UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ROSS IMBLER, STUART and ILENE HIRSH, KEVIN SMITH and CATHERINE BUSHMAN, SHARIF AILEY, APRIL ALLRED, ROBERT and THERESA FOULON, CRYSTAL HAYES, BARBARA LYNCH, KEVIN MCLALLEN, SURYA PRAKASH, GABRIEL and LAURA WEBSTER, individually and on behalf of the proposed classes,

Plaintiffs,

v.

PREMERA BLUE CROSS, a Washington nonprofit corporation,

Defendant.

NO.

COMPLAINT – CLASS ACTION

JURY DEMAND

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF CONTENTS

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF CONTENTS
(continued)

Page

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiffs Ross Imbler, Stuart and Ilene Hirsh, Kevin Smith and Catherine Bushman, Sharif Ailey, April Allred, Robert and Theresa Foulon, Crystal Hayes, Barbara Lynch, Kevin McLallen, Surya Prakash, Gabriel and Laura Webster, individually and on behalf of the proposed Classes defined below, allege as follows upon personal knowledge, experience, information and belief, including investigation conducted by their attorneys.

I. NATURE OF THE CASE

1. Plaintiffs bring this class action lawsuit against Premera because of its failure to protect the confidential information of millions of consumers-including their names, dates of birth, mailing addresses, telephone numbers, email addresses, Social Security numbers, member identification numbers, medical claims information, financial information, and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information").

2. Premera is one of the largest healthcare benefits companies in the Pacific Northwest and is also a participant in the national Blue Cross Blue Shield Association (which offers healthcare to consumers throughout the United States and its territories, covering more than 105 million Americans). Premera's participation in the Blue Cross Blue Shield Association provides its members with access to healthcare providers throughout the country and provides non-Premera Blue Cross members (referred to as "Blue members") with access to its network.

3. In order to become a Premera member (or, for Blue members, receive healthcare services from a provider within the Premera network), an individual must give Premera his or her Sensitive Information. Plaintiffs and the putative class took reasonable steps to preserve the confidentiality of their Sensitive Information in many ways, including protecting the Sensitive Information with confidential passwords and relying upon physician-patient privilege and confidentiality. Premera maintains this Sensitive Information in a centralized database.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

4. As a healthcare benefits provider, Premera is required to protect both its members' and also Blue members' Sensitive Information, including by adopting and implementing specific data security regulations and standards set forth under HIPAA.

5. In addition to its implied statutory obligation, Premera expressly promises—throughout its Notice of Privacy Practices, Code of Conduct, public statements, and other written assurances—to safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards.

6. Unfortunately, Premera's failure to protect the Sensitive Information in its control resulted in one of the largest healthcare data breaches in history. On March 17, 2015, Premera revealed that its computer network had been breached and the Sensitive Information of approximately 11 million of its former and current members, Blue members, and employees was compromised.

7. According to Premera, the breach started in May 2014 and went undetected for nearly one year. Worse yet, after discovering the breach, Premera waited months before notifying all affected individuals preventing Plaintiffs and the Class from taking steps to further prevent the misuse of their Sensitive Information.

8. The breach not only revealed that Premera failed to provide the level of data protection that it promised and that members paid for, it also exposed millions of individuals' Sensitive Information to an increased risk of misuse by unauthorized third parties (e.g., identity theft). In fact, affected individuals face a particularly real risk of misuse here (i.e., to the extent their information hasn't been misused already) because their Sensitive Information was specifically targeted by hackers seeking to steal consumer data. Many of the class members have already suffered medical fraud, tax fraud, credit card fraud, and phishing scams, as a result of Premera's illegal conduct. All class members are in real and imminent danger of the same fate.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

9. Had Premera informed Plaintiffs and other members of the Classes that it would use inadequate security measures—including by using data security practices at odds with its own affirmative representations—members would not have been willing to sign-up or pay for Premera's healthcare benefits at the price charged, if at all, and would not have been willing to provide their Sensitive Information to Premera.

10. Premera's failure to implement adequate security protocols jeopardized millions of consumers' Sensitive Information, fell well short of its statutory and professional standard obligations, fell short of Plaintiffs' and other Class members' reasonable expectations when they provided their Sensitive Information to Premera, and diminished the value of the services that Premera provided (in other words, because Premera failed to disclose its gross security inadequacies, it delivered a fundamentally less useful and less valuable service than the one members paid for).

11. Accordingly, Plaintiffs bring suit, on behalf of themselves and all others similarly situated, to seek redress for Premera's unlawful conduct.

II. PARTIES

12. Plaintiff Ross Imbler is a natural person and citizen of the State of Alaska. Plaintiff Imbler brings this action on behalf of himself and the Nationwide and Alaska Classes, as defined below.

13. Plaintiffs Stuart and Ilene Hirsh are natural persons and citizens of the State of Oregon. Plaintiffs Hirsh bring this action on behalf of themselves and the Nationwide and Oregon Classes, as defined below.

14. Plaintiffs Kevin Smith and Catherine Bushman are natural persons and citizens of the State of Tennessee. Plaintiffs Smith and Bushman bring this action on behalf of themselves and the Nationwide and Tennessee Classes, as defined below.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

15. Plaintiff Sharif Ailey is a natural person and citizen of the State of Texas. Plaintiff Ailey brings this action on behalf of himself and the Nationwide and Texas Classes, as defined below.

16. Plaintiff April Allred is a natural person and citizen of the State of Washington. Plaintiff Allred brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

17. Plaintiffs Robert & Theresa Foulon are natural persons and citizens of the State of Washington. Plaintiffs Foulon bring this action on behalf of themselves and the Nationwide and Washington Classes, as defined below.

18. Plaintiff Crystal Hayes is a natural person and citizen of the State of Washington. Plaintiff Hayes brings this action on behalf of herself and the Nationwide and Washington Classes, as defined below.

19. Plaintiff Kevin McLallen is a natural person and citizen of the State of Washington. Plaintiff McLallen brings this action on behalf of himself and the Nationwide and Washington Classes, as defined below.

20. Plaintiff Surya Prakash is a natural person and citizen of the State of Washington. Plaintiff Prakash brings this action on behalf of himself and the Nationwide and Washington Classes, as defined below.

21. Plaintiffs Gabriel & Laura Webster are natural persons and citizens of the State of Washington. Plaintiffs Webster bring this action on behalf of themselves and the Nationwide and Washington Classes, as defined below.

22. Defendant Premera Blue Cross is a healthcare benefits provider existing under the laws of the State of Washington with its headquarters and principal place of business located at 7001 220th Street SW, Building 1, Mountlake Terrace, Washington 98043. Premera's relevant operations, including its primary marketing, administration and information security operations, as well as its vital employees (such as its Chief Information Security

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Officer) are all located in the State of Washington. Premera is also registered to conduct business in the State of Oregon (Oregon Secretary of State Registry Number 447360-80) and Alaska (Premera Blue Cross of Alaska, which is a trade name only).

III. JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Classes is a citizen of a state different from Defendant, and (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

24. This Court has personal jurisdiction over Defendant because it is registered to and regularly does conduct business in this District, and the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

25. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the unlawful conduct alleged in this Complaint occurred in, was directed to, and/or emanated from this District. Venue is additionally proper because Defendant is registered to and does conduct business in this District.

IV. FACTUAL BACKGROUND

A. Premera Had A Duty And Contractual Obligation To Protect Its Members' Sensitive Information From Unauthorized Disclosures.

26. Premera had a duty and obligation to keep confidential the Sensitive Information it obtained and to protect that information from unauthorized disclosures. Premera's duty and obligations are based on: 1) HIPAA; 2) industry standards; 3) specific governmental warnings to Premera about its failure to meet those obligations; and 4) the promises it made to its members. All Class members provided their Sensitive Information to Premera with the common sense and reasonable understanding that Premera would comply with its obligations to keep Sensitive Information confidential and secure from unauthorized disclosures.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

27. HIPAA mandates that Premera provide to every insured and everyone whose plan Premera administers a privacy notice. In its HIPAA mandated privacy notice, Premera promises every insured and everyone whose plan Premera administers it will keep Sensitive Information confidential and protect it from unauthorized disclosure, even beyond Premera's regulatory obligations. In its Notice of Privacy Practices effective September 23, 2013 Premera promises in relevant part:

> THE PRIVACY OF YOUR MEDICAL AND FINANCIAL INFORMATION IS VERY IMPORTANT TO US.
>
> At Premera Blue Cross, we are committed to maintaining the confidentiality of your medical and financial information, which we refer to as your "personal information," regardless of format: oral, written, or electronic.
>
> * * *
>
> OUR RESPONSIBILITIES TO PROTECT YOUR PERSONAL INFORMATION
>
> Under both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act, Premera Blue Cross must take measures to protect the privacy of your personal information. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of your personal information include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.
>
> We protect your personal information in a variety of ways. For example, 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. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of your information even if you no longer maintain coverage through us.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> We are required by law to:
>
> protect the privacy of your personal information; provide this Notice explaining our duties and privacy practices regarding your personal information; notify you following a breach of your unsecured personal information; and abide by the terms of this Notice.

28. Premera posts the same Notice of Privacy Practices on its website, acknowledging its duty and promising to protect all Sensitive Information in its possession.

29. Premera admitted its duty and promised to keep the Sensitive Information confidential and secure in other ways. For example, all individuals who register on Premera's website must "accept" Premera's Terms and Conditions. These Terms and Conditions contain a section entitled "Security of Your Personal Information," in which Premera promises that "Premera.com takes precautions to protect users' personal information both online and offline."

30. Premera's policy booklets, which form its member contracts, contain a section on "Privacy Policies and Practices" or a "Notice of Information Use and Disclosure," which include promises such as:

> "We protect your privacy by making sure your information stays confidential. We have a company confidentiality policy and we require all employees to sign it."[1]
>
> "To safeguard your privacy, we take care to ensure that your information remains confidential by having a company confidentiality policy and by requiring all employees to sign it."[2]

31. Premera's website includes its Code of Conduct, which appears to include the "company confidentiality policy" referenced in the policy booklets.[3] On "Customer Privacy," Premera's Code of Conduct promises:

> We are committed to complying with federal and state privacy laws, including the HIPAA privacy regulations, that protect financial and health information of our customers. We use the following privacy principles to guide our actions:

---

[1] *See, e.g.*, PBC00044925–44926, MSP Preferred Select Bronze 5250 HAS Benefit Booklet (2014).

[2] *See, e.g.*, PBC00046821, Premera Preferred Bronze 5250 HSA Benefit Booklet (2014).

[3] Premera, *Code of Conduct* 12 (2016), *available at* https://www.premera.com/documents/030553.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> Customers – Customers should enjoy the full array of privacy protections afforded to them by law and routinely granted by their providers. This is a values-based approach whereby we are focused on two core values: Customer Care and Integrity.
>
> * * *
>
> Where appropriate, we use technical and/or physical security safeguards to ensure our privacy policies are followed.
>
> * * *
>
> We are committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' protected personal information (PPI).
>
> We are expected to be aware of and follow established corporate policies, processes and procedures that are designated to secure our buildings and electronic systems in compliance with HIPAA Security requirements.

32. To further protect Sensitive Information from disclosure, Premera requires all vendors and contractors to sign Premera's Vendor/Contractor Privacy Basics,[4] which states:

> Our policies and procedures require compliance with federal and state privacy laws, including HIPAA privacy and security regulations. Contractors, too, must follow our policies and procedures and comply with all laws and regulations to which the Company is subject.

33. As demonstrated by these excerpts from Premera's Notice of Privacy Practices, contracts with Policyholder Plaintiffs (i.e., the policy booklets), Code of Conduct, and Vendor/Contractor Privacy Basics, Premera recognized the importance of keeping consumers' Sensitive Information private and repeatedly promised to protect that Sensitive Information and comply with the data security requirements mandated by, among other things, federal and state privacy laws.

34. Premera's data security obligations and promises were particularly important given the substantial increase in data breaches (particularly those in the healthcare industry) in the time period preceding Premera's data breach. Premera's failure to comply with those

[4] Premera, *Vendor/Contractor Privacy Basics* (2014), *available at* https://www.premera.com/documents/030628.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

obligations and promises was particularly egregious in light of specific governmental warnings regarding the possibility of hacker attacks on companies like Premera. Such warnings further established Premera's duty to keep class members' Sensitive Information private and secure.

35. For example, on April 8, 2014—just one month before the Premera breach occurred—the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)."[5]

36. Worse yet, a couple weeks before Premera's breach, the U.S. Office of Personnel Management directly notified Premera about its network security vulnerabilities.[6] The U.S. Office of Personnel Management's April 18, 2014 report revealed that Premera failed to implement adequate measures to secure its network. It found "several areas of concern related to Premera's network security controls" and noted that "patches are not being implemented in a timely manner," "a methodology is not in place to ensure that unsupported or

[5] *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), FBI Cyber Division Private Industry Notification, *available at* http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf.

[6] Mike Baker, Feds Warned Premera About Security Flaws Before Breach, Seattle Times, Mar. 18, 2015, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (last visited Oct. 6, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

out-of-date software is not utilized," and a vulnerability scan identified "insecure server configurations."[7]

37. Federal auditors notified Premera weeks before the breach that its network-security procedures were inadequate and informed it that some of the vulnerabilities could be exploited by hackers and expose sensitive information.[8]

B. Premera Failed To Properly Protect Consumers' Sensitive Information.

38. On May 5, 2014, hackers began the initial phase of their intrusion on Premera's servers. A "phishing" email was sent to a Premera employee falsely purporting to be from a Premera Information Technology (IT) employee. The email included instructions to download a "security update." Premera's employee downloaded this "update," which was actually malware that allowed hackers access to Premera's servers.

39. Notably, various internal security assessments that Premera had undertaken prior to this period confirmed that it was vulnerable to this exact type of attack.

40. The hackers used the domain name in their email of "premrera.com" (i.e., using an additional "r"). This wrong domain was visible in the email message. Around this same time, another phishing domain of "prennera.com" was also registered. Premera did not warn employees that scam domain names had been registered that were close to "Premera.com."

41. After the Premera employee downloaded the malware, hackers had access to at least two of Premera's servers for many months completely undetected.

42. In June of 2014, the U.S. Computer Emergency Readiness Team issued alerts regarding the danger of data hacking from a malware virus known as Gameover Zeus.

---

[7] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Audit of Information Systems General and Application Controls at Premera Blue Cross (Nov. 28, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf.

[8] Mike Baker, *Feds Warned Premera About Security Flaws Before Breach*, Seattle Times, *available at* http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/ (Oct. 6, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

43. In July of 2014, an end user reported a Trojan message to Premera's IT department.

44. In August of 2014, a Premera virus scan detected a backdoor Trojan virus.

45. In September of 2014, Premera's IT department indicated it was concerned about a possible "Gameover Zeus" infiltration, the dangers of which the media and U.S. government had been reporting on for many months.

46. On September 8, 2014, Premera IT employee, Gabriel Bigger, sent malware byte logs to Mandiant based on these concerns over Gameover Zeus infiltration. Mandiant quickly informed Premera the virus looked like Gameover Zeus on September 9, 2014.

47. On September 23, 2014, Premera IT informed senior executives that Premera computers had been infected with a virus.

48. On October 10, 2014, Premera engaged Mandiant, a cyber-security firm, to perform an assessment of the security of its network. Mandiant provided its Mandiant Intelligent Response (MIR) agents (a tool to identify indicators of compromise and malware) to install on Premera's workstations and laptops for the purposes of scanning for malware and other infections.

49. On October 13, 2014, Jerry Vergeront provided a network status report that identified deficiencies in Premera's Intrusion Detection System, a repeat deficiency initially identified in 2007

50. The pilot phase of the Mandiant project did not begin until December 2014 and continued until early January 2015. Premera did not begin searching end-user work stations until January 8, 2015. Premera did not install network sensors until January 28, 2015.

51. On January 29, 2015, Mandiant discovered a signature for SOGU malware traffic on the Premera network, confirmed infection of two servers, and confirmed that the malware was "beaconing" to attacker sites. SOGU is a type of Trojan that has been around for

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

years. By January 30, 2015, Premera had finally uncovered that the SOGU malware had been in its system since May 2014.

52. In February 2015, Mandiant continued to try to understand the full extent of the breach and whether and how much information had been removed from Premera's system. At this time, Premera finally agreed to deploy Mandiant's agents on all Premera servers, workstations, and laptops in order to assess the scope of the breach. This installation was only complete in late February, nearly a month after Mandiant first confirmed that a breach had occurred.

53. On February 20, 2015, Premera notified the FBI of the data breach. On February 25, 2015, the FBI met with Premera and Mandiant. The FBI began its own investigation, as well.

54. Premera chose not to inform the public of the breach at this time although it had sufficient knowledge of the extent and scope of the breach, deciding instead to further investigate and attempt to remediate the breach before letting the public know that their Sensitive Information had been stolen (and was continuing to be stolen).

55. Premera further waited until the weekend of March 6-8 to perform the complete remediation of its network, during which time information was still being accessed and stolen. Mandiant continued to monitor the network for the following week to ensure Premera had completely cleansed its system.

56. It wasn't until March 17, 2015—over eight months after being warned of a Trojan virus and 46 days after confirming the data breach—that Premera finally revealed to the public and governmental authorities other than the FBI that a massive data breach had occurred.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

57. In its notice, Premera revealed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [its] Information Technology (IT) systems."[9] As a result, the Sensitive Information belonging to approximately 11 million consumers—including its current and former members, employees, and other Blue members—was compromised. The breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and affiliate brands Vivacity and Connexion Insurance Solutions, Inc. The breach also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington, Oregon or Alaska.

58. Premera eventually acknowledged that the breach actually started in May 2014 and went undetected by it for nearly one year.[10]

59. One month before Premera announced the Sensitive Information had been breached, another major healthcare provider reported that hackers had successfully taken sensitive information of approximately eighty million consumers. Security researchers believe that attackers initially gained access to the databases containing that information through phishing attempts (i.e., using legitimate-looking emails or websites to trick individuals into revealing confidential information, such as database login credentials) and linked malware[11] involved in those phishing attacks to Chinese hackers who authorities refer to as "Deep Panda."

60. Malware thought to have been authored by Deep Panda was later discovered in connection with the phishing website www.prennera.com.

---

[9] *Premera Has Been The Target Of A Sophisticated Cyberattack*, Premera Blue Cross, *available at* http://premeraupdate.com/ (last visited Oct. 6, 2015).

[10] *Id.*

[11] "Malware" refers to malicious software designed to infiltrate and damage computers or computer systems.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

C. Premera Violated HIPAA, Industry Standard Data Protection Protocols, And Its Own Representations Regarding Data Security.

61. HIPAA requires that healthcare providers (like Premera) adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of consumers' Sensitive Information.

62. Unfortunately, Premera's data breach resulted from a variety of failures to follow HIPAA mandated data-security protocols, many of which are also industry standard. Among such deficient practices, Premera's breach shows that it failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training on phishing attempts, adequate intrusion detection systems, regular reviews of audit logs and authentication records, and other similar measures designed to protect the confidentiality of the Sensitive Information it maintained in its data systems.

63. More specifically, Premera's security fiascos demonstrate that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiffs' and the Classes' Sensitive Information;

c. Ensuring the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing 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);

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4); and

j. Training all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

64. Likewise, Premera's security lapses demonstrate that it failed to follow through on its own representations about its data security practices, including those discussed above. Specifically, Premera did not:

a. Take precautions to protect users information, whether online or offline;

b. Maintain the confidentiality or privacy of the personal information—as defined by its Notice of Privacy Practices—in its control, specifically including information stored in electronic form;

c. Take steps to secure its electronic systems from unauthorized access;

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

d. Train its employees on Premera's confidentiality policy and procedures and did not enforce its policy and procedures;

e. Timely or reasonably notify affected individuals following the breach of their personal information;

f. Protect individuals' privacy by making sure their information stayed confidential, including by failing to enforce or monitor employee compliance with its confidentiality policy or practices;

g. Ensure the security of its facilities and electronic systems to prevent unauthorized access to Premera's and its customers' protected personal information (PPI); and

h. Remain aware of or follow corporate policies, processes and procedures designated to secure electronic systems in compliance with HIPAA Security requirements.

65. Had Premera implemented the above-described data security protocols or policies, the consequences of the data breach could have been avoided, or at least significantly reduced (as the breach could have been detected nearly one year earlier, the amount of Sensitive Information compromised could have been greatly reduced or avoided entirely, and affected consumers could have been notified—and taken protective/mitigating actions—much sooner). For instance, had Premera (i) adequately trained its employees to protect themselves against phishing attempts (like those attempts described above), (ii) implemented adequate security protocols to detect breaches (i.e., detecting unauthorized access to its databases), or (iii) adequately reviewed authentication logs for anomalies (e.g., detecting abnormal access to its databases from unknown locations, or accessing or transferring large amounts of Sensitive Information), the breach could have been identified and thwarted before considerable amounts of Sensitive Information were compromised.

66. As discussed above, major healthcare entities (like Premera) have been targeted in damaging hacking attempts in recent years, and Premera was specifically warned that its network-security procedures were inadequate and that some of the vulnerabilities could be

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

exploited by hackers to expose sensitive information (as described above). Premera thus knew or should have known that a data breach would likely result from its deficient security and privacy practices described above. Despite these warnings—and Premera's own knowledge about the significant holes in its data security regime—Premera continued to assure its customers (and potential customers) that its data security systems were secure, including by making the express representations discussed above.

67. Even though Premera promised its members and Blue members the above-described security measures (i.e., that Premera's promises, as well as HIPAA-mandated and industry standards would be used to protect their Sensitive Information), they were not adequately implemented (if at all), which resulted in the unauthorized release of Sensitive Information.

D. It Is Well Established That Security Breaches Lead To Instances Of Identity Theft.

68. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[12] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

69. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[13]

---

[12] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* http://www.gao.gov/new.items/d07737.pdf.

[13] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

70. According to the Federal Trade Commission ("FTC"), identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit.[14] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[15]

71. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit various types of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services, prescription drugs and goods, and fraudulent medical billing in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.[16] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of job employment, blackmail and other negative effects.

72. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available. In

---

[14] *See Identity Theft*, Federal Trade Commission, http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Oct. 6, 2015).

[15] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[16] *See Identity Theft*, Federal Trade Commission, *available at* http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Oct. 6, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

one study, researchers found hundreds of websites displaying stolen Sensitive Information. The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[17]

73. A study by Experian found that the "average total cost" of medical identity theft to an individual is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[18] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[19] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

74. Further, medical databases are particularly high value targets for identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[20] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

---

[17] *See The Underground Credit Card Blackmarket*, StopTheHacker, *available at* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Oct. 6, 2015).

[18] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), http://news.cnet.com/8301-27080_3-10460902-245.html (last visited Oct. 6, 2015).

[19] *Id.*

[20] *See Study: Few Aware of Medical Identity Theft Risk*, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited Oct. 6, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

75. In fact, individuals whose information was compromised in a similar data breach by the same hackers—Deep Panda—have already fallen victims to identity theft, such as tax return fraud.[21]

76. Indeed, Premera's own data breach notification statements recognize the long-lasting harmful effects of its misconduct and recommends that affected individuals remain vigilant to the possibility of fraud and identity theft by indefinitely reviewing their credit card, bank, and other financial statements for unauthorized activity.

E. Plaintiffs' Experiences Underscore The Fact That All Class Members Are In Imminent Danger Of Identity Theft.

ALASKA

77. Plaintiff Ross Imbler is a resident of Fairbanks, Alaska and was an Alaska resident during the period of the Premera Breach. Plaintiff Imbler has been a Premera policyholder since 2011 and makes partial premium payments through his employer. In or around March 2015, Plaintiff Imbler received three letters from Premera indicating that his, his wife's, and his then 2-year-old daughter's personal information may be compromised. Plaintiff Imbler is especially concerned about the long-term threat of identity theft to his daughter, as well as the immediate threat of fraud and identity theft for him and his wife. Plaintiff Imbler has spent about six hours to date addressing issues arising from the Premera Breach.

OREGON

78. Plaintiffs Stuart and Ilene Hirsh are residents of Salem, Oregon and were Oregon residents during the period of the Premera Breach. Mr. Hirsh was a Premera policyholder, with Mrs. Hirsh as a dependent insured, from approximately 1999 to 2006 and made partial premium payments through his employer. In or around March 2015, Mr. and Mrs. Hirsh received letters from Premera notifying them that their personal information may

[21] *See* Jose Pagliery, *A Hacker Stole Our $3,500 Tax Refund*, CNN Money (Apr. 15, 2015), http://money.cnn.com/2015/04/15/technology/tax-hacker/ (last visited Oct. 6, 2015).

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

have been compromised. Mr. and Mrs. Hirsh have spent about six hours to date addressing issues arising from the Premera Breach, including monitoring their credit reports for fraudulent activity.

TENNESSEE

79. Plaintiffs Kevin Smith and Catherine Bushman, husband and wife, are residents of Franklin, Tennessee and were Tennessee residents during the period of the Premera Breach. Plaintiffs Smith and Bushman were both Premera policyholders at various times from approximately 2005 to 2010, then approximately 2011 to 2013, and each made partial premium payments through their employer. In or around March 2015, Plaintiffs Smith and Bushman received letters from Premera notifying them that their personal information may have been compromised. Also in and around March 2015, Plaintiffs Smith and Bushman received a large IRS tax refund check despite having not yet filed their 2014 tax return. After contacting the IRS, they discovered that someone had filed a fraudulent tax return using their names and Social Security numbers. Plaintiffs Smith and Bushman then filed identity theft affidavits with the IRS and the FTC, a police report, and sought a credit watch with one of the credit bureaus. At an in-person appointment with the IRS in Nashville, they were informed that, going forward, they will have to manually submit their tax returns with a security PIN. The processing of their 2014 tax return and refund was delayed approximately four months. In or around July of 2015, a criminal attempted to fraudulently open a credit card in both of their names, but the bank called Plaintiffs Smith and Bushman and they were able to confirm the fraud and cancel the account. Plaintiffs Smith and Bushman have spent about 30 hours each to date addressing issues arising from the Premera Breach.

TEXAS

80. Plaintiff Sharif Ailey is a resident of Keller, Texas and was a Texas resident during the period of the Premera Breach. Plaintiff Ailey has been a Premera policyholder since November 2011 and makes partial premium payments through his employer. In or around

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

March 2015, Plaintiff Ailey received a letter from Premera notifying him that his personal information may have been compromised. In or around June 2015, Plaintiff Ailey discovered fraudulent credit accounts were being opened in his name. He has spent approximately $100 requesting credit reports, freezing his credit report, and attempting to remove the fraudulent activity from his credit report. As a result of these credit issues caused by the Premera Breach, Plaintiff Ailey was unable to refinance the mortgage on his house. Plaintiff Ailey has spent about 25 hours to date addressing issues arising from the Premera Breach.

WASHINGTON

81. Plaintiff April Allred is a resident of Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Allred and her son were Premera insureds from 2007 to 2009 and from 2011 to 2012, and her husband, the policyholder, made partial premium payments through his employer. In or around March 2015, Plaintiff Allred received a letter from Premera notifying her that her and her family's personal information may have been compromised. On or about April 15, 2015, Plaintiff Allred's 2014 income tax return was rejected due to the use of her son's Social Security number in another fraudulently filed return. Plaintiff Allred had to take additional trips to her accountant's office, submit her tax return manually by mail, and wait several weeks longer to receive her tax refund. Plaintiff Allred has spent about 25 hours to date addressing issues arising from the Premera Breach, including monitoring her credit report and bank accounts for fraudulent activity.

82. Plaintiffs Robert and Theresa Foulon are residents of Bellevue, Washington and were Washington residents during the period of the Premera Breach. Mr. Foulon has been a Premera policyholder, with Mrs. Foulon and their children as dependent insureds, from approximately 1992 to 2009, then 2010 to present. Mr. Foulon now makes premium payments through his self-employment; prior to 2009 he made partial premium payments through his employer. In or around March 2015, the Foulons received letters from Premera notifying them that their and their children's personal information may have been compromised. In or around

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

April 2015, they then received a letter from the IRS indicating that their $9,539 tax refund was processing even though they had not yet filed a return. After logging into his tax account and seeing the bank account destination for the direct deposit was not theirs, Mr. Foulon contacted the IRS and reported that the tax return was fraudulent. The Foulons had to fill out the necessary forms to report the fraud and file their actual tax return manually, which they will always have to do going forward. On or about September 14, 2015, they received another letter from the IRS verifying that the prior return was fraudulent and providing a PIN for future filings. Mr. Foulon is still attempting to sort out his family's 2014 tax return due to this attempted identity theft. The Foulons have spent about 30 hours to date addressing issues arising from the Premera Breach, including monitoring their credit reports for additional fraudulent activity.

83. Plaintiff Crystal Hayes is a resident of Lynnwood, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Hayes has been a Premera policyholder since 2012 and makes partial premium payments through her employer. In or around March 2015, Plaintiff Hayes received a letter from Premera notifying her that her personal information may have been compromised. Soon after the breach notification, her credit cards were cancelled and reissued due to fraudulent activity, but Plaintiff Hayes was unaware of the cancellation and her cards were declined when she attempted to use them. She had to reset her automatic bill payments with the reissued card information as well. Plaintiff Hayes has spent about five hours to date addressing issues arising from the Premera Breach, including requesting and checking her credit report and bank statements for fraudulent activity.

84. Plaintiff Kevin McLallen is a resident of Covington, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff McLallen has been a Premera policyholder since approximately 2011 and makes partial premium payments through his employer (and now through COBRA). In or around March 2015, Plaintiff McLallen received a letter from Premera notifying him that his personal information may have been

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

compromised. In or around April 2015, fraudulent charges appeared on Plaintiff McLallen's credit and debit cards for small charges in New Jersey and Michigan. Even more recently, Plaintiff McLallen has received phishing calls where the criminals already have many of his personal identifying information. Plaintiff McLallen has spent about ten hours to date addressing issues arising from the Premera Breach, including pulling credit reports and purchasing his credit scores - and unreimbursed expense - to ensure they were accurate. He also spent time calling his banks to notify them of the fraudulent activity and researching additional credit security services.

85. Plaintiff Surya Prakash is a resident of Seattle, Washington and was a Washington resident during the period of the Premera Breach. Plaintiff Prakash was a Premera policyholder from 2005 to 2012 and made partial premium payments through his employer. In or around December 2014, approximately $3,500 in fraudulent charges appeared on his bank account. Plaintiff Prakash immediately notified the bank and canceled the account, but was without access to the stolen funds for two weeks until reimbursement. In or around February 2015, he again experienced fraudulent activity totaling approximately $250 on different bank accounts. Again, Plaintiff Prakash canceled the cards and had to wait a few weeks for reimbursement of the stolen funds. In or around March 2015, Plaintiff Prakash received a letter from Premera notifying him that his personal information may have been compromised. In or around August 2015, Plaintiff Prakash received a letter from a collections company indicating he purchased over $2,000 in plane tickets that he never purchased. He has contacted all three credit bureaus to place alerts and freezes on his credit report. Plaintiff Prakash has spent about five hours to date addressing issues arising from the Premera Breach, including monitoring his bank accounts and credit report for additional fraud.

86. Plaintiffs Gabriel and Laura Webster are residents of Seattle, Washington and were Washington residents during the period of the Premera Breach. Mr. Webster has been a Group Health and Regence Blue Cross policyholder, with Mrs. Webster and their 12-year-old

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

son as dependent insureds, from approximately 2009 to 2011 and 2012 to present, respectively. Mr. Webster made premium payments on these policies through his employer, and the Websters all received medical treatment in Washington State from 2009 to present. In or around November 2014, Mr. Webster had fraudulent charges on his credit card. Although these charges were ultimately reimbursed, he temporarily lost access to his line of credit. In or around February 2015, the Websters attempted to file their 2014 tax return but were prevented from doing so due to a fraudulent return already filed in their names. They had to pay their accountant an extra fee to submit an amended filing and had to manually file the tax return. Going forward, the Websters will have to file their taxes using a new security PIN provided to them by the IRS every year. In or around March 2015, the Websters received letters from Premera notifying them that their and their son's personal information may have been compromised. The Websters have spent about 25 hours to date addressing issues arising from the Premera Breach, including numerous hours on the telephone attempting to resolve the fraudulent tax return.

V. CLASS ALLEGATIONS

A. Nationwide Data Breach Class

87. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), Plaintiffs assert statutory claims under the Washington Consumer Protection Act (First Claim for Relief) and the Washington data breach notification statute (Second Claim for Relief), and common law claims for negligence (Third Claim for Relief), contract implied-in-fact (Fifth Claim for Relief) and misrepresentation by omission (Ninth Claim for Relief) on behalf of a nationwide class defined as follows:

> **Nationwide Data Breach Class**: All persons in the United States whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

1. Nationwide Premera Policyholder and Plan Administration Subclass

88. Plaintiffs Ross Imbler, Sharif Ailey, Robert and Theresa Foulon, Crystal Hayes, Barbara Lynch, Kevin McLallen, Gabriel and Laura Webster assert their common law claims for breach of express contract (Fourth Claim for Relief), breach of implied contract (Fifth Claim for Relief), and unjust enrichment (Sixth Claim for Relief) on behalf of a nationwide subclass defined as follows:

> **Nationwide Premera Policyholder and Plan Administration Subclass**: All Nationwide Data Breach Class members who paid money to Premera prior to March 17, 2015 in exchange for health insurance or plan administration.

89. As alleged herein, Premera's headquarters are in Mountlake Terrace, Washington, its data centers and servers are located in Washington, and the Premera employees responsible for making decisions with respect to data security are based in Washington. Premera's conduct resulting in the data breach took place exclusively, or primarily, in Washington. Premera, being headquartered in Washington, would reasonably expect to be bound by the laws of Washington. Furthermore, the majority of the Nationwide Data Breach Class members are residents of the state of Washington. Accordingly, applying Washington law to the claims of the Nationwide Data Breach Class and Nationwide Premera Policyholder and Plan Administration Subclass is appropriate.

B. Alternate Statewide Common Law Classes

90. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), and in the alternative to the common law claim for negligence asserted on behalf of the Nationwide Data Breach Class,

91. Plaintiffs assert their common law claim for negligence (Third Claim for Relief) on behalf of separate statewide classes defined as follows:

> **Statewide [name of State] Common Law Classes**: All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

1. Statewide Premera Policyholder and Plan Administration Subclasses

92. Plaintiffs Imbler, Ailey, Foulon, McLallen, and Webster, assert their common law claims for breach of contract (Fourth Claim for Relief), breach of implied contract (Fifth Claim for Relief), unjust enrichment (Sixth Claim for Relief), and misrepresentation by omission (Ninth Claim for Relief) on behalf of separate statewide subclasses defined as follows:

> **Statewide [name of State] Premera Policyholder and Plan Administration Subclasses**: All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015, and who paid money to Premera prior to March 17, 2015 in exchange for health insurance or plan administration.

C. Alternate Statewide Statutory Classes

93. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and (b)(3), and in the alternative to the statutory claims asserted on behalf of the Nationwide Data Breach Class, Plaintiffs Imbler, Hirsh, Smith, Bushman, Ailey, Allred, Foulon, McLallen, Prakash, and Webster assert statutory claims for violation of state consumer protection statutes (Seventh Claim for Relief) and state data breach notification statutes (Eighth Claim for Relief) on behalf of separate statewide classes, defined as follows:

> **Statewide [name of State] Statutory Classes**: All residents of [name of State] whose Sensitive Information was maintained on Premera's database and compromised as a result of the breach announced by Premera on or around March 17, 2015.

94. Plaintiffs Imbler, Hirsh, Ailey, Allred, Foulon, McLallen, Prakash, and Webster assert the state consumer protection statute claims (Seventh Claim for Relief) under the consumer protection laws of the following states: Alaska, Oregon, Texas, and Washington.

95. Plaintiffs Smith, Bushman, Ailey, Allred, Foulon, Hayes, McLallen, Prakash, and Webster assert the state data breach notification law claims (Eighth Claim for Relief) on

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

behalf of separate statewide classes in and under the respective data breach statutes of the following states: Tennessee, Texas, and Washington.

96. Excluded from the Classes and Subclass are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Class should be expanded, divided into further subclasses or modified in any other way.

D. Certification Of The Proposed Classes And Subclasses Is Appropriate.

97. Each of the proposed classes and subclasses meet the requirements for certification under Fed. R. Civ. P. 23(a), (b)(1), (b)(2), and (b)(3).

98. **Numerosity**: The exact number of members of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are approximately 11 million individuals in the Classes, making joinder of each individual member impracticable. Ultimately, members of the Classes will be easily identified through Premera's records.

99. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

a. Whether Defendant failed to safeguard Plaintiffs' and the Classes' Sensitive Information adequately;

b. Whether Defendant failed to protect or otherwise keep Plaintiffs' and the Classes' Sensitive Information secure, as promised;

c. Whether Defendant's storage of Plaintiffs' and the Classes' Sensitive Information in the manner alleged violated HIPAA, federal, state and local laws, or industry standards;

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

d. Whether Defendant engaged in unfair or deceptive practices by failing to safeguard Plaintiffs' and the Classes' Sensitive Information properly as promised;

e. Whether Defendant violated the consumer protection statutes applicable to Plaintiffs and each of the Classes;

f. Whether Defendant failed to notify Plaintiffs and members of the Classes about the security breach as soon as practical and without delay after the breach was discovered;

g. Whether Defendant acted negligently in failing to safeguard Plaintiffs' and the Classes' Sensitive Information;

h. Whether Defendant violated the California Confidential Medical Information Act;

i. Whether contracts existed between Defendant, on the one hand, and Plaintiffs and the members of the each of the Classes, on the other;

j. Whether Defendant's conduct described herein constitutes a breach of its contracts with Plaintiffs and the members of each of the Classes;

k. Whether Defendant should retain the money paid by Plaintiffs and members of each of the Classes to protect their Sensitive Information; and

l. Whether Plaintiffs and the members of the Classes are entitled to damages as a result of Defendant's conduct.

100. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Classes. Plaintiffs and the members of the Classes sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

101. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

prosecuting this action vigorously on behalf of the members of the proposed Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

102. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Classes.

103. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes, and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendant's practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiffs' challenge of those practices hinges on Defendant's conduct with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiffs.

104. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendant. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Violation of the Washington Consumer Protection Act
(On behalf of Plaintiffs, the Nationwide Data Breach Class,
and the Nationwide Premera Policyholder and Plan Administration Subclass)

105. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

106. Plaintiffs and the Nationwide Data Breach Class are current and former members of Premera or those who received services from healthcare providers in the Premera network and who provided Premera with their Sensitive Information.

107. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington. The conduct that Plaintiffs challenge directly affects the people of the State of Washington.

108. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

109. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce. . . ." RCW § 19.86.020.

110. Defendant expressly represented-including in its Notice of Privacy Practices, Code of Conduct, public statements, and other consumer-facing representations-that it would safeguard and protect Sensitive Information, including in accordance with HIPAA regulations, federal, state and local laws, and industry standards. Premera's specific representations are set forth above in paragraphs 27-33. Premera made these representations available to the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Nationwide Data Breach Class at all times (including through its website) and at the time that Class Members received services from its healthcare facilities. These representations were made to the Nationwide Premera Policy Holder and administration Subclass in the enrollment process.

111. Consistent with its representations, Defendant accepted responsibility for securing Plaintiffs' and the Nationwide Data Breach Class's Sensitive Information. Given that it was Defendant's responsibility for creating, overseeing, maintaining, and otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiffs' or the Nationwide Data Breach Class's Sensitive Information in accordance with its express guarantees. This is particularly true given the many warning signs that Premera's systems were at risk of a breach-including those affecting the larger healthcare industry (e.g., the many other medical data breaches and warning of the Federal Bureau of Investigation's Cyber Division) and those relating to Premera's own security (e.g., the findings of the U.S. Office of Personnel Management investigation of Premera's own systems). See especially paragraphs 35-37 infra.

112. Despite this knowledge, Defendant failed to disclose that its data security systems and practices did not comport with the express representations set forth above in paragraph 27-33, and otherwise described herein. In sum, and as set forth specifically above in paragraphs 54-57, Defendant did not disclose that it did not take appropriate steps to secure electronic systems from unauthorized use, did not ensure that authorized personal had access to Sensitive Information only to the extent necessary to conduct their business, and did not meet its obligations under HIPAA and other state, local, and federal laws. Instead, Defendant continued to represent that its data security system was secure, even though it knew (or should have known) that it was not.

113. Premera's conduct was deceptive. By failing to honestly disclose its true data security practices at the time that it accepted and maintained the Sensitive Information of

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiffs and members of the Nationwide Data Breach Class, Premera made affirmative misrepresentations and, thus, engaged in deceptive acts or practices.

114. Given that Defendant alone knew about the true state of its data security and privacy practices and Defendant also knew that no reasonable consumer would purchase insecure health insurance services (i.e., services that did not comport with a provider's own representations about its data security, or its other duties to comply with applicable law and/or industry standards), Defendant purposefully used its inflated representations of data security and privacy protocols, which it knew were false at the time they were made to consumers, to mislead Plaintiffs into using and/or paying for its insecure services. Premera's conduct therefore had the capacity to deceive a substantial portion of the public.

115. Prior to the Premera's public announcement of the data breach, neither Plaintiffs, nor members of the Nationwide Data Breach Class, nor the general public could have known that Defendant was not implementing the data security and privacy protocols in accordance with its own consumer-facing representations and applicable duties. Defendant knew that Plaintiffs and the Nationwide Data Breach Class would not allow Defendant access to their Sensitive Information-and thereby not give Defendant their business-if they knew Defendant could not and would not protect their Sensitive Information as it represented. And rather than implement the data security and privacy protocols it promised-including by timely notifying Plaintiffs and the Nationwide Data Breach Class promptly about the data breach-Defendant actively concealed its true practices and protocols (which were of material concern to all of its customers) in order to lead consumers to give Defendant access to their Sensitive Data, while at the same time expressly promising that Sensitive Information would be protected as described above.

116. Premera's conduct was also unfair. By failing to disclose its compliance with its own data security representations and other obligations, Premera engaged in unfair acts or practices. Premera made the data security representations discussed above to attract

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

consumers-including Plaintiffs and members of the Nationwide Data Breach Class-who were concerned about the privacy and security of their Sensitive Information.

117. Premera, however, failed to make good on its promises of data security by not investing the necessary resources in its cybersecurity program, not promptly notifying Plaintiffs and the Nationwide Data Breach Class promptly about the data breach, and otherwise not living up to the specific representations and obligations set forth above in paragraphs 27-33. Given the known risk of maintaining Sensitive Information with lax cybersecurity practices, Premera's conduct was likely to cause substantial injuries to consumers.

118. As set out above, because only Premera knew (or should have known) that it was not complying with its own data security representations and obligations, there was no way for members of the public, including Plaintiffs and members of the Nationwide Data Breach Class, to avoid the injury caused by Premera's conduct. Further, Premera's failure to live up to its data security representations and obligations did not create any countervailing benefits.

119. Consumers-like Plaintiffs and members of the Classes-value their privacy. Companies (such as health insurers) that offer adequate data security protections are more valuable to consumers than those with substandard security practices. As such, consumers will, if given the choice between two otherwise identical services, choose one with adequate security practices over one with substandard security practices.

120. Because of this consumer preference for data security, a healthcare benefits company safeguarding and protecting Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards-in addition with its own affirmative representations of its data security practices-commands a higher market price for its coverage than a provider with substandard security.

121. Based on the representations made by Defendant, Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass believed Defendant would adequately protect their Sensitive Information, those security protections were valuable to them, and the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

protections formed the basis of their bargain inasmuch as Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass would not have purchased healthcare benefits from Defendant at the prices charged (if at all) had Defendant disclosed its substandard security practices. Accordingly, Defendant's omission regarding its true protection practices was material.

122. To Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass, Defendant's as-promised healthcare benefits offered significantly more utility or value than what was delivered, which lacked meaningful security protections. Thus, to Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass, Defendant's secured healthcare benefits-as promised and paid-for-was substantially more valuable than the unsecure insurance received.

123. Accordingly, had Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass known that Defendant did not actually implement its promised data security and privacy protocols, they would not have been willing to purchase its healthcare benefits at the prices charged, if they would have paid money at all.

124. Likewise, had Plaintiffs and members of the Nationwide Data Breach Class known that Defendant did not actually implement its promised data security and privacy protocols, they would not have been willing to provide Defendant with their Sensitive Information.

125. Defendant's failure to disclose its actual (and substandard) security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiffs' and the Nationwide Class's Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

126. Defendant's deceptive and unfair acts or practices occurred in its trade or business and has proximately caused injury to Plaintiffs and the putative Nationwide Class.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendant's general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years (e.g., affected individuals could experience identity theft for years). As a direct and proximate result of Defendant's unfair acts, Plaintiffs and members of the Nationwide Data Breach Class have suffered actual injuries, including without limitation investing substantial time or money in monitoring and remediating the harm inflicted upon them.

127. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Data Breach Class have suffered actual damages, including the lost value of their privacy, the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

128. Further, as a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass have suffered actual damages in an amount equal to the difference in the market value of the secure healthcare benefits they paid for and the unsecured healthcare benefits they received.

129. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class and Nationwide Premera Policyholder and Plan Administration Subclass,

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

seek to enjoin further violation and recover actual damages and treble damages (where applicable), together with the costs of bringing this suit, including reasonable attorneys' fees.

130. With respect to injunctive relief, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class and Nationwide Premera Policyholder and Plan Administration Subclass, seek an Order requiring Premera to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and ordering Premera to correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera; (5) curing checks; (6) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (7) meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

SECOND CLAIM FOR RELIEF

Violation of Washington Data Breach Disclosure Law
(On behalf of Plaintiffs and the Nationwide Data Breach Class)

131. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

132. Plaintiffs allege additionally and alternatively that RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *See* RCW § 19.255.010(2) (2005).

133. The data breach described in Section II resulted in an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant and, therefore, experienced a "breach of [its] security of [its] system", as defined by RCW § 19.255.010(4) (2005).

134. Defendant failed to disclose the breach of its network immediately, after discovering the breach. Instead, it waited months before notifying all affected individuals. Defendant unreasonably delayed informing Plaintiffs and members of the Nationwide Data Breach Class about the data breach after it knew or should have known that the data breach had occurred.

135. Defendant's failure to provide notice immediately after discovering the breach is a violation of RCW § 19.255.010.

THIRD CLAIM FOR RELIEF

Negligence
(On behalf of Plaintiffs and the Nationwide Data Breach Class or, alternatively, the Statewide Common Law Classes)

136. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

137. Plaintiffs allege additionally and alternatively that Premera required Plaintiffs and Nationwide Data Breach Class members or alternatively, members of the Statewide Common Law Classes, to submit Sensitive non-public personal health and financial information in order to obtain coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network.

138. By collecting and storing this data, Premera had a duty of care to use reasonable means to secure and safeguard this personal and health information, to prevent disclosure of the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information, and to guard the information from theft. Premera's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give immediate notice in the case of a data breach.

139. Furthermore, given the other major data breaches affecting the healthcare industry and the warnings provided by federal auditors that Premera's network-security procedures were inadequate and that the vulnerabilities could be exploited by hackers and expose sensitive information (as described above), Plaintiffs and the Nationwide Data Breach Class members or alternatively, members of the Statewide Common Law Classes, are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Sensitive Information stolen.

140. Premera owed a duty to Plaintiff and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to provide security consistent with industry standards, statutory requirements, and the other requirements discussed herein, and to ensure that its systems and networks—and the personnel responsible for them—adequately protected its consumers' Sensitive Information.

141. Premera admitted and assumed its duty to implement reasonable security measures as a result of its general conduct, internal policies and procedures, its Privacy Policy, and its Code of Conduct, in which Premera states that it is "committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' personal protected information (PPI)." Through these and other statements, Premera specifically assumed the duty to comply with industry standards and HIPAA in protecting confidential information.

142. Premera's duty to use reasonable security measures arose as a result of the special relationship that existed between Premera and the Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes. The special relationship arose because Plaintiffs and the members of the Nationwide

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Data Breach Class or alternatively, members of the Statewide Common Law Classes, entrusted Defendant with their confidential data, as part of the health treatment process. Only Premera was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, from a data breach.

143. Premera's duty to use reasonable security measures also arose under HIPAA, pursuant to which Premera is required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

144. In addition, Premera had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by healthcare benefit providers like Defendant. The FTC publications and data security breach orders described above further form the basis of Premera's duty.

145. Premera's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because it was bound by, and had committed to comply with, industry standards for the protection of confidential Sensitive Information.

146. Premera breached its common law, statutory and other duties—and thus, was negligent—by failing to use reasonable measures to protect consumers' confidential data from hackers and by failing to provide timely notice of the at-issue breach. The specific negligent acts and omissions committed by Premera include, but are not limited to, the following:

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes', confidential data;

b. Failing to monitor the security of its networks adequately;

c. Allowing unauthorized access to Plaintiffs' and the proposed Nationwide Data Breach Class members' or, alternatively, members of the Statewide Common Law Classes', confidential data;

d. Failing to recognize in a timely manner that Plaintiffs' and proposed Nationwide Data Breach Class members' or alternatively, members of the Statewide Common Law Classes', confidential data had been compromised; and

e. Failing to warn Plaintiffs and the members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, in a timely manner that their Sensitive Information was likely to be and had been compromised.

147. It was foreseeable that Premera's failure to use reasonable measures to protect confidential data, to disclose to Plaintiffs its inadequate security system, and to provide timely notice of a breach of such data would result in injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes were reasonably foreseeable, particularly in light of the other major data breaches affecting the healthcare industry and the warning provided by federal auditors (described in Section I, above) that Premera's network-security procedures were inadequate and that the vulnerabilities could be exploited by hackers and expose sensitive information.

148. It was therefore reasonably foreseeable that the failure to adequately safeguard confidential data would result in one or more of the following injuries to Plaintiffs and the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

members of the proposed Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

149. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, seek an order declaring that Defendant's conduct constitutes negligence, and awarding them damages in an amount to be determined at trial.

150. Washington law should apply to the negligence claim of the Nationwide Class, or, alternatively, the negligence claims of the Statewide Common Law Classes should be governed by the law of each state in which such state specific claims are brought.

FOURTH CLAIM FOR RELIEF

Breach of Express Contract
(On behalf of Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass or, alternatively, the Statewide Premera and Plan Administration Policyholder and Plan Administration Subclasses)

151. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

152. Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses, allege additionally and alternatively that they entered into valid and enforceable contracts with Defendant whereby Defendant promised to provide healthcare and to protect their Sensitive information. Plaintiffs and members of the Nationwide

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Premera Policyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses, agreed to, among other things, pay money in consideration for such services.

153. Both the provision of healthcare and the protection of Plaintiffs' Sensitive Information were material aspects of Plaintiffs' and the Nationwide Premera Policyholder and Plan Administration Subclass members' or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses', agreements with Defendant.

154. As alleged in Paragraphs 27-34, above, Premera sends its Notice of Privacy Policy and its policy booklets to all members of the Nationwide Premera Policyholder and Plan Administration Subclass, forming an express contract requiring Premera to implement data security adequate to safeguard and protect the confidentiality of Sensitive Information.

155. Premera's policy booklets incorporate by reference Premera's company confidentiality policy, Code of Conduct, and Vendor/Contractor Privacy Basics in each of which, as alleged in Paragraphs 27-34, above, Premera explicitly promised to implement data security that would comply with federal and state laws, as well as industry standards, and that would safeguard and protect the confidentiality of Sensitive Information.

156. Alternatively, the express contracts between Premera and Plaintiffs and members of Nationwide Premera Policyholder and Plan Administration Subclass (or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses) included implied terms requiring Premera to implement data security adequate to safeguard and protect the confidentiality of their Sensitive Information, including in accordance with HIPAA regulations, federal, state and local laws, and industry standards. No member of the Subclass would have entered into contracts with Premera without understanding that their Sensitive Information would be safeguarded and protected; stated otherwise, data security—as set forth in Premera's Notice of Privacy Practices, Code of Conduct, and Vendor/Contractor Privacy Basics—was an essential implied term of the Parties' express contract.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

157. These contracts required that Defendant protect Plaintiffs' and the Nationwide Premera Policyholder and Plan Administration Subclass members' or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses', Sensitive Information and to prevent unauthorized access to such information.

158. Unfortunately, Defendant did not safeguard Plaintiffs' and the Nationwide Premera Policyholder and Plan Administration Subclass members' or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses', Sensitive Information. Specifically, Defendant did not comply with its promises to abide by HIPAA, federal, state and local laws, or industry standards, or otherwise protect individuals' Sensitive Information, as set forth above in paragraphs 62-67.

159. The failure to meet these promises and obligations constitutes a breach of express contract.

160. Because Defendant allowed unauthorized access to Plaintiffs' and the Nationwide Premera Policyholder and Plan Administration Subclass members' or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses', Sensitive Information and otherwise failed to safeguard it as promised, Defendant breached its contracts with Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass (or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses).

161. A meeting of the minds occurred, as Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, agreed to, among other things, provide Defendant with their accurate and complete information (including their

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Sensitive Information) and to pay Defendant in exchange for its agreement to, among other things, protect their Sensitive Information.

162. Defendant breached these contracts by failing to implement (or adequately implement) sufficient security measures to protect Plaintiffs' and the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass members' or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses', Sensitive Information.

163. Defendant's failure to fulfill its data security and management promises resulted in Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, receiving healthcare benefits that was of less value than they paid for (i.e., healthcare benefits coverage without adequate protection of Plaintiffs Sensitive Information).

164. Defendant's failure to fulfill its data security and management promises resulted in Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, losing the value of their privacy.

165. Stated otherwise, because Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, paid for privacy protections (as part of, among other things, their premiums) they did not receive what they paid for— even though

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

such protections were a material part of their contracts with Defendant— i.e. the full benefit of their bargain.

166. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, have suffered damages because they did not get the benefit of the bargain, including but not limited to the difference in the value of the secure healthcare benefits they paid for and the insecure healthcare benefits they received.

167. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, have suffered actual damages in an amount equal to the value of their privacy.

168. Accordingly, Plaintiffs, on behalf of themselves and the other members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass, or alternatively, the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, seek an order declaring that Defendant's conduct constitutes breach of express contract, and awarding them damages in an amount to be determined at trial.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

FIFTH CLAIM FOR RELIEF

Breach of Contract Implied-In-Fact
(On Behalf of Plaintiffs and the Nationwide Data Breach Class, or in the alterative, the Statewide Common Law Subclasses) (Plead in the Alternative to the Fourth Claim for Relief on Behalf of the Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses)

169. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

170. In order to procure Defendant's health insurance and/or other benefits, Plaintiffs and all Class members provided Defendant with their Sensitive Information.

171. By providing their Sensitive Information, and upon Defendant's acceptance of such information, Plaintiffs and all Class members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contracts concerning health insurance or other benefits that such Plaintiffs or Class members may have had with Defendant.

172. These implied contracts between Defendant and all Class members obligated Defendant to take reasonable steps to secure and safeguard Class members' Sensitive Information. The terms of these implied contracts are further described in the federal laws, state law, local laws, and industry standards alleged above, and Defendant expressly assented to these terms in its Notice of Privacy Practices, Code of Conduct, and public statements, also alleged above.

173. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiffs and all Class members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

174. Without such implied contracts, Plaintiffs and all Class members would not have provided their Sensitive Information to Defendant.

175. As described throughout, Defendant did not take reasonable steps to safeguard Plaintiffs' and other Class members' Sensitive Information.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

176. Because Defendant allowed unauthorized access to Plaintiffs' Sensitive Information and failed to take reasonable steps to safeguard that information, Defendant breached its implied contracts with Plaintiffs and all Class members.

177. Plaintiffs and all Class members suffered damages as a result of Defendant's breach of its implied contracts in the amount of the value of the privacy that was lost in Plaintiffs' and other Class members' Sensitive Information, which amount will be determined at trial.

178. With regard to members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass, members of the Statewide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclasses, and any other Class members who paid Defendant for health benefits, Defendant's failure to fulfill its data security and management promises also resulted in such Plaintiffs and Class members receiving less than the benefit of their bargain (e.g., treatment without adequate data security and management practices).

179. Stated otherwise, because such Plaintiffs paid for privacy protections (as part of, among other things, premiums or other payments for health treatment) they did not receive what they paid for—even though such protections were a material part of their contracts with Defendant—i.e. the full benefit of their bargain.

180. As a result of Defendant's conduct, members of the Nationwide Premera Policyholder and Plan Administration SubclassPolicyholder and Plan Administration Subclass, members of the Statewide Premera Policyholder and Plan Administration Subclasses, and any other Class members who paid Defendant for healthcare, suffered damages because they did not get the benefit of their bargain, including but not limited to the difference in the value of the secure health benefits for which they paid and the insecure health benefits they received.

181. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Statewide Premera Policyholder and Plan Administration Subclasses, have suffered actual damages in an amount equal to the value of their privacy.

182. Accordingly, Plaintiffs, on behalf of themselves and all Class members, seek an order declaring that Defendant's conduct constitutes breach of contract implied-in-fact, and awarding them damages in an amount to be determined at trial.

SIXTH CLAIM FOR RELIEF

Quasi-Contract/Restitution/Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Premera Policyholder and Plan Administration Subclass or, alternatively, the Statewide Premera Policyholder and Plan Administration Subclasses)

183. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

184. Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses, allege additionally and alternatively that they conferred a monetary benefit on Defendant in the form of fees paid for healthcare benefits. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses.

185. The fees for healthcare benefits that Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the Statewide Premera Policyholder and Plan Administration Subclasses, paid (directly or indirectly) to Defendant were supposed to be used by Defendant, in part, to pay for the administrative costs of data management and security.

186. Defendant did not use such fees to pay for the administrative costs of data management and security.

187. As a result of Defendant's conduct, Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass or alternatively, members of the

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Statewide Premera Policyholder and Plan Administration Subclasses, suffered actual damages in an amount equal to the difference in the free-market value of the secure healthcare benefits for which they paid and the insecure healthcare benefits they received.

188. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Nationwide Premera Policyholder and Plan Administration Subclass, or alternatively, the Statewide Premera Policyholder and Plan Administration Subclasses, because Defendant failed to implement (or adequately implement) the data management and security measures that they paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

SEVENTH CLAIM FOR RELIEF

Violation of State Consumer Protection Laws
(In the Alternative to Count I)
(On behalf of Plaintiffs and the Statewide Statutory Classes)

189. Plaintiffs incorporate all the foregoing allegations as if fully set forth herein.

190. Plaintiffs allege additionally and alternatively that the consumer protection laws listed below were enacted to protect consumers by promoting fair competition in commercial markets for goods and services. Specifically, they prohibit unlawful, unfair, deceptive, or fraudulent business acts or practices.

191. As described herein, Defendant has engaged in unlawful, unfair, and deceptive business acts or practices.

192. Based on its statutory and common law obligations, and as admitted and assumed by its own statements, Defendant had a duty to safeguard and protect Sensitive Information. Defendant expressly represented—including in its Notice of Privacy Practices, Code of Conduct, public statements, and other consumer-facing representations—that it would safeguard and protect Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards. Premera's specific representations are set forth

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

above in paragraphs 27-34. Defendant made these misrepresentations to Plaintiffs and the Statewide Statutory Subclasses when they enrolled in Defendant's health plans or agreed to provide Sensitive Information to Premera in exchange for coverage of healthcare services.

193. Consistent with its representations, Defendant accepted responsibility for securing Plaintiffs' and the Statewide Statutory Classes' Sensitive Information. Given that it was Defendant's responsibility for creating, overseeing, maintaining, and otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiffs' or the Statewide Statutory Classes' Sensitive Information in accordance with its express guarantees. This is particularly true given the many warning signs that Premera's systems were at risk of a breach—including those affecting the larger healthcare industry (e.g., the many other medical data breaches and warning of the Federal Bureau of Investigation's Cyber Division) and those relating to Premera's own security (e.g., the findings of the U.S. Office of Personnel Management investigation of Premera's own systems).

194. In particular, Defendant failed to disclose that its data security systems and practices did not comport with the express representations set forth above in paragraph 27-34, and otherwise described herein. As set forth specifically above in paragraphs 62-67, Defendant did not disclose that it did not take appropriate steps to secure electronic systems from unauthorized use, did not ensure that authorized personal had access to Sensitive Information only to the extent necessary to conduct their business, and did not meet its obligations under HIPAA and other state, local, and federal laws. In other words, Premera's data security representations amounted to affirmative misrepresentations or, at least, were misleading because of Premera's failure to disclose its actual data security practices. Its conduct was therefore unlawful.

195. Consistent with its representations, Defendant accepted responsibility for securing Plaintiffs' and the Statewide Statutory Classes' Sensitive Information. Given that it

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

was Defendant's responsibility for creating, overseeing, maintaining, and otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiffs' or the Statewide Statutory Classes' Sensitive Information in accordance with its express guarantees.

196. By failing to disclose its compliance with its own data security representations and other obligations, Premera engaged in unfair acts or practices. Premera made the data security representations discussed above to attract consumers—including Plaintiffs and members of the Statewide Statutory Classes —who were concerned about the privacy and security of their Sensitive Information.

197. Premera, however, failed to make good on its promises of data security by not investing the necessary resources in its cybersecurity program, not promptly notifying Plaintiffs and the Statewide Statutory Classes promptly about the data breach, and otherwise not living up to the specific representations and obligations set forth above in paragraphs 27-34. Given the known risk of maintaining Sensitive Information with lax cybersecurity practices, Premera's conduct was likely to cause substantial injuries to consumers.

198. As set out above, because only Premera knew (or should have known) that it was not complying with its own data security representations and obligations, there was no way for members of the public, including Plaintiffs and members of the Statewide Statutory Classes, to avoid the injury caused by Premera's conduct. Further, Premera's failure to live up to its data security representations and obligations did not create any countervailing benefits.

199. Consumers—like Plaintiffs and members of the Statewide Statutory Classes—value their privacy. Services (including healthcare benefits) that offer greater data security protections are more valuable to consumers than those with substandard security practices. Consumers will, if given the choice between two otherwise identical services, choose one with adequate security practices over one with substandard security practices.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

200. Because of this consumer preference for data security, a healthcare benefits company safeguarding and protecting Sensitive Information in accordance with HIPAA regulations, federal, state and local laws, and industry standards commands a higher market price for its coverage than a provider with substandard security.

201. Prior to the breach, neither Plaintiffs, nor members of the Statewide Statutory Classes, nor the general public knew that Defendant was not implementing data security and privacy protocols in accordance with its own consumer-facing representations and applicable duties. Defendant knew that Plaintiffs and the Statewide Statutory Classes would not allow Defendant access to their Sensitive Information—and thereby not give Defendant their business—if they knew Defendant could not and would not protect their Sensitive Information as it represented. And rather than implement the data security and privacy protocols it promised, Defendant actively concealed its true practices and protocols (which were of material concern to all of its customers) in order to lead consumers to give Defendant access to their Sensitive Data, while at the same time expressly promising that Sensitive Information would be protected as described above.

202. Based on the representations made by Defendant, Plaintiffs and the Statewide Statutory Classes believed Defendant would adequately protect their Sensitive Information, those security protections were valuable to them, and the protections formed the basis of their bargain inasmuch as Plaintiffs and the Statewide Statutory Classes would not have purchased healthcare benefits from Defendant at the prices charged (if at all) had Defendant disclosed its substandard security practices. Accordingly, Defendant's omission regarding the true protection standard was material.

203. To Plaintiffs and the Statewide Statutory Classes, Defendant's as-promised healthcare benefits offered significantly more utility or value than what was delivered, which lacked meaningful security protections. Thus, to Plaintiffs and the Statewide Statutory Classes,

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendant's secured healthcare benefits—as promised and paid-for—was substantially more valuable than the unsecure insurance received.

204. Accordingly, had Plaintiffs and members of the Statewide Statutory Classes known that Defendant did *not* actually implement its promised data security and privacy protocols, they would not have been willing to purchase its healthcare benefits at the prices charged, if they would have paid money at all.

205. Likewise, had Plaintiffs and members of the Statewide Statutory Classes known that Defendant did *not* actually implement its promised data security and privacy protocols, they would not have been willing to provide Defendant with their Sensitive Information.

206. Defendant's failure to disclose its substandard security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiffs' and the Statewide Statutory Classes' Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

207. Defendant's unfair acts or practices occurred in its trade or business and have injured a substantial portion of the public. Defendant's general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years (e.g., affected individuals could experience identity theft years later). As a direct and proximate result of Defendant's unfair acts, Plaintiffs and members of the Statewide Statutory Classes have suffered and will suffer actual injuries. Accordingly, Defendant's inadequate data security measure practices and/or omissions regarding its data security and privacy-related practices constitutes unlawful, deceptive, and unfair conduct in violation of the following State-specific consumer protection laws:

a. Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(E), (G), and (U);

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

b. Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code Ann. § 17.46(A), (B)(5) and (7);

c. Washington Consumer Protection Act, Wash. Rev. Code RCW §§ 19.86.010, *et seq.*;

208. As a result of Defendant's conduct, Plaintiffs and members of the Statewide Statutory Classes have suffered actual damages, including from the lost value of their privacy, the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm. Plaintiffs also suffered damages because, among other things, Premera promised them one thing (health care with adequate identity protection), but provided them a different, less valuable thing (health care without it).

209. Accordingly, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Classes, seek to enjoin further violation and recover actual damages (and treble damages where applicable).

210. With respect to injunctive relief, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Classes, seek an Order requiring Premera to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and ordering Premera to promptly correct any problems or issues detected by

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

such third-party security auditors; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera's systems; (5) purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services; (6) conduct regular database scanning and securing checks; (7) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

EIGHTH CLAIM FOR RELIEF

Violation of State Data Breach Notification Laws
(In the alternative to Second Claim for Relief)
(On behalf of Plaintiffs and the Statewide Statutory Classes)

211. Plaintiffs incorporate all the foregoing factual allegations as if fully set forth herein.

212. Plaintiffs allege additionally and alternatively that the data breach notification laws listed below were enacted to protect (or at least mitigate damage for) consumers from the consequences associated with data breaches. In relevant part, those laws require that businesses that maintain consumer data (including Sensitive Information) notify the owner of any breach of that data in the most expedient time and manner possible and without unreasonable delay.

213. The data breach described in Section II resulted in a breach of Plaintiffs' and the Statewide Statutory Class Members' Sensitive Information.

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

214. Defendant failed to disclose the breach of Plaintiffs' and the Statewide Statutory Class members' Sensitive Information in the most expedient time possible inasmuch as, after discovering the breach, it waited months before notifying all affected individuals. Defendant unreasonably delayed informing Plaintiffs and members of the Statewide Statutory Class about the data breach after it knew or should have known that the data breach had occurred.

215. Defendant's failure to provide timely notice of the data breach violated the following State-specific data breach notification laws:

a. Tenn. Code Ann. § 47-18-2107, *et seq.*;

b. Tex. Bus. & Com. Code Ann. § 521.053, *et seq.*; and

c. Wash. Rev. Code RCW §§ 19.86.010, *et seq.*

216. As a result of Defendant's conduct, Plaintiffs and members of the Statewide Statutory Class have suffered actual damages, including from the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

217. Accordingly, Plaintiffs, on behalf of themselves and members of the Statewide Statutory Class, seek all remedies available under their state data breach statute, including but not limited to (a) damages suffered by Plaintiffs and the Statewide Statutory Class members as

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

alleged above, (b) equitable relief, including injunctive relief, and (c) reasonable attorney fees and costs, as provided by law.

NINTH CLAIM FOR RELIEF

Misrepresentation by Omission
(On behalf of Plaintiffs and the Nationwide Data Breach Class or, alternatively, the Statewide Common Law Classes)

218. Plaintiffs incorporate all foregoing factual allegations as if fully set forth herein.

219. Premera knew or should have known that it failed to use sufficient measures to protect consumers' confidential data from hackers as described above.

220. Premera fraudulently, negligently, or recklessly concealed from, or failed to disclose to, the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, the fact that the measures it employed to protect consumers' confidential data from hackers were insufficient because they did not comport with its affirmative representations and other legal obligations (specifically set out in ¶¶ 27-34) in the manner set forth above (specifically set out in ¶¶ 62-67).

221. Premera was under a duty to the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to disclose the insufficient nature of its security measures because: Premera was in a superior position to know the true state of the facts about the design of its security measures because the design of such security measures is not public and Premera made partial representations and disclosures about maintaining the confidentiality of confidential data without revealing that it had taken insufficient and incomplete measures to protect that information from hackers.

222. The facts not disclosed to the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, are material facts in that a reasonable person would have considered those facts to be important in deciding whether or not to purchase insurance through Premera or otherwise allow Premera access to their Sensitive Information. Had the Nationwide Data Breach Class or alternatively, members of the Statewide Common

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Law Classes, known the insufficient nature of Premera's security measures, they would not have purchased insurance through Premera, would have paid less for it, or would not have permitted Premera to access their Sensitive Information in the first instance.

223. Premera intentionally, recklessly, or negligently concealed or failed to disclose the insufficient nature of its security measures for the purpose of inducing the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, to act thereon, and the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, justifiably relied to their detriment upon the truth and completeness of Premera's representations, including those set forth above in paragraphs 27-34. This is evidenced by the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, purchase of insurance through Premera and their willingness to let their Sensitive Information enter Premera's systems.

224. In order to prevent its statements from being misleading or from being a half-truth, Defendant should have disclosed its true practices with regard to storing and safeguarding the Sensitive Information in its control. Specifically, Premera should have disclosed that it did not implement industry-standard access controls, that it did not fix known vulnerabilities in its electronic security protocols, failed to protect against reasonably anticipated threats, and otherwise did not comport with its public-facing representations and legal obligations as set forth above in paragraphs 62-67. Thus, even if Premera was in compliance with certain HIPAA regulations; applicable state, federal, and local laws; or representations it made to consumers and customers, including those described above in paragraphs 27-34, it still should have disclosed to consumers those regulations, laws, and representations that it did not follow or comply with, whether in whole or in part.

225. As a direct and proximate cause of Premera's misconduct, the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, have suffered and will continue to suffer actual damages in ongoing, imminent, certainly impending threat of

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and the difference in the free-market value of the secure healthcare benefits for which they paid and the insecure healthcare benefits they received.

226. Accordingly, Plaintiffs, on behalf of themselves and members of the Nationwide Data Breach Class or alternatively, members of the Statewide Common Law Classes, seek an order declaring that Defendant's conduct constitutes a misrepresentation, and awarding them damages in an amount to be determined at trial.

227. Washington law should apply to the misrepresentation claim of the Nationwide Class, or, alternatively, the claims of the Statewide Common Law Classes should be governed by the law of each state in which such state specific claims are brought.

VII. REQUEST FOR RELIEF

Plaintiffs, on behalf of themselves and the Classes, respectfully request that this Court enter an Order:

1. Certifying this case as a class action on behalf of Plaintiffs and the Classes defined above, appointing Plaintiffs as representatives of their respective Classes, and appointing Interim Lead Counsel as Class Counsel;

2. Declaring that Premera's actions, as described above, constitute violations of the Washington Consumer Protection Act and the Washington Data Breach Disclosure law; Negligence; Breach of Express Contract; Breach of Implied Contract; Restitution/Unjust

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Enrichment; violations of the consumer protection laws of Oregon, and Texas; violations of the data breach notification laws of Tennessee, and Texas.

3. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Classes, including an order (i) prohibiting Premera from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Premera to protect all data collected through the course of its business in accordance with HIPAA regulations, federal, state and local laws, and industry standards; (iii) requiring Premera to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Premera's systems on a periodic basis, and ordering Premera to promptly correct any problems or issues detected by such third-party security auditors; (iv) requiring Premera to engage third-party security auditors and internal personnel to run automated security monitoring; (v) requiring Premera to audit, test, and train its security personnel regarding any new or modified procedures; (vi) requiring Premera to segment data by, among other things, creating firewalls and access controls so that if one area of Premera's network is compromised, hackers cannot gain access to other portions of Premera's systems; (vii) requiring Premera to purge, delete, and destroy in a reasonably secure manner Sensitive Information not necessary for its provisions of services; (viii) requiring Premera to conduct regular database scanning and securing checks; (ix) requiring Premera to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (x) requiring Premera to meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

4. Awarding actual, statutory, exemplary and punitive damages to Plaintiffs and the Classes, where applicable, in an amount to be determined at trial;

TOUSLEY BRAIN STEPHENS PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

5. Awarding restitution to Plaintiffs and the Classes in an amount to be determined at trial;

6. Awarding Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

7. Awarding Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable;

8. Permitting Plaintiffs and the Classes to amend their pleadings to conform to the evidence produced at trial; and

9. Awarding such other and further relief as equity and justice may require.

VIII. JURY DEMAND

Plaintiffs request a trial by jury.

DATED this 21st day of July, 2017.

TOUSLEY BRAIN STEPHENS PLLC

By: s/ *Kim D. Stephens*
Kim D. Stephens, #11984

By: s/ *Christopher I. Brain*
Christopher I. Brain #05054

By: s/ *Jason T. Dennett*
Jason T. Dennett #30686

By: s/ *Chase C. Alvord*
Chase C. Alvord, #26080

1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
Email: kstephens@tousley.com
cbrain@tousley.com
jdennett@tousley.com
calvord@tousley.com

Attorneys for Plaintiffs

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Ross Imbler, Stuart & Ilene Hirsh, et al.

(b) County of Residence of First Listed Plaintiff Fairbanks, Alaska
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Tousley Brain Stephens, 1700 7th Ave., #2200, Seattle, WA 98101
(206) 682-5600

DEFENDANTS

Premera Blue Cross, a Washington nonprofit corporation

County of Residence of First Listed Defendant King County, Washington
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	❒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
☒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
					❒ 893 Environmental Matters
					❒ 895 Freedom of Information Act
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 896 Arbitration
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 950 Constitutionality of State Statutes
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Class Action for data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Michael Simon DOCKET NUMBER 3:15-md-2633-SI

DATE 07/21/2017

SIGNATURE OF ATTORNEY OF RECORD s/ Kim D. Stephens

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Western District of Washington

ROSS IMBLER, STUART and ILENE HIRSH, KEVIN SMITH and CATHERINE BUSHMAN, SHARIF AILEY, APRIL ALLRED, ROBERT and THERESA FOULON, CRYSTAL HAYES, et al.

Plaintiff(s)

v.

PREMERA BLUE CROSS, a Washington nonprofit corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* PREMERA BLUE CROSS, a Washington nonprofit corporation
c/o CT Corporation, Registered Agent
711 Capitol Way S., Ste 204
Olympia, WA 98501

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Kim D. Stephens
TOUSLEY BRAIN STEPHENS PLLC
1700 7th Avenue, Suite 2200
Seattle, WA 98101

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: