ELECTRONICALLY FILED
7/11/2019 10:16 AM
03-CV-2019-901292.00
CIRCUIT COURT OF
MONTGOMERY COUNTY, ALABAMA
GINA J. ISHMAN, CLERK

IN THE CIRCUIT COURT OF MONTGOMERY COUNTY, ALABAMA
FIFTEENTH JUDICIAL CIRCUIT

STATE OF ALABAMA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**CV NO.:_____**
	)	
PREMERA BLUE CROSS,	)	
	)	
Defendant.	)	

COMPLAINT FOR INJUNCTIVE AND OTHER RELIEF

Plaintiff, State of Alabama, by and through its Attorney General, Steve Marshall, and the undersigned Assistant Attorney General, Noel Barnes, brings this action against Defendant Premera Blue Cross ("Defendant" or "Premera"). The State alleges that Premera engaged in unlawful and deceptive acts or practices in violation of the Deceptive Trade Practices Act ("DTPA"), Ala. Code § 8-19-1 *et seq.*, by failing to adequately safeguard consumer information, and engaged in violations of 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. §§ 160 *et seq.* (collectively "HIPAA").

The State alleges the following on information and belief:

I. PARTIES

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

1.2 Defendant is Premera Blue Cross ("Premera"), a Washington Non-Profit Corporation with its principal place of business at 7001 220th St. SW, Mountlake Terrace, WA, 98043.

1.3 In the course of its business, Premera collects, maintains, and/or processes sensitive personal data and health information including protected health information ("PHI") and electronic

protected health information ("ePHI") (collectively, "sensitive data") from Alabama consumers.

1.4 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.

II. JURISDICTION AND VENUE

2.1 Plaintiff files this Complaint and institutes these proceedings pursuant to the statutory authority in the DTPA, §§ 8-19-4, 8-19-8, and 8-19-11 of the Code of Alabama.

2.2 This Court has personal jurisdiction over Defendant pursuant to the DTPA § 8-19-11(b) because Defendant has engaged in the conduct set forth in this Complaint in Montgomery County and elsewhere in the State of Alabama.

2.3 Venue is proper in Montgomery County pursuant to the Code of Alabama §§ 8-19-4, 8-19-8, 8-19-11, 12-11-30, and 12-11-31 because Defendant transacts business in Montgomery County and engaged in the conduct set forth in this Complaint in Montgomery County and elsewhere in the State of Alabama.

2.4 The Attorneys General have or will, shortly after filing, provide written notice of this action to the Secretary of HHS as required by 42 U.S.C. § 1320d-5(d)(4).

III. FACTS

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

3.2 On March 17, 2015, Premera publicly announced that it had discovered that an unknown user had gained unauthorized access to its networks and that this breach exposed the sensitive information of eleven million individuals. Upon further investigation, Premera revised the number of affected consumer to 10.466 million, approximately 27,775 of whom were Alabama 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.

3.3 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. 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.

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

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

3.6 Premera's failure to adequately safeguard personal data permitted unauthorized access to the sensitive information of over twenty-seven thousand Alabama consumers for nearly a year.

3.7 In 2015, after the 2014 security breach became public, Premera's call center agents represented to consumers, "[w]e 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.

3.8 Prior to and during the data breach, Premera made representation 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 authorized 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 withy 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 violation of the CMIA and HIPAA.

IV. FIRST CAUSE OF ACTION
(Violation of the HIPAA)

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

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

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

4.4 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.

4.5 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 establish 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 ePHI 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).

4.6 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 4.5(a)-(q) herein.

4.7 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).

V. SECOND CAUSE OF ACTION
(Violation of the Deceptive Trade Practices Act)

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

5.2 Premera engages in "trade or commerce" within the meaning of the DTPA, § 8-19-3(8), by providing services to Alabama consumers, including insurance plans and other health services, and advertising, marketing, and soliciting business in Alabama.

5.3 Premera engaged in unlawful deceptive acts or practices within the meaning of § 8-19-5 by misrepresenting directly or indirectly, the following:

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

b. Failing to maintain appropriate administrative and technical safeguards to protect consumers' personal information and ePHI;

c. Failing to remedy or mitigate known security risks that Premera was alerted to, which had the potential of exposing personal information and ePHI; and

d. Misrepresenting to consumers, after the breach, the security measures in place at Premera at the time of the breach.

5.4 Premera's conduct was unlawful and deceptive, and had the capacity to deceive a substantial number of Alabama consumers.

5.5 Premera's conduct affects the public interest.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, State of Alabama, prays for relief as follows:

6.1 That the Court adjudge and decree that the Defendant has engaged in the conduct complained of herein;

6.2 That the Court adjudge and decree that the conduct complained of constitutes deceptive acts and practices and is unlawful in violation of the DTPA and violates HIPAA;

6.3 That the Court issue a permanent injunction enjoining and restraining the Defendant, and its representatives, successors, assigns, officers, agents, servants, employees, and all other persons acting or claiming to act for, on behalf of, or in active concert or participation with the Defendant, from continuing or engaging in the unlawful conduct complained of herein;

6.4 That the Court assess civil penalties pursuant to DTPA § 8-19-11 of up to two thousand dollars ($2,000) per violation against the Defendant for each and every violation of the DTPA caused by the conduct complained of herein;

6.5 That the Court assess 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;

6.6 That the Court make such orders pursuant to the DTPA to provide for appropriate restitution to consumers because of the conduct complained of herein;

6.7 That the Court make such orders pursuant to DTPA § 8-19-11(e) to provide that the Plaintiff, State of Alabama, recovers from the Defendant the costs of this action, including reasonable attorneys' fees; and

6.8 For such other relief as the Court may deem just and proper.

DATED this 11th day of July, 2019.

State of Alabama
STEVE MARSHALL
Attorney General of the State of Alabama

By: */s/ Noel S. Barnes*

NOEL S. BARNES
Assistant Attorney General
Office of the Alabama Attorney General
501 Washington Avenue
Montgomery, Alabama 36130-0152
(334) 353-9196
nbarnes@ago.state.al.us