employees and business associates only to  
11 the extent necessary to conduct our business of serving you, such as paying your claims." After  
12 Premera publicly announced the data breach, the company misrepresented the scope and severity  
13 of the data breach to affected consumers and misrepresented the security measures Premera had  
14 in place at the time of the breach. For example, Premera provided its call-center agents with a  
15 script that stated that "[w]e have no reason to believe that any of your information was accessed  
16 or misused" and "[t]here were already significant security measures in place to protect your  
17 information." All of these assertions are contradicted by Premera's numerous security failures  
18 and violations of the CPA and HIPAA.

19 **IV. FIRST CAUSE OF ACTION**  
20 **(VIOLATION OF THE HIPAA)**

21 4.1 The State realleges and incorporates by reference the allegations set forth in each  
22 of the preceding paragraphs of this Complaint.

23 4.2 At all times relevant, Premera has been a Covered Entity and a Business  
24 Associate pursuant to HIPAA, specifically 45 C.F.R. § 160.103.

25 4.3 At all relevant times, Premera has maintained the ePHI of millions of individuals  
26 pursuant to HIPAA, specifically 45 C.F.R. § 160.103.

1           4.4    As a Covered Entity and Business Associate, Premera is required to comply with  
2 the HIPAA standards, safeguards, and implementation that govern the privacy of ePHI, including  
3 the Privacy Rule and the Security Rule. 45 C.F.R. Part 164, Subparts A, C, & E.

4           4.5    Premera failed to comply with the following standards, administrative  
5 safeguards, physical safeguards, technical safeguards, and implementation specifications as  
6 required by HIPAA, the Privacy Rule, and the Security Rule:

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

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

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

16          d.    Premera failed to adequately implement and follow procedures to  
17 regularly review records of information system activity, including but not limited to audit logs,  
18 access reports and security incident tracking reports, in violation of  
19 45 C.F.R. § 164.308(a)(1)(ii)(D).

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

22          f.    Premera failed to adequately identify and respond to suspected or known  
23 security incidents; mitigate, to the extent practicable, harmful effects of security incidents that  
24 were known to it; and document security incidents and their outcomes, in violation of  
25 45 C.F.R. § 164.308(a)(6)(ii).

26          g.    Premera failed to adequately update its security awareness and training

1 program to address known deficiencies, in violation of 45 C.F.R. § 164.308(a)(5)(ii)(A).

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

4 i. Premera failed to adequately implement policies and procedures for  
5 monitoring log-in attempts and reporting discrepancies, in violation of  
6 45 C.F.R. § 164.308(a)(5)(ii)(C).

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

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

12 l. Premera failed to adequately perform periodic technical and nontechnical  
13 evaluations, based initially upon the HIPAA standards, and subsequently, in response to  
14 environmental or operational changes affecting the security of ePHI, that establishes the extent  
15 to which Premera's security policies and procedures meet the requirements of  
16 45 C.F.R. § 164.308 in violation of 45 C.F.R. § 164.308(a)(8).

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

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

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

25 p. Premera failed to adequately train all members of its workforce on the  
26 policies and procedures with respect to PHI as necessary and appropriate for the members of its

1 workforce to carry out their functions and to maintain the security of PHI, in violation of  
2 45 C.F.R. § 164.530(b)(1).

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

6 4.6 Each violation of the above standards, administrative safeguards, physical  
7 safeguards, technical safeguards, and/or implementation specifications by Premera constitutes a  
8 separate violation of HIPAA on each day the violation occurred, as to each and every Plaintiff  
9 State authorized to enforce HIPAA. 42 U.S.C § 1320d-5(d)(2); 45 C.F.R. § 160.406. Each  
10 Plaintiff State separately alleges each and every HIPAA violation identified in paragraph  
11 5.5(a)-(q) herein.

12 4.7 Each and every Plaintiff State is separately and independently entitled to statutory  
13 damages pursuant to 42 U.S.C. § 1320d-5(d)(2) and attorneys' fees pursuant to  
14 42 U.S.C. § 1320d-5(d)(3).

15 **V. SECOND CAUSE OF ACTION**  
16 **(VIOLATION OF THE CONSUMER PROTECTION ACT, RCW 19.86)**

17 5.1 The State realleges and incorporates by reference the allegations set forth in each  
18 of the preceding paragraphs of this Complaint.

19 5.2 Premera engages in "trade" or "commerce" within the meaning of the  
20 Consumer Protection Act, RCW 19.86.010(2), by providing services to Washington consumers,  
21 including insurance plans and other health services, and advertising, marketing, and soliciting  
22 business in Washington.

23 5.3 Premera engaged in unfair and deceptive acts or practices within the meaning of  
24 RCW 19.86.020 by misrepresenting directly or indirectly, the following:

25 a. Misrepresenting that Premera adequately safeguards personal information  
26 and ePHI from unauthorized access or exposure;



