IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN RE: PREMERA BLUE CROSS CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 3:15-md-2633-SI
This Document Relates to All Actions.	**OPINION AND ORDER PRELIMINARILY APPROVING CLASS ACTION SETTLEMENT AND NOTICE PROCEDURES AND SETTING FINAL APPROVAL HEARING**

Kim D. Stephens, Christopher I. Brain, and Jason T. Dennett, TOUSLEY BRAIN STEPHENS PLLC, 1700 Seventh Avenue, Suite 2200, Seattle, WA 98101; Keith S. Dubanevich, Steve D. Larson, and Yoona Park, STOLL BERNE, 209 SW Oak Street, Suite 500, Portland, OR 97204; Tina Wolfson, AHDOOT AND WOLFSON PC, 1016 Palm Avenue, West Hollywood, CA 90069; James Pizzirusso, HAUSFELD LLP, 1700 K Street NW, Suite 650, Washington, DC 20006; and Karen Hanson Riebel and Kate M. Baxter-Kauf, LOCKRIDGE GRINDAL NAUEN PLLP, 100 Washington Avenue South, Suite 2200, Minneapolis, MN 55401. Of Attorneys for Plaintiffs.

Paul G. Karlsgodt, BAKERHOSTETLER LLP, 1801 California Street, Suite 4400, Denver, CO 80202; James A. Sherer, BAKERHOSTETLER LLP, 45 Rockefeller Plaza, New York, NY 10111; Daniel R. Warren and David A. Carney, BAKERHOSTETLER LLP, 127 Public Square, Suite 2000, Cleveland, OH 44114; and Darin M. Sands, LANE POWELL PC, 601 SW Second Avenue, Suite 2100, Portland, OR 97204. Of Attorneys for Defendant.

Michael H. Simon, District Judge.

Premera Blue Cross ("Premera") is a provider and servicer of healthcare benefits. On March 17, 2015, Premera publicly disclosed that its computer network had been breached (the "Data Breach"), compromising the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera. The confidential information included names, dates of birth, social security numbers, member identification numbers, mailing addresses, telephone numbers, email addresses, medical claims information, financial information, and other protected health information (collectively, "Sensitive

Information"). Shortly after Premera's public disclosure, numerous plaintiffs sued Premera in separate putative class action lawsuits filed in multiple jurisdictions.

In June 2015, the Judicial Panel on Multidistrict Litigation ("JPML") transferred the lawsuits to this Court. In July 2015, the Court consolidated for pretrial purposes the transferred cases and all later-filed related lawsuits (collectively, the "Action"). In August 2015, the Court appointed Interim Lead Plaintiffs' Counsel and Interim Liaison Plaintiffs' Counsel, who filed a Consolidated Class Action Allegation Complaint, asserting state statutory and common law claims and requesting money damages and injunctive relief. Premera filed a motion to dismiss the consolidated complaint, which the Court granted in part and denied in part. In September 2016, Plaintiffs filed a First Amended Consolidated Class Action Allegation Complaint. Among other things, Plaintiffs alleged that the Data Breach began in May 2014 and went undetected for almost a year and that after Premera learned of the breach, Premera unreasonably delayed in notifying all affected individuals. In November 2016, Premera moved to dismiss the amended consolidated complaint, which the Court granted in part and denied in part in February 2017.

The parties conducted discovery, and the Court resolved several discovery disputes. In August 2018, Plaintiffs moved for class certification. The Court heard oral argument in November 2018, but before the Court issued its ruling, the parties requested time to discuss a possible settlement. On May 30, 2019, after several rounds of mediation, Plaintiffs filed under Rule 23 of the Federal Rules of Civil Procedure an unopposed motion for preliminary approval of a proposed class action settlement ("Settlement" or "Settlement Agreement"). For the reasons discussed below, the Court grants Plaintiffs' motion and preliminarily approves the proposed Settlement, subject to receiving any objections and holding a final approval hearing.

STANDARDS

A. Preliminary Approval Versus Final Approval

"Approval under [Rule] 23(e) involves a two-step process in which the Court first determines whether a proposed class action settlement deserves preliminary approval and then, after notice is given to class members, whether final approval is warranted." Carlin v. DairyAmerica, Inc., 380 F. Supp. 3d 998, 1005 (E.D. Cal. 2019) (quoting Nat'l Rural Telecomms. Coop. v. DIRECTV, Inc., 221 F.R.D. 523, 525 (C.D. Cal. 2004)). Plaintiffs assert that the standards the Court should apply in considering whether the Settlement deserves preliminary approval are not as stringent as the standards governing final approval. The Court disagrees and finds more persuasive the reasoning of several district courts that reject the older practice of engaging in an inquiry that is more lax when considering a motion for preliminary approval.

As explained by District Judge Vince Chhabria in the Northern District of California:

> Nobody appears to have offered a rationale for this [more lax] approach. . . . In any event, the idea that district courts should conduct a more lax inquiry at the preliminary approval stage seems wrong. Certainly nothing in the text of Rule 23 suggest courts should be more forgiving of flaws in a settlement agreement at the preliminary stage than at the final stage, or that courts should merely give settlement agreements a "quick look" at the outset. And lax review makes little practical sense, from anyone's standpoint. If the district court, by taking a quick look rather than a careful one, misses a serious flaw in the settlement, the parties and the court will waste a great deal of money and time notifying class members of the agreement, only to see it rejected in the end, requiring the parties to start over. . . . What's worse, if a court waits until the final approval stage to thoroughly assess the fairness of the agreement, momentum could have a way of slanting the inquiry, in a manner that deprives the class members of the court protection that Rule 23 demands.
>
> * * *
>
> [B]y scrutinizing the agreement carefully at the initial stage and

> identifying any flaws that can be identified, the court allows the parties to decide how to respond to those flaws (whether by fixing them or opting not to settle) before they waste a great deal of time and money in the notice and opt-out process.

Cotter v. Lyft, Inc., 193 F. Supp. 3d 1030, 1036-37 (N.D. Cal. 2016); see also Stoddart v. Express Servs., 2019 WL 414489, at *5 (E.D. Cal. Feb. 1, 2019) ("Rather, in light of the court's duty to absent class members, this court opts to 'review class action settlements just as carefully at the initial stage as [it] do[es] at the final stage.'" (alterations in original) (quoting Cotter, 193 F. Supp. 3d at 1037); *O'Connor v. Uber Techs., Inc.*, 201 F. Supp. 3d 1110, 1122 (N.D. Cal. 2016) (agreeing with the analysis in Cotter). This approach is even more compelling in a case such as this one, which involves a potential class of nearly 11 million people and thus will involve significant time and expense in class notification.

B. Settlement Class Versus Litigation Class

To certify either a settlement class or a litigation class, the requirements of Rule 23 of the Federal Rules of Civil Procedure must be satisfied. See Hanlon v. Chrysler Corp., 150 F.3d 1011, 1019 (9th Cir. 1998). Rule 23 affords the Court with "broad discretion over certification of class actions." Stearns v. Ticketmaster Corp., 655 F.3d 1013, 1021 (9th Cir. 2011). A plaintiff seeking class certification must satisfy each of the four express requirements of Rule 23(a)—numerosity, commonality, typicality, and adequacy of representation—plus at least one subsection of Rule 23(b). See, e.g., Lozano v. AT & T Wireless Servs., Inc., 504 F.3d 718, 724 (9th Cir. 2007).

"The criteria for class certification are applied differently in litigation classes and settlement classes." In re Hyundai & Kia Fuel Econ. Litig., 926 F.3d 539, 556 (9th Cir. 2019) (en banc). In considering a litigation class, the court "must be concerned with manageability at trial," whereas in considering a settlement class, "such manageability is not a concern . . . [because], by

definition, there will be no trial." Id. at 556-57. "On the other hand, in deciding whether to certify a settlement class, a district court must give heightened attention to the definition of the class or subclasses." Id. at 557. This will "demand undiluted, even heightened, attention in the settlement context" because the court "will lack the opportunity, present when a case is litigated, to adjust the class, informed by the proceedings as they unfold." Amchem Prods., Inc. v. Windsor, 521 U.S. 591, 620 (1997); see also Ortiz v. Fibreboard Corp., 527 U.S. 815, 848-49 (1999) ("When a district court, as here, certifies for class action settlement only, the moment of certification requires heightened attention.").

C. When a Proposed Settlement is Fair, Reasonable, and Adequate

Under Rule 23(e) of the Federal Rules of Civil Procedure, "[t]he claims, issues, or defenses of a certified class may be settled, voluntarily dismissed, or compromised only with the court's approval." "The purpose of Rule 23(e) is to protect the unnamed members of the class from unjust or unfair settlements affecting their rights." In re Syncor ERISA Litig., 516 F.3d 1095, 1100 (9th Cir. 2008). Thus, to approve a class action settlement, a court must find that the settlement is "fair, reasonable, and adequate." Fed. R. Civ. P. 23(3); Lane v. Facebook, Inc., 696 F.3d 811, 818 (9th Cir. 2012).

The settlement must be considered as a whole, and although there are "strict procedural requirements on the approval of a class settlement, a district court's only role in reviewing the substance of that settlement is to ensure it is 'fair, adequate, and free from collusion.'" Lane, 696 F.3d at 818-19 (quoting Hanlon v. Chrysler Corp., 150 F.3d 1011, 1027 (9th Cir. 1998). There are a number of factors guiding this review, including: (1) the strength of the plaintiffs' case; (2) the risk, expense, complexity, and likely duration of further litigation; (3) the risk of maintaining class action status throughout the trial; (4) the amount offered in settlement; (5) the extent of discovery completed and the stage of the proceedings; (6) the experience and views of

counsel; (7) the presence of a governmental participant; and (8) the reaction of the class members to the proposed settlement.[1] Id. at 819. Courts within the Ninth Circuit "put a good deal of stock in the product of an arms-length [sic], non-collusive, negotiated resolution." Rodriguez *v. West Publ'g Corp.*, 563 F.3d 948, 965 (9th Cir. 2009).

Class action settlements involve "unique due process concerns for absent class members who are bound by the court's judgments." Radcliffe v. Experian Info. Solutions Inc., 715 F.3d 1157, 1168 (9th Cir. 2013) (quotation marks and citation omitted). When the settlement agreement is negotiated before formal class certification, as in this case, the court should engage in "an even higher level of scrutiny for evidence of collusion or other conflicts of interest than is ordinarily required under Rule 23(e)." Id. (quotation marks and citation omitted). This more "exacting review" is warranted "to ensure that class representatives and their counsel do not secure a disproportionate benefit at the expense of the unnamed plaintiffs who class counsel had a duty to represent." Lane, 696 F.3d at 819.

The Ninth Circuit has recognized, however, that "[j]udicial review also takes place in the shadow of the reality that rejection of a settlement creates not only delay but also a state of uncertainty on all sides, with whatever gains were potentially achieved for the putative class put at risk." Staton v. Boeing Co., 327 F.3d 938, 952 (9th Cir. 2003). Thus, there is a "strong judicial policy that favors settlements, particularly where complex class action litigation is concerned." In re Hyundai, 926 F.3d at 556 (quoting Allen v. Bedolla, 787 F.3d 1218, 1223 (9th Cir. 2015)).

[1] This final factor may not be relevant when review is conducted at the preliminary approval stage, because class members have not yet had the opportunity to receive notice and respond to the proposed settlement. There may be circumstances, however, when class members respond to general public notice of the settlement and a court has some information on which to base an analysis of this factor. See, e.g., *O'Connor*, 201 F. Supp. 3d at 1132 (analyzing this factor based on some preliminary reactions from the class).

FACTUAL BACKGROUND

A. Premera's Operations

Premera is one of the largest health insurance benefit providers and servicers in the Pacific Northwest. Premera's headquarters is in Mountlake Terrace, Washington. Premera provides health insurance benefits and policies to companies headquartered in Washington, Oregon, and Alaska. Those companies, however, may have employees working in all 50 states and U.S. territories. Premera is also a member of a network of Blue Cross/Blue Shield companies that share provider networks, known as the "Blue Card Program." This program allows Premera's insureds to visit health care providers of other Blue Card Program members. In these situations, Premera services or administers the benefits, but not the claims, of its insureds. It also allows other, non-Premera insured Blue Card member insureds ("Blue Members") to visit providers within Premera's network in Washington and Alaska. For Blue Members visiting health care providers in Premera's network, Premera administers the claims. Premera also provides claims administration services for companies who provide their employees with self-funded (or employer-funded) insurance.

B. Premera's Representations about Protecting Sensitive Information

To provide benefits and claims administration services, Premera obtains the Sensitive Information of its insureds, Blue Members, and self-funded insureds for whom Premera provides claim administration. This information includes persistent identifying information such as names, dates of birth, social security numbers, member identification numbers, medical claims information, mailing addresses, and telephone numbers. It also includes transient identifiers such as credit card information.

Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Premera has certain obligations to keep Sensitive Information protected. Premera sent its

insureds a Notice of Privacy Practices ("Privacy Notice") in which Premera "committed to maintaining the confidentiality of your medical and financial information" and promised that Premera would "take steps to secure [its] buildings and electronic systems from unauthorized access." For companies with self-funded insurance for whom Premera provided claims administration, Plaintiffs contend that Premera includes a contractual provision that those entities must send a Privacy Notice containing similar text as provided by Premera. Thus, Plaintiffs contend that employees of self-funded employers receive a substantively similar Privacy Notice, for which Premera is legally responsible.

C. Premera's Understanding that Sensitive Information Requires Protection

Sensitive Information has value on the "black market" or "dark web" for illegal purposes, such as fraud and identity theft. Recognizing this, companies increasingly work to keep Sensitive Information protected. Health care companies are no exception and were targets for intrusions seeking Sensitive Information. In 2012 and 2013, Verizon Business Solutions ("Verizon Business"), a data breach industry consultant, reported that health care and social assistance industries represented more than seven percent of data breaches worldwide. On April 8, 2014, the Cyber Division of the Federal Bureau of Investigation ("FBI") issued a Private Industry Notification to companies within the healthcare sector, stating that the health care industry was a particularly susceptible target for cyber-attacks. The Notification specifically warned that "[t]he health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely."

Premera was aware that it might be a target for an intrusion. In its 2013 information technology ("IT") security training, Premera included training on malicious social engineering,

including phishing.[2] Premera's training provided examples of persons pretending to be from Premera's IT department asking Premera's employees to perform certain systems-related actions. Another example was other persons pretending to be users (such as a Premera associate, member, or vendor) who needed assistance from a Premera employee in gaining access to Premera's systems. Premera's training also included other pretextual methods that might be used, such as telephone or email "spoofing."

D. Premera's Awareness of Prior Problems with Its Data Security

Premera regularly had both internal and external audits of Premera's IT security. These audits showed deficiencies, many of them repeat deficiencies. For example, in 2011, Premera hired Verizon Business to perform a review. Verizon Business identified numerous critical and high risks within Premera's IT security system and procedures, including issues relating to patching, intrusion detection system ("IDS") and intrusion prevention system ("IPS") monitoring, logging, servers, and employee awareness.

In 2012 and 2013, Accuvant performed similar reviews for Premera. In 2012 Accuvant noted critical and high deficiencies with respect to, among other things: social engineering, network segmentation, security policies, log aggregation, patching, IPS, and weak passwords. In 2013, Accuvant again found problems at Premera, including issues concerning network segmentation, patching, social engineering, and passwords. Network segmentation can "help contain incidents" by allowing a company "to isolate some of the different systems and data from each other." Segmenting, thus, makes it more difficult for an intruder who has breached one

[2] "Social engineering" or "pretexting" is a technique in which the attacker invents a scenario to persuade, manipulate, or trick the target into performing an action or divulging information. "Phishing" is a specific social engineering technique in which an attacker uses fraudulent electronic communication (usually e-mail) to lure the recipient into divulging information.

protected section to obtain access to a company's entire network. In 2012, Accuvant found that Premera had "limited segmentation between different security tiers within this network, potentially allowing attackers to move freely from inconsequential systems to highly sensitive areas." In 2013, Accuvant increased the severity of its finding on network segmentation and warned that "once a system is compromised, adjacent systems can be targeted through traditionally less secure interior services to gain deeper access in the network if controls are not in place to isolate high-risk systems. A lack of strong segment and service access controls results in a larger attack surface and may allow an attacker to gain access to sensitive data assets." In 2014, Coalfire Labs performed an assessment for Premera. Coalfire Labs found deficiencies in patching, social engineering, and network segmentation.

Premera also performed internal audits. Premera employed two IT auditors who would conduct annual and biennial audits to assess various aspects of IT at Premera, including security. In 2013 and 2014, Premera conducted IT HIPAA audits, which identified "persistent significant deficiencies" and "deficiencies." One significant issue with Premera's IT security system, which was regularly noted as deficient, was Premera's IDS. An IDS is a critical tool in the detection of malicious activity. It is a set of systems that looks at information being passed throughout Premera to determine if there are any unauthorized accesses or to see if there are attempts to access, and reports the unwanted or malicious activity to the security organization.

In 2011, Verizon Business noted that although Premera had firewalls, there was no IDS monitoring on Premera's critical networks. Verizon Business stated the repercussion of this was: "An attacker could launch an attack against a system located behind one of these firewalls and gain access to sensitive data." Additionally, a senior manager of IT at Premera expressed concerns in 2012 regarding Premera's IDS.

Premera made some improvements to its IDS but continued to fail in its audits because it did not monitor the IDS logs. Premera's IDS remained a passive system that merely logged events (as compared to a system that would block intrusions). Premera's documented IT policies and procedures called for daily monitoring of the IDS logs. The 2007 and 2012 internal audits found deficiencies because the logs were not being monitored. The 2014 internal audit again found this to be a "significant deficiency" after determining that IDS monitoring had not been performed since March 2013.

Premera's audits also revealed deficiencies with Premera's "data loss prevention" ("DLP"), which monitors data leaving Premera's environment through email, exiting the firewalls, being transferred to a USB drive, and the like. A properly configured DLP blocks such transfers of data until they are reviewed and approved. Premera's DLP, "Vontu," was not properly implemented or monitored. It did not block any transfers but merely logged them. For example, the 2013 internal audit "identified multiple failures of the data loss prevention (DLP) software to block unauthorized PPI transfer via . . . external email accounts. . . . This may result in unauthorized transfer of PPI without the company being aware." The Vontu logs for the relevant time period have been destroyed and are unavailable for the pending litigation.

Another deficient area of Premera's IT security system was Premera's failure to monitor its logs, particularly those required by HIPAA. Premera was required to log and monitor access to its most sensitive information. The 2012 internal audit noted that there was "no evidence that IT has developed a logging and monitoring process that would satisfy the HIPAA requirements." The 2014 internal audit similarly found that "log-in monitoring was not being adequately or consistently monitored in accordance with published IT procedures" and designated it a repeat deficiency, in violation of HIPAA requirements.

To assist with monitoring the various logs, including IDS, in late 2013 Premera implemented a log aggregator system called "Splunk." Splunk was intended to assemble and aggregate the log data into one file that Splunk could analyze and Premera could monitor. Splunk could also send out alerts based on programmed rules. As of December 2013, however, Splunk was programmed to send out an alert on only one data point—signifying a membership change in the "admins" group. Given that the 2014 internal audit found significant deficiencies in IDS monitoring and HIPAA compliance monitoring, and a deficiency with DLP, it does not appear that Splunk had been properly configured in 2014 to achieve those monitoring functions.

There were also problems with monitoring Splunk itself. IT employees requested automated monitoring of the Splunk consolidated logs and manual review was flagged as a deficiency, but resources were not allocated for automated review. Additionally, the manual review was not consistently performed. An email summary of the 2014 internal audit explained, for example, that IDS logs are sent to Splunk, must then be manually reviewed, no one is assigned to manually review them, and thus this is a significant deficiency. Another deficiency repeatedly found in both internal and external assessments of Premera's IT security system was patching. Operating system, network, and software patching is necessary to respond to evolving threats and vulnerabilities, particularly malware.

The U.S. Office of Personnel Management ("OPM") also performed an audit of Premera. On April 17, 2014, OPM issued a draft report relating to its IT audit of Premera. Premera responded to the draft report's findings and concerns, both in writing and by implementing changes. OPM issued its final report on November 28, 2014. The final report noted "several areas of concern related to Premera's network security controls." These included that: (1) "critical patches, service packs, and hot fixes are not always implemented in a timely manner"; (2) "several servers contained noncurrent software applications that were no longer

supported by the vendors and have known security vulnerabilities," which "increases the risk of a successful malicious attack on the information system"; and (3) "several servers contained insecure configurations that could allow hackers or unprivileged users to insert code that would result in privilege escalation," which "could grant the hackers unauthorized access to sensitive and proprietary information." The report further noted that: (1) Premera had not created necessary baseline configurations; (2) "Premera cannot effectively audit its server and database security settings without an approved baseline, as a baseline configuration is the benchmark for comparison"; and (3) this failure increases the risk that the system may not meet security requirements. The report concluded, however, that nothing came to OPM's "attention to indicate that Premera is not in compliance with the various requirements of HIPAA regulations."

In the latter part of 2014, IT personnel at Premera prepared a presentation for members of Premera's contracting team to educate the team members on the importance of security questionnaires when contracting with third-party vendors. This presentation highlighted the threats to Premera of malicious software and hackers. From 2007 through 2014, Premera invested well below the healthcare industry average in security, when analyzed as a percentage of IT spending. IT management personnel would request funding for security-related items, which "often" would be denied, or would be funded significantly below the requested amount. For example, in September 2013, Eric Robinson, senior manager of Premera's Information Security Department, requested more than $1.5 million to fix some significant deficiencies identified in an IT audit and implement certain security measures to comply with HIPAA if Premera was going to start providing Medicare Advantage-related services. Mr. Robinson's request was ultimately funded at approximately a "few hundred thousand dollars."

Premera's IT security team also repeatedly complained that they were understaffed, and one member described working during the relevant time period before the Data Breach as feeling

like he was on a "sinking ship." Another noted that the feeling with the IDS was that "we won't get what we want until we have a breach." Various IT leaders recognized Premera's security deficiencies in 2014. One recommended hiring Mandiant to evaluate Premera, although the perception of some IT security employees was that the hiring of Mandiant was unnecessarily delayed, which itself was a security risk.

E. The Data Breach

The Data Breach began with phishing—an email sent to a Premera employee. Historical audits and assessments demonstrated that employees were vulnerable to phishing. For example, in 2012, Accuvant found that a significant number of targeted employees clicked on phishing links or provided credentials to unauthorized websites: 45% followed the provided link, 23% filled out a provided form, and 18% provided login credentials. In 2013, Accuvant had a 55% success rate in getting Premera employees to provide login credentials to a fake website. In 2014, Coalfire Labs conducted a similar test and of the 50 employees sent simulated phishing emails, 66% of those employees clicked on the link and 32% provided login credentials.

On May 5, 2014, hackers sent the phishing email to a Premera employee, purporting to be from Premera IT, but using a visibly incorrect email address that read "@premrera.com." The email provided a link to download a document. The employee clicked the link and downloaded the document, which contained malware that allowed the hackers access to Premera's server.

In the fall of 2014, Premera experienced an outbreak of "Zeus" malware infections. This was unrelated to the Data Breach. Premera hired Mandiant to perform a compromise analysis of the Zeus infections. Several months later, on January 29, 2015, Mandiant discovered the hackers in Premera's systems. Premera then had Mandiant perform a comprehensive assessment of this intrusion. In February 2015, Mandiant was investigating the full extent of the Data Breach. On February 20, 2015, Premera notified the FBI of the breach.

During Mandiant's investigation, it discovered at least seven deleted Roshal Archive Compressed ("RAR") files on Premera's servers that had been created during the time the hackers had been accessing the servers. These deleted RAR files totaled more than 350 MB of compressed data. Early in Mandiant's investigation, it noted that the evidence suggested that the deleted RAR files were more than likely created by the hackers. Mandiant's final report, however, did not include this conclusion. Mandiant also notified Premera that one of its servers was infected with a "full-featured backdoor" referred to as PHOTO. Mandiant explained that "PHOTO drops a driver that contains a keylogger and networking hooks. The malware has the ability to manipulate files, processes, the registry, and services and can also upload and download files and execute programs."

The evidence suggests that the group responsible for the ongoing breach of Premera's system was a Chinese Advanced Persistent Threat ("APT") group. Mandiant and other security consultants agree that this group specifically targets companies with a large amount of Sensitive Information so that it can exfiltrate the data, and that this group also was likely responsible for the OPM and Anthem data breaches, where large amounts of data were exfiltrated.

During its investigation, Mandiant informed Premera that the APT group had breached another of Mandiant's client's data and had exfiltrated large amounts of data. Mandiant informed Premera that Mandiant would begin searching Premera's servers for large file archives, which is when Mandiant found the RAR files.

On March 17, 2015, Premera notified the public, and its affected insureds and others whose Sensitive Information was potentially compromised, of the Data Breach. Premera revealed that its computer network was the target of "a sophisticated attack to gain unauthorized access to [its] Information Technology (IT) systems." The notice indicated that the "initial" attack occurred on May 5, 2014 and that the attackers "may have gained unauthorized access" to

Sensitive Information. The notice further stated: "The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately." Premera acknowledged how frustrating the incident is to affected individuals and offered "affected individuals" free credit monitoring and identity theft protection services for two years.

On April 14, 2015, Mandiant prepared a report for Premera. This report explained that the investigation was ongoing, but that it appeared the breach was from an APT group in China. The report explained that "state-sponsored groups target and steal" Sensitive Information to aid in espionage efforts and sometimes for financial profit. Mandiant specifically noted that some China-based threat groups operate on a contract basis and are motivated in part for financial gain. The financial motive may be particularly strong with information stored by healthcare companies because their "records are often worth more money in underground markets than stolen credit card numbers because the PII data can be used to mount more sophisticated financial crimes."

After the Data Breach, some Premera employees and other persons whose data was potentially accessed complained of suspicious activity. One Premera employee notified her supervisor that credit cards were opened using her social security number and her Premera work telephone number, commenting "it may be true that data did get out." After this report was sent up the supervisory chain, Kacey Kemp, Executive Vice President of IT and Operations at Premera, stated that Premera was relying on Mandiant and the FBI's investigations and thus Premera did not need to track this type of information from employees.

Consumers also called with concerns. Customers reported fraudulent tax filings, unauthorized bank charges, and medical charges for unrecognized services and prescriptions. Some Representative Plaintiffs also experienced instances of fraud after the Data Breach. In June 2015, Sharif Ailey had several unauthorized lines of credit opened in his name at retailers

such as Macy's, Lowe's, Sam's Club, and Best Buy. In February 2015, Elizabeth Black was notified by a cellular telephone retailer that multiple mobile phones were ordered using her name, address, social security number, and date of birth. Barbara Lynch learned in January and February 2015 that numerous unauthorized financial accounts had been opened in her name. Gabriel Webster experienced unauthorized charges on his credit card in November 2014, and in February 2015 his families' federal tax return was rejected because someone else had already filed a return using their names, address, social security numbers, and dates of birth. Catherine Bushman suffered tax fraud in 2015 and again in 2016, and several credit cards were opened fraudulently in her name. April Allred's minor son's social security number was used to file a tax return, and his social security number had not been provided anywhere other than to receive medical care and insurance and to her knowledge was not part of another data breach.

F. The Litigation

This consolidated lawsuit has been continuing for more than four years. The parties have exchanged significant document discovery totaling 1.5 million pages, litigated two motions to dismiss, filed and responded to several discovery motions, addressed Plaintiffs' motion for sanctions for spoliation of evidence, and attended several court hearings and numerous telephone status conferences. The parties collectively have taken more than 50 depositions, including eight expert depositions. Plaintiffs' motion for class certification and the parties' cross-motions to exclude certain expert testimony were fully briefed and argued before the parties asked the Court to stay consideration of these motions because the parties were close to reaching a settlement.

The parties engaged in extensive arm's-length settlement negotiations spanning several months. The parties, along with representatives of Premera's insurers, had three sessions with the Honorable Jay C. Gandhi (ret.) of Judicial Mediation and Arbitration Services, Inc. ("JAMS"). For two of the sessions, the parties had the additional aid of Peter K. Rosen, Esq. of JAMS. The

parties had multiple follow-up emails and telephone conferences with Judge Gandhi and Mr. Rosen. On February 15, 2019, the parties reached a preliminary agreement on the terms of a nationwide settlement. Numerous additional negotiations occurred to draft and complete a final written Settlement Agreement. The proposed Settlement Agreement was signed by the parties on May 29, 2019.

DISCUSSION

A. Preliminary Certification of the Settlement Class

Plaintiffs request preliminary certification for settlement purposes only of a Settlement Class defined as:

> All persons in the United States whose Personal Information was stored on Premera's computer network systems that was compromised in the Security Incident as publicly disclosed on March 17, 2015. Excluded from the Settlement Class are: (1) the Judge presiding over the Action, and members of his family; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former officers and directors; (3) Persons who properly execute and submit a request for exclusion prior to the expiration of the Opt-Out Period; and (4) the successors or assigns of any such excluded Persons.

The Court preliminarily considers whether certification of a settlement class is appropriate under the factors set forth in Rule 23.

Before certifying a class, the Court must assure itself that the proposed class action satisfies four prerequisites: (1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class. Fed. R. Civ. P. 23(a). In addition to meeting the numerosity, commonality, typicality, and adequacy prerequisites, the class action must fall within one of the three types specified in Rule 23(b). To

conclude that the requirements of Rule 23(b)(3) have been satisfied, the Court must find that questions of law or fact common to class members "predominate over any questions affecting only individual members" ("predominance") and that the class action must be "superior to other available methods for fairly and efficiently adjudicating the controversy" ("superiority"). Fed. R. Civ. P. 23(b)(3). Further, "[t]he district court's Rule 23(a) and (b) analysis must be 'rigorous.'" In re Hyundai, 926 F.3d at 556 (quoting Comcast Corp. v. Behrend, 569 U.S. 27, 33(2013)). The Court proceeds to consider the four requirements under Rule 23(a) plus the additional implicit requirement of ascertainability, followed by the requirements under Rule 23(b)(3).

1. Rule 23(a)

a. Numerosity

In this district, there is a "rough rule of thumb" that 40 class members is sufficient to meet the numerosity requirement. Giles v. St. Charles Health Sys., Inc., 294 F.R.D. 585, 590 (D. Or. 2013); see also Wilcox Dev. Co. v. First Interstate Bank of Or., N.A., 97 F.R.D. 440, 443 (D. Or. 1983) (same); 1 McLaughlin on Class Actions § 4:5 (15th ed.) ("The rule of thumb adopted by most courts is that proposed classes in excess of 40 generally satisfy the numerosity requirement."). With an alleged class size of approximately 10.6 million people, the Court finds that the numerosity requirement is met.

b. Commonality

In order to satisfy the commonality requirement, Plaintiffs must show that the class members suffered the "same injury"—that their claims depend upon a "common contention." Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338, 350 (2011) (quotation marks omitted). "That common contention, moreover, must be of such a nature that it is capable of classwide resolution—which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." Id. Class members, however, need

not have every issue in common: commonality requires only "a single significant question of law or fact" in common. Mazza v. Am. Honda Motor Co., 666 F.3d 581, 589 (9th Cir. 2012); see also Wal-Mart, 564 U.S. at 359.

The alleged harm is that all purported class members had their Sensitive Information accessed due to Premera's challenged conduct and inaction. There are many common issues of law and fact. These include whether Premera's data security practices were sufficient, whether the contracts issued by Premera included enforceable data security promises, whether Premera engaged in unfair or deceptive business practices with its data security practices or response to the Data Breach, whether the Data Breach compromised class members' Sensitive Information, and whether class members are entitled to damages as a result of Premera's conduct. The Court finds that the commonality requirement is satisfied.

c. Typicality

In order to meet the typicality requirement, Plaintiffs must show that the named parties' claims or defenses are typical of the claims or defenses of the class. Fed. R. Civ. P. 23(a)(3). Under the "permissive standards" of Rule 23(a)(3), the "representative's claims are 'typical' if they are reasonably co-extensive with those of absent class members; they need not be substantially identical." Hanlon v. Chrysler Corp., 150 F.3d 1011, 1020 (9th Cir. 1998). "The purpose of the typicality requirement is to assure that the interest of the named representative aligns with the interests of the class." Hanon v. Dataproducts Corp., 976 F.2d 497, 508 (9th Cir. 1992). To determine whether claims and defenses are typical, courts often look to "whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct." Id. (quotation marks omitted); see also Wolin v. Jaguar Land Rover N. Am., LLC, 617 F.3d 1168, 1175 (9th Cir. 2010).

In this case, the claims of the Representative Plaintiffs are reasonably co-extensive with those of the absent class members. They all allegedly suffered the same or similar injury from the same alleged conduct by Premera. The Court finds that the typicality requirement is satisfied.

d. Adequacy of representation

Rule 23(a)(4) states that before a class can be certified, a court must find that "the representative parties will fairly and adequately protect the interests of the class." This requirement turns on two questions: (1) whether "the named plaintiffs and their counsel have any conflicts of interest with other class members"; and (2) whether "the named plaintiffs and their counsel [will] prosecute the action vigorously on behalf of the class." Hanlon, 150 F.3d at 1020. The adequacy requirement is based on principles of constitutional due process, and a court cannot bind absent class members if class representation is inadequate. Hansberry v. Lee, 311 U.S. 32, 42-43 (1940); Hanlon, 150 F.3d at 1020.

During the briefing on Plaintiffs' motion for class certification, Premera argued that Representative Plaintiffs are inadequate because they are abandoning significant individual claims of identity theft (which likely could not be certified as a class due to the predominance of individual issues) in favor of smaller potential classwide damages for loss of value of Sensitive Information and overpayment of health insurance premiums (or a "market price premium" damages theory). Premera argued that abandoning identity theft damages constitutes "claim splitting" to the detriment of absent class members. Premera asserted that certification cannot be "purchased at the price of presenting putative class members with significant risks of being told later that they had impermissibly split a single cause of action." Feinstien v. Firestone Tire and Rubber Co., 535 F. Supp. 595, 606 (S.D.N.Y. 1982); see also Thompson v. Am. Tobacco Co., 189 F.R.D. 544, 550-51 (D. Minn. 1999) (noting, when the plaintiffs attempted to reserve

personal injury claims, that "[a] subsequent court may very well find that individual injury and damage claims should have been litigated in this lawsuit").

The Settlement, however, provides for a maximum recovery of $10,000 for Class Members to be reimbursed for out-of-pocket damages actually incurred that are plausibly traceable to the Data Breach, including up to 20 hours of personal time spent addressing the problem, at $20 per hour. In the briefing for class certification, Plaintiffs' expert opined that the average cost for medical identity theft, which is greater than regular identity theft, is approximately $13,453. Thus, Class Members who suffered damages from individual identity theft that can plausibly be traced to the Data Breach will be able to recover most of that average cost under the Settlement, regardless of whether the Action included a claim for individual identity theft. This recovery under the Settlement mitigates the concern of claim splitting. Furthermore, because the Settlement provides Class Members with the ability to opt-out, this further mitigates any potential concern of claim splitting. See Slade v. Progressive Sec. Ins. Co., 856 F.3d 408, 414 (5th Cir. 2017) (noting that the preclusion risk is smaller under a certification under Rule 23(b)(3) due to the opportunity to opt out); Andren v. Alere, Inc., 2017 WL 6509550, at *8 (S.D. Cal. Dec. 20, 2017) ("[C]ourts have noted that any risk of preclusion can be mitigated through the opt-out provisions under Rule 23(b)(3).").

The Court finds that Representative Plaintiffs share an interest with absent class members and do not have claims adverse to absent class members or that would benefit Representative Plaintiffs to the detriment of absent class members. The Court also finds that the Representative Plaintiffs and class counsel will prosecute this action vigorously on behalf of the class. The Court specifically selected class counsel for their extensive experience in prosecuting complex class actions. Class counsel has vigorously prosecuted the case thus far, including: responding to two motions to dismiss; obtaining and reviewing extensive discovery; filing several discovery

motions, a sanctions motion, and motions to strike portions of the testimony of Premera's experts; and moving for class certification. Class Counsel has demonstrated their willingness to continue prosecuting this case, including taking this matter to trial if necessary. Accordingly, the Court finds that the Representative Plaintiffs and Class Counsel are adequate to represent the class.

e. Ascertainability

Rule 23 also requires, at least implicitly, that the members of the proposed class be objectively ascertainable. Ott v. *Mortg. Inv'rs Corp. of Ohio, Inc.*, 65 F. Supp. 3d 1046, 1064 (D. Or. 2014). A proposed class must be "precise, objective, [and] presently ascertainable." See Williams v. Oberon Media, Inc., 468 F. App'x 768, 770 (9th Cir. 2012) (quotation marks omitted) (alteration added). Class members must be identifiable through "a manageable process that does not require much, if any, individual factual inquiry." Lilly v. Jamba Juice Co., 308 F.R.D. 231, 237 (N.D. Cal. 2014) (quoting William B. Rubenstein, 1 Newberg on Class Actions § 3:3 (5th ed.)). This requirement does not entail, however, that "every potential member . . . be identified at the commencement of the action." Id. (quotation marks omitted) (emphasis added). The purported class members have been identified through Premera's records. The Court finds that any ascertainability requirement is met.

2. Rule 23(b)(3)

Rule 23(b)(3) requires a court to find that "the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). This analysis, in accord with Rule 23's "principal purpose" of "promot[ing] efficiency and economy of litigation," inquires into "the relationship between the common and individual issues in the case, and tests whether the proposed class is

sufficiently cohesive to warrant adjudication by representation." Abdullah v. U.S. Sec. Assocs., Inc., 731 F.3d 952, 963-64 (9th Cir. 2013) (quotation marks omitted). The focus of this inquiry, however, is on "questions common to the class"—plaintiffs need not, at this threshold, "prove that the predominating question[s] will be answered in their favor." Amgen Inc. v. Conn. Ret. Plans & Tr. Funds, 568 U.S. 455, 459, 468 (2013) (emphasis in original).

a. Predominance

"[T]here is substantial overlap between" the test for commonality under Rule 23(a)(2) and the predominance test under 23(b)(3). Wolin v. Jaguar Land Rover N. Am., LLC, 617 F.3d 1168, 1172 (9th Cir. 2010). The predominance test, however, "is 'far more demanding,' and asks 'whether proposed classes are sufficiently cohesive to warrant adjudication by representation.'" Id. (citation omitted) (quoting Amchem, 521 U.S. at 623-24). To determine whether common questions predominate, the Court begins with "the elements of the underlying cause of action." Erica P. John Fund, Inc. v. Halliburton Co., 563 U.S. 804, 809 (2011).

In the class action context, choice of law should be considered as part of the predominance inquiry. Mazza v. Am. Honda Motor Co., 666 F.3d 581, 589-90 (9th Cir. 2012). "Subject to constitutional limitations and the forum state's choice-of-law rules, a court adjudicating a multistate class action is free to apply the substantive law of a single state to the entire class." In re Hyundai, 926 F.3d at 539. Additionally, in the context of considering predominance for a settlement class, "the district court need not consider trial manageability issues" such as "[t]he prospect of having to apply the separate laws of dozens of jurisdictions." Id. at 563.

The Settlement seeks to resolve four factually related causes of action: nationwide consumer protection act claims ("CPA"), nationwide negligence claims, nationwide breach of contract claims, and claims under California's Confidentiality of Medical Information Act

("CMIA"). Plaintiffs argue, and Premera does not object, that Washington law applies to the nationwide claims and California law applies to the CMIA claims.

i. Choice of law

In briefing the motion for class certification, Plaintiffs argued that Washington's choice-of-law rules should apply because Representative Plaintiffs are all from cases that were transferred from the Western District of Washington, and thus the "forum" state for those cases is Washington. Plaintiffs did not discuss which state's choice-of-law rules should apply in their motion for preliminary approval of the Settlement. The Ninth Circuit, however, recently accepted the "forum" state for purposes of an MDL case as the forum to which the MDL cases were transferred to, not from, in noting that generally when a federal court sits in diversity the forum state's choice-of-law rules apply, particularly absent argument by one of the parties to use the choice-of-law rules of a different state. In re Hyundai, 926 F.3d at 561.

Notably, Washington and Oregon apply the same choice-of-law analysis—first determining whether an actual conflict exists and then applying the "most significant relationship" test. See FutureSelect Portfolio Mgmt., Inc. v. Tremont Grp. Holdings, Inc., 180 Wash. 2d 954, 967 (2014) ("To settle choice of law questions, Washington uses the most significant relationship test as articulated by Restatement (Second) of Conflict of Laws § 145 (1971) [hereinafter ("Restatement Conflict of Laws"]); Spirit Partners, LP v. Stoel Rives LLP, 212 Or. App. 295, 304 (2007) ("We apply the 'most significant relationship' approach of the Restatement (Second) of Conflict of Laws (1971) to tort claims."); Citizens First Bank v. Intercontinental Exp., Inc., 77 Or. App. 655, 657 (1986) ("In deciding choice of law issues in contract actions, Oregon applies the law of the state which has the most significant relationship to the parties and to the transaction."). Both jurisdictions also look to § 148 of the Restatement Conflict of Laws when considering claims that sound in fraud. See FutureSelect, 180 Wash. 2d

at 967; Spirit Partners, 212 Or. App. at 305. Thus, the analysis is not meaningfully different, regardless of which state's choice-of-law analysis is applied. Accordingly, the Court applies choice-of-law rules of Oregon, the forum state.

A. Negligence and unfair practices claims

The Court presumes that there are conflicts between the law of Oregon and the laws and interests of various other states with respect to Plaintiffs' CPA and negligence claims. See, e.g., In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 486 (D. Minn. 2015) (assuming conflicts in a data breach case alleging similar claims). The Court therefore applies the most significant relationship test.

Plaintiffs' remaining unfair practices claim under the CPA is that Premera did not provide adequate data security. This claim does not sound in fraud and therefore is analyzed under § 145. Plaintiffs' negligence claim is also analyzed under § 145.

The contacts to be weighed in Restatement Conflict of Laws § 145 are: (a) the place where the injury occurred; (b) the place where the conduct causing the injury occurred; (c) the domicile, residence, place of incorporation, and place of business of the parties; and (d) the place where the relationship, if any, between the parties is centered. A court also must evaluate the interests and policies of the potentially concerned jurisdictions by applying the factors set forth in Restatement Conflict of Laws § 6. Portland Trailer & Equip., Inc. v. A-1 Freeman Moving & Storage, Inc., 182 Or. App. 347, 358-59 (2002). This approach is not merely to count contacts, but rather to consider the state that "has the most significant contacts with this dispute." Manz v. Continental Am. Life Ins. Co., 117 Or. App. 78, 80-81 (1992).

For the first § 145 factor, although generally in the case of injury to persons or property the place where the injury occurred plays an important role, other factors such as the place where the conduct occurred is given particular weight where the place of injury is fortuitous.

Restatement Conflict of Laws § 145 cmt. e at 420; see also Myers v. Cessna Aircraft Corp., 275 Or. 501, 516 (1976); Foster v. United States, 768 F.2d 1278, 1282-83 (11th Cir. 1985); Veridian Credit Union v. Eddie Bauer, LLC, 295 F. Supp. 3d 1140, 1153 (W.D. Wash. 2017). The place where the injury incurred is, for many class members, Washington, but for the out-of-state class members, it is their home state. Because Premera's conduct allegedly caused harm in all fifty states, however, this factor is not particularly important to the Court's analysis. Myers, Veridian, 295 F. Supp. 3d at 1153 ("Veridian alleges that Eddie Bauer's conduct with respect to the Data Breach caused injury in a variety of states throughout country; thus, the location of the alleged harm was fortuitous, and the place of injury does not play an important role in the court's choice of law analysis here." (citation omitted)).

The place where the conduct causing the injury occurred is Washington. Although for Plaintiffs' negligence action some conduct occurred by others in other locations (e.g., Plaintiffs providing Sensitive Information in their home states and the hackers engaging in conduct supposedly in China), the alleged negligent conduct was by Premera in Washington. See id. ("Veridian alleges that Eddie Bauer 'orchestrated and implemented' the decisions that lead to the Data Breach 'at its corporate headquarters in Bellevue, Washington,' and its failure to employ adequate data security measures 'emanated from [its] headquarters.' Based on these allegations, the court concludes that the place where the conduct alleged to have caused the injury occurred was in Washington." (alteration in original) (citation omitted)). Because the first factor is less important, this factor becomes more important. Id. The residence factor is neutral because Premera is incorporated and its principal place of business is Washington, and out-of-state Plaintiffs reside in another state.

The place where the relationship of the parties is centered, for purposes of the unfair practices claim alleging Premera's provision of inadequate data security, is Washington.

Washington is where the servers housing Plaintiffs' Sensitive Information resided, Premera implemented its data security, Premera employees received their allegedly inadequate training, the Premera employee opened the email providing access to the hackers, and the hackers were able to access the Sensitive Information. See In re Target Corp., 309 F.R.D. at 486 (applying Minnesota law to a negligence claim in a data breach case, noting that "Minnesota's contacts with this action are legion: Target is headquartered in Minnesota; its computer servers are located in Minnesota; the decisions regarding what steps to take or not take to thwart malware were made in large part in Minnesota"). Although there is some contact with Plaintiffs' various home states because Plaintiffs reside there, suffered injury there, and some provided Sensitive Information from there, that contact is more attenuated with the claim of Premera's inadequate provision of data security. Premera did not provide data security in any state other than Washington. The contacts with other states are more "fortuitous" than in the usual consumer protection case because where a particular plaintiff lives is not directly related to Premera's provision of data security, unlike consumer-protection cases involving the marketing and sale of goods to a consumer in a different state, or when products are purchased and readily could be taken to another state.[3] Moreover, for states other than Oregon and Alaska, Premera has not

[3] See, e.g., Mazza, 666 F.3d at 592 ("The automobile sales at issue in this case took place within 44 different jurisdictions, and each state has a strong interest in applying its own consumer protection laws to those transactions."); Pilgrim v. Universal Health Card, LLC, 660 F.3d 943, 947-48 (6th Cir. 2011) (noting that having the injured parties' state law apply is especially strong when the alleged misconduct involves companies from multiple states, and finding that the state law of the companies' is not strong when the alleged misconduct operated differently in every state and advertisements in each state were tailored to comply with state's consumer-protection laws); In re Bridgestone/Firestone, Inc., 288 F.3d 1012, 1018 (7th Cir. 2002) ("Indiana has consistently said that sales of products in Indiana must conform to Indiana's consumer-protection laws and its rules of contract law. It follows that Indiana's choice-of-law rule selects the 50 states and multiple territories where the buyers live, and not the place of the sellers' headquarters, for these suits." (citations omitted)); Coe v. Philips Oral Healthcare Inc., 2014 WL 5162912, at *3 (W.D. Wash. Oct. 14, 2014) ("The Toothbrushes were sold and purchased, and representations of their quality made and relied on, entirely outside of

directly marketed to or contracted with class members in that state. Premera contracts with employers in Washington, Oregon, and Alaska, and those employers, in turn, have employees in other states. This makes Premera's connection to those employees and their home states even more tenuous.

For Plaintiffs' negligence claims, there are multiple contacts within the relationship between Premera and the putative class members. Premera contracts to provide services for employers in Washington, Alaska, and Oregon. These employers, however, may have employees in all fifty states. Premera contracts with individuals in Washington and Alaska. Premera provides processing services for BlueCard members who receive health care in Washington. The bulk of these relationships, therefore, is in Washington. Furthermore, although the relationship between the putative class members and Premera involves contacts with more than one location, the place where the conduct causing the injury occurred is Washington. Ultimately, when the relationship is not clearly centered in one location, this factor bears little weight. See Veridian, 295 F. Supp. 3d at 1154. Although there are many relationships and many relevant locations, the most dominant location is Washington. Considering the factors and looking beyond merely counting contacts, the Court finds that the most substantive contact is the location causing the injury, which is Washington.

Considering the general policy concerns of Restatement Conflict of Laws § 6 and each state's CPA and similar laws also supports the application of Washington law to Plaintiffs' unfair practices claim. Some of these interests were discussed above in considering foreign state contacts. Additionally, Washington's interest in having businesses within its state comply with

---

Washington. No Plaintiff resides in Washington. . . . [T]he crux of Plaintiffs' action involves the marketing and sale of the Toothbrushes, which took place in other states.").

its statutes and provide adequate data security is greater than the interest of other states in having an out-of-state business provide adequate data security. Washington also has a paramount interest in enforcing its CPA against one of its own corporate citizens. See Veridian, 295 F. Supp. 3d at 1155 ("Application of the CPA to Veridian's claims effectuates the broad deterrent purpose of CPA, especially as applied to one of Washington's leading corporate citizens."); Coe v. Philips Oral Healthcare Inc., 2014 WL 5162912, at *3 (W.D. Wash. Oct. 14, 2014) ("Washington has a significant relationship to alleged deceptive trade practices by a Washington corporation. Washington has a strong interest in promoting a fair and honest business environment in the state, and in preventing its corporations from engaging in unfair or deceptive trade practices in Washington or elsewhere."). As discussed above, other state's interests in protecting their consumers are not as strong when the connection to that state is more fortuitous and there is no product sale or other transaction at issue. Under the facts of this data breach, the Court finds the choice-of-law interests better served by applying Washington law, where Premera is located, the data was maintained, the data security allegedly was inferior, and the breach occurred. See, e.g., Nat'l Union Fire Ins. Co. of Pittsburgh v. Tyco Integrated Sec., LLC, 2015 WL 3905018, at *13 (S.D. Fla. June 25, 2015) (applying Florida law even though injury occurred in Connecticut because defendant is headquartered in Florida, its "pertinent departments" are located in Florida, "a substantial portion of [its] IT and cybersecurity operations are based in Florida," it maintained computer servers in Florida, and thus it was "more likely than not, [its] failure to safeguard the information is an event that took place in Florida"); Willingham v. Glob. Payments, Inc., 2013 WL 440702, at *14-15 (N.D. Ga. Feb. 5, 2013) (applying the law of the state where the defendant was domiciled instead of where the injury occurred in part because the "Defendant's principal place of business is in Georgia, the

data breach occurred in Georgia, and to the extent, if any, Defendant breached a duty to consumers, it did so in Georgia").

Considering § 6 also supports applying Washington law to Plaintiffs' negligence claim. Washington had the "paramount" interest in applying its law, including negligence, to cyber-intrusion claims. Veridian, 295 F. Supp. 3d at 1155. Washington has a strong interest in deterring tortious conduct by its resident corporations. See, e.g., Johnson v. Spider Staging Corp., 87 Wash. 2d 577, 583 (1976). Although other states have an interest in seeing their residents compensated for injury committed by another's negligence, they do not have as strong an interest in punishing nonresident corporations. See, e.g., id. at 583-84 (noting in the context of alleged product defects that application of Washington law would deter tortious conduct and encourage manufacturers to make safe products, while the other state had no interest in applying its limitation to nonresident defendants being sued in their home state); see also Zenaida-Garcia v. Recovery Sys. Tech., Inc., 128 Wash. App. 256, 265 (2005) ("Washington has strong policy interests in deterring the design, manufacture and sale of unsafe products within its borders. In contrast, Oregon has no strong interest in application of its statute of repose to protect a Washington corporation . . . .").

Additionally, some of the differences in other states' negligence laws involve limitations on financial recovery, such as the economic loss doctrine, which is not a part of Washington law on negligence. These types of differences, "preventing financial burdens and exaggerated claims is primarily local; that is, a state by enacting a damage limitation seeks to protect its own residents." Johnson, 87 Wash. 2d at 582-83. Because Premera is a Washington resident, the interest of these other states in enforcing their damage limitations is reduced.

Similarly, some other states do not enforce a duty to maintain confidential information. Again, the interests of those state in protecting their resident companies from such a duty is

weakened when the defendant is a nonresident. To the extent Washington does enforce a duty to maintain confidential information, its interest in enacting and enforcing that duty on its resident corporations is stronger than a different state's interest in allowing a nonresident corporation not to be subject to such a duty. Considering the factors in Restatement Conflicts of Law § 6 and the purposes of each state's law, the Court finds application of Washington law to be appropriate.[4] See First Choice, 2018 WL 2729264, at *7 (applying the law of the state where the alleged conduct—improper data security—took place to multi-state negligence claims in data breach case); In re Target Corp., 309 F.R.D. 482, 486 (applying the law of the state where the alleged lack of security took place to nationwide negligence claims in data breach class action case); see also SELCO Cmty. Credit Union v. Noodles & Co., 267 F. Supp. 3d 1288, 1292 n.1 (D. Colo. 2017) (finding no actual conflict among the several relevant states, but noting that had there been a conflict, the court would apply to the negligence claims the law of the state where the alleged tortious conduct—improper data security—occurred because the "tortious conduct

[4] Even if the Court found that Washington law could not uniformly apply, the Court would still find that "the common factual and legal issues relevant to Plaintiffs' negligence claims greatly outweigh any individualized differences [in state law]." In re Anthem, 327 F.R.D. at 314. Similar to the Anthem data breach case, "the main issue boils down to the common factual contention of whether [Premera's] data security levels were reasonable. Plaintiffs' negligence claims would not get bogged down in the individualized causation issues that sometimes plague products-defects cases. Those cases often cannot clear the predominance hurdle because '[n]o single happening or accident occurs to cause similar types of physical harm or property damage.'" Id. (quoting Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1231 (9th Cir. 1996)). By contrast, this case involves "the same actions by a single actor [that] wrought the same injury on all [class members] together." Id.; see also Amchem, 521 U.S. at 625 ("Even mass tort cases arising from a common cause or disaster, may, depending upon the circumstances, satisfy the predominance requirement."). As the court noted in In re Anthem, this "is particularly true in light of Plaintiffs' unifying theory of damages based on the difference in value between the market price of the product [Premera] should have provided and the product actually provided. Therefore, the adequacy of [Premera's] security measures also permeates Plaintiffs' negligence claims and is not overwhelmed by state-law distinctions." In re Anthem, 327 F.R.D. at 314.

occurred at the company's headquarters in Colorado; more weight is accorded to the location of this conduct than normal because the resulting injuries occurred in multiple states; and the location of these injuries is fortuitous because the Noodles & Company customers whose information was compromised could have belonged to banks located anywhere in the world").

B. Breach of contract claim

Plaintiffs' breach of contract claim is based on the Privacy Notice. Contracts by Premera were entered into in Alaska, Oregon, and Washington. The Court need not conduct a choice-of-law analysis on this claim because common issues predominate regardless of the law applied, as discussed below.

C. CMIA claim

Plaintiffs' CMIA claim involves only Class Members who resided in California as of March 17, 2015, and asserts a claim under California law. Although Premera's conduct occurred in Washington, Premera offered insurance to persons in California knowing it was subjecting itself to additional statutory protections put in place by the California legislature. California has a significant interest in enforcing its statutory protections with respect to its citizens. Thus, California has the most significant interest with respect to this claim. The application of California law, therefore, is appropriate.

ii. Claim specific application

A. CPA unfair practices claim

Whether Premera implemented proper data security is a general question relating to Premera's practices and procedures and does not relate to individual class members' conduct. Premera is obligated under HIPAA to protect all Sensitive Information on Premera's servers. Determining the proximate cause of harm to Class Members is a fact question that involves common proof, such as whether Premera had adequate data security, whether Premera's lax

security led to the data breach, and whether there was exfiltration of data. Additionally, under Washington law reliance is not an element of this claim.

The unfair practices claim is not a claim involving deception. The Washington Supreme Court acknowledged that "unfair" could be different from "deceptive" under Washington's CPA. Klem v. Wash. Mut. Bank, 176 Wash. 2d 771, 787 (2013) (defining unfair practices as an act that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits") (quoting 15 U.S.C. § 45(n)). Challenges to the legal sufficiency of this claim (including whether it is nothing more than a negligence claim and impermissible under the CPA) and would survive on the merits is a uniform question for the entire class and does not pose individualized questions. Accordingly, this claim does not present a predominance issue. The Court finds common issues predominate with respect to Plaintiffs' unfair practices CPA claim.[5]

B. Negligence claim

To prove a negligence claim under Washington law, a plaintiff must show: "(1) the existence of a duty, (2) breach of that duty, (3) resulting in injury, and (4) proximate cause."

[5] Even if the Court did not uniformly apply Washington law, the Court would still conclude that under non-identical state CPA laws "this is a case in which 'the idiosyncratic differences between state consumer protection laws are not sufficiently substantive to predominate over the shared claims.'" In re Anthem, 327 F.R.D. at 315 (quoting Hanlon, 150 F.3d at 1022-23). Because Plaintiffs' unfair practices act claim is based on Premera's alleged failure to provide adequate data security, it involves the uniform aspects of state CPA laws. Id. "Liability is not tied to an element, like reliance, that may sometimes require evaluating each individual Plaintiff's circumstances. Rather, because the common issues turn on a common course of conduct by the defendant, '[a] common nucleus of facts and potential legal remedies dominates this litigation.'" Id. (alteration in original) (quoting Hanlon, 150 F.3d at 1022) (citation omitted). Moreover, concerns about trial manageability with applying the varying laws of separate states, which is often a major concern with respect to predominance when there are differences in state law, is not applicable when considering certification for settlement purposes only. In re Hyundai, 926 F.3d at 563.

Ranger Ins. Co. v. Pierce Cty, 164 Wash. 2d 545, 552 (2008). These elements can be resolved on a classwide basis, because Plaintiffs' negligence claim predominantly turns on whether Premera provided adequate data security. Premera's duty, if any, to protect Sensitive Information, would be owed classwide and whether that duty was breached also would be a class question. Proximate cause similarly would be shown by class wide evidence. Plaintiffs also had two theories of damages that involved classwide proof and apply uniformly. See, e.g., In re Anthem, 327 F.R.D. at 314 (noting, in finding that common issues of law and fact predominate with respect to the plaintiffs' negligence claim, that predominance "is particularly true in light of Plaintiffs' unifying theory of damages based on the difference in value between the market price of the product Defendants should have provided and the product actually provided"). Thus, common issues of law and fact predominate.[6]

C. Breach of contract claim

Common issues predominate in Plaintiffs' breach of contract claim regardless of whether Washington, Alaska, or Oregon law governs. The question of contract formation and whether the Privacy Notice representations are included in the relevant contract is common. There may be a question for a specific subcategory of class members—employees of self-funded employers—as

[6] Even if the Court did not uniformly apply Washington law, the Court would still conclude that under non-identical state negligence laws, "[t]his case does not implicate any of the state-specific issues that can sometimes creep into the negligence analysis. Plaintiffs allege that Defendants breached a duty of care to their customers because of Anthem's inadequate security measures. Again, the main issue boils down to the common factual contention of whether Anthem's data security levels were reasonable. Plaintiffs' negligence claims would not get bogged down in the individualized causation issues that sometimes plague products-defect cases. Those cases often cannot clear the predominance hurdle because '[n]o single happening or accident occurs to cause similar types of physical harm or property damage.' Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1231 (9th Cir. 1996). Here, by contrast, the same actions by a single actor wrought the same injury on all Settlement Class Members together." In re Anthem, 327 F.R.D. at 314 (citation omitted) (first alteration added, second alteration in original).

to whether Premera's purported instructions on what to include in the privacy notice sent by those employers is sufficient to impute liability onto Premera for a breach of that privacy notice, but that, too, is a common question for that entire category of people. Whether the representations in the Privacy Notice created obligations on Premera to provide a certain level of data security is also a common question.

The key issues of interpretation and breach asserted in this case do not require individualized adjudication. "The central issue of breach turns on the common question [of] whether [Premera's] security measures are adequate." In re Anthem, 327 F.R.D. at 314. The central issues of interpretation are whether Premera's contracts incorporated by reference the Privacy Notice, whether the Privacy Notice created any obligation by Premera, and whether Premera bears legal responsibility for the privacy notice sent by self-funded employers. All of those involve common issues of law and fact and do not require the resolution of individualized inquiries.

Courts routinely certify classes involving standardized conduct and standard from contracts and documents. See, e.g., Sacred Heart Health Systems, Inc. v. Humana Military Healthcare, 601 F.3d 1159, 1171 (11th Cir. 2010) ("It is the form contract, executed under like conditions by all class members, that best facilitates class treatment."); Allapattah Servs., Inc. v. Exxon Corp., 333 F.3d 1248, 1261 (11th Cir. 2003) (certifying breach of contract claims where "all of the dealer agreements were materially similar and Exxon purported to reduce the price of wholesale gas for all dealers" and collecting cases); Smilow v. Sw. Bell Mobile Sys., 323 F.3d 32, 39-42 (1st Cir. 2003) (certifying breach of contract claim based on standard form mobile phone contract and alleged breach thereof in charging for incoming calls, finding "that common issues of law and fact predominate" because "[t]he case turns on interpretation of the form contract, executed by all class members and defendant"); Zepeda v. Paypal, Inc., 2015 WL 6746913, at *8

(N.D. Cal. Nov. 5, 2015) ("Plaintiffs allege that PayPal utilized standardized form contracts and uniformly breached those contracts in the same manner with respect to Plaintiffs and the other members of the Claims Class. This is sufficient to show that common questions of fact and law predominate."); In re Med. Capital Secs. Litig., 2011 WL 5067208, at *3 (C.D. Cal. July 26, 2011) ("Courts routinely certify class actions involving breaches of form contracts."); Winkler v. DTE, Inc., 205 F.R.D. 235, 243 (D. Ariz. 2001) (certifying breach of contract claim based on standard purchase contracts of used car dealer and overcharges of official registration fees); Mortimore v. Fed. Deposit Ins. Corp., 197 F.R.D. 432, 438 (W.D. Wash. 2000) ("Since this case involves the use of form contracts, it is particularly appropriate to use the class action procedure").

"The basic elements of breach of contract are the same across states." In re Anthem, 327 F.R.D. at 314 (citing cases). The Court had identified a material difference between Oregon and Washington law relating to Plaintiffs' alternative theory of breach of an implied term in the express contract in its opinion on Premera's second motion to dismiss. See In re Premera, 2017 WL 539578, at *13-14. Plaintiffs, however, are not pursuing that theory. Plaintiffs are pursuing only a theory of breach of the express terms of the contract.

Although the Court does not find any material conflict with applying Washington law to the basic elements of breach of contract, Plaintiffs' contract allegations also include that the Privacy Notice was incorporated into the parties' contract by reference. There are differences between Oregon, Alaska, and Washington law on how documents are incorporated by reference into a contract. Under Oregon law, "[o]ne document need not expressly incorporate the other by reference if the connection between them is unmistakable." McInnis v. Lind, 198 Or. App. 139, 149 (2005). Washington law, however, requires "the parties to a contract clearly and unequivocally incorporate by reference into their contract some other document." Cedar River

Water & Sewer Dist. v. King Cty., 178 Wash. 2d 763, 785 (2013), as modified (Jan. 22, 2014) (quoting Satomi Owners Ass'n v. Satomi, LLC, 167 Wash. 2d 781, 801 (2009)). Under Alaska law, "[p]arties do not undertake obligations contained in a separate document unless their contract clearly says so. . . . A reference in a contract to another document will incorporate the other document only to the extent indicated and for the specific purpose indicated." Prichard v. Clay, 780 P.2d 359, 361-62 (Alaska 1989). Accordingly, the Court finds that there are material differences between Oregon, Washington, and Alaska law on how documents are incorporated by reference.

The fact that there are material differences in the laws of the three states on this point of contract law, however, does not preclude certification of a nationwide class. Because the individual state law issues do not "swamp" the common issues and there are only three states involved, the Court finds that common issues predominate even when portions of Plaintiffs' breach of contract claims are governed by state law. Moreover, because trial manageability is not a concern when a court is considering certification at settlement, this difference in state law does not defeat predominance. In re Hyundai, 926 F.3d at 563.

D. CMIA claim

California's CMIA requires covered entities to maintain medical information "in a manner that preserves the confidentiality of the information" and establishes than any such entity "who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties" set forth in the act. Cal. Civ. Code § 56.101(a). Protected medical information includes information "regarding a patient's medical history, mental or physical condition, or treatment" and "individually identifiable information . . . such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly

available information, reveals the individual's identity." Id. § 56.05(j). To state a claim under the CMIA, a plaintiff must show that the defendant had the plaintiff's medical information, negligently maintained, preserved, stored, abandoned, destroyed, or disposed of that information, and that as a result "the confidential nature of the plaintiff's medical information was breached," meaning that the information was "accessed, viewed, or used." Regents of the Univ. of Cal. v. Superior Court, 220 Cal. App. 4th 549, 570, 570 n.15 (2013).

Plaintiffs' CMIA claim only includes Class Members who resided in California before March 17, 2015. This claim involves common issues of law and fact. The question of whether Premera had Sensitive Information is not disputed. The question of whether Premera negligently maintained, preserved, or stored the information would be resolved on a classwide basis. The question of whether a third party (the alleged hackers) accessed the data is also a common question, because it involves common evidence regarding whether data was exported or exfiltrated from Premera's servers. Finally, the question of whether a particular Class Member resided in California during the relevant time period is easily resolved on a classwide basis. Accordingly, common issues of law and fact predominate with respect to this claim.

b. Superiority

Rule 23(b)(3)'s superiority requirement tests whether "classwide litigation of common issues will reduce litigation costs and promote greater efficiency." Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1234 (9th Cir. 1996). To make this determination, a court looks to "whether the objectives of the particular class action procedure will be achieved in the particular case." Hanlon, 150 F.3d at 1023. In turn, this inquiry "necessarily involves a comparative evaluation of alternative mechanisms of dispute resolution." Id. The Ninth Circuit recognizes that "[d]istrict courts are in the best position to consider the most fair and efficient procedure for conducting any given litigation, and so must be given wide discretion to evaluate superiority." Bateman v.

Am. Multi-Cinema, Inc., 623 F.3d 708, 712 (9th Cir. 2010) (quotation marks and citation omitted). Relating to superiority, the purpose of Rule 23(b)(3) is "to allow integration of numerous small individual claims into a single powerful unit." Id. at 722. This allows plaintiffs that otherwise likely would be "unable to proceed as individuals because of the disparity between their litigation costs and what they hope to recover. . . . 'to pool claims which would be uneconomical to litigate individually.'" Local Joint Exec. Bd. of Culinary/Bartender Tr. Fund v. Las Vegas Sands, Inc., 244 F.3d 1152, 1163 (9th Cir. 2001) (quoting Phillips Petroleum Co. v. Shutts, 472 U.S. 797, 809 (1985)).

Rule 23(b)(3) provides four non-exhaustive factors to consider. These factors are:

> (A) the class members' interests in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing a class action.

Fed. R. Civ. P. 23(b)(3).

Regarding the first factor, "[w]here recovery on an individual basis would be dwarfed by the cost of litigating on an individual basis, this factor weighs in favor of class certification." Wolin v. Jaguar Land Rover N. Am., LLC, 617 F.3d 1168, 1175 (9th Cir. 2010). The amount at stake for putative class members is too small when compared to the cost of litigating individual claims. Even the small percentage of class members who have suffered actual identity theft have claims that are too small. "Litigation costs would be quite high, given that the case involves complex technical issues and requires substantial expert testimony." In re Anthem, Inc. Data Breach Litig., 327 F.R.D. 299, 314 (N.D. Cal. 2018). Accordingly, "[b]ecause individual damages pale in comparison to the costs of litigation, this factor points toward certification." Id. at 316.

Regarding the second factor, the JPML originally transferred 29 related federal cases to this Court for coordinated pretrial proceedings. ECF 1. As additional related actions were filed and brought to the attention of the JPML, they also were transferred. Currently, there are 42 actions pending before this Court. The parties have not identified any other related cases. As articulated by the JPML, the "actions share factual questions arising from [the same] data security breach" and "[c]entralization will eliminate duplicative discovery, prevent inconsistent pretrial rulings, particularly with respect to class certification, and conserve the resources of the parties, their counsel, and the judiciary." ECF 1. This factor thus weighs in favor certification. See In re Anthem, 327 F.R.D. at 316.

With respect to the third factor, the JPML explained that this district "is a convenient and accessible forum for this litigation" and "has the necessary judicial resources and expertise to manage this litigation efficiently." ECF 1. The Court agrees that this forum is convenient for Premera, who is headquartered in Washington, and who contracts in Oregon. Plaintiffs are located in all 50 states, but have a higher concentration in Washington, Oregon, and Alaska. This factor is also less important in the context of a settlement because it is likely that the only remaining in-court proceeding will be the final hearing to evaluate whether the Settlement is fair, reasonable, and adequate and to consider the requested attorney's fees and costs and Service Awards ("Final Fairness Hearing"). Consequently, this factor also supports certification.

The fourth factor requires courts to consider the likely difficulties in managing a class action. Manageability concerns, however, are not relevant in the context of a settlement. Amchem, 521 U.S. at 620; In re Hyundai, 926 F.3d at 563. Thus, this factor is not applicable. The applicable superiority factors support certification.

3. Conclusion Under Rule 23(a) and Rule 23(b)(3)

The Court preliminarily finds that the proposed Settlement Class meets the requirements of Rule 23(a) and Rule 23(b)(3). Accordingly, the Court preliminary certifies, for settlement purposes only, the proposed Settlement Class.

B. Preliminary Approval of the Settlement

Plaintiffs ask the Court preliminarily to find that Settlement Agreement is fair, reasonable, and adequate and that the notice procedures comport with due process. The Court considers the relevant factors as set forth by the Ninth Circuit and previously stated.

1. Strength of Plaintiffs' case and the risk, expense, complexity, and likely duration of further litigation and maintaining class action status through trial

Plaintiffs have several strong arguments regarding the level of data security implemented by Premera, particularly in light of the internal and external audits that occurred before the Data Breach and the fact that the breach was able to go on for so long without being detected. Whether Premera breached its contractual promises, was negligent, or engaged in unfair practices under Washington's CPA with respect to Premera's provision of data security are relatively strong claims. Plaintiffs have a weaker case with respect to damages, because their damages theories and experts are vulnerable to challenge and the number of Class Members who appear to have suffered actual identity theft or out-of-pocket damages that can reasonably be attributed to the Data Breach appears to be relatively low. Thus, at trial Premera could challenge Plaintiffs' contention that their Sensitive Information actually was exfiltrated and used. In response, however, Plaintiffs could argue that it is a reasonable inference that hackers would not continue an incursion for a such a long period of time only to take no data (notwithstanding the ability to do so) or otherwise do nothing with the data that was taken. Plaintiffs also would face

Premera's dispositive motions, including Premera's argument under the filed-rate doctrine, and the risk that some or all of Plaintiffs' claims might not survive.

On the other hand, Premera faces the risk that at least some of Plaintiffs claims likely would be certified for class status and might survive dispositive motions. Premera also faces a potentially large liability if they were to lose at trial. Premera also has some difficult facts regarding its past data security practices as well as how Premera handled the Data Breach after it became known.

This case is complex, involving evidence spanning multiple years, technical information regarding computer servers and hackers, state-sponsored hacking versus other types of hacking, medical information, the dark web, and the implications of spoliation of a particular server. The parties exchanged 1.5 million pages of documents. The case has been expensive to litigate, and continuing litigation would be time-consuming and add further expense. There is currently pending a motion for partial summary judgment that requires additional briefing, and the case schedule includes additional dispositive motions that the parties anticipate would be filed. If at least some of Plaintiffs' claims survive dispositive motions, the parties would spend significant time and expense preparing for a class action or bellwether trial, possible additional trials in other jurisdictions, and likely appeals. The case schedule that was put on hold and ultimately stricken because of the Settlement included another nearly 11 months of litigation.

The motion for class certification was fully briefed and argued at the time of Settlement. Plaintiffs risk that none of their claims would be certified for class treatment, and Premera risks that all or some of Plaintiffs' claims would be certified. If certified, there remains a risk for Plaintiffs that certification would not be able to be maintained throughout trial, including after Premera's dispositive motions were resolved. Considering these three factors (the strength of Plaintiffs' case; the risk, expense, complexity, and likely duration of continued litigation; and the

risk of maintaining class action status through trial), the Court finds that they weigh in favor of granting approval to the Settlement.

2. The amount offered in settlement

The Settlement Agreement provides for both monetary and non-monetary relief.

a. Monetary relief

In considering the potential fairness of the recovery, courts often compare the total amount of recovery in a settlement to the estimated total amount of damages that could be recovered if the case was litigated when considering the fairness of the recovery. See, e.g., In Re Mego Fin. Corp., 213 F.3d 454, 459 (9th Cir. 2000). Nonetheless, "[i]t is well-settled law that a cash settlement amounting to only a fraction of the potential recovery does not per se render the settlement inadequate or unfair." Id. (quoting Officers for Justice v. Civil Serv. Comm'n, 688 F.2d 615, 628 (9th Cir. 1982).

The Settlement Agreement provides that Premera will pay $32 million to fund a non-reversionary Qualified Settlement Fund. This fund will pay the costs of recovery to Class Members, attorney fees and costs, Service Award to the Representative Plaintiffs, and the costs to administer the Settlement, including giving notice to Class Members. No less than $10 million will be used to provide the recovery to Class Members. This recovery includes: (1) up to $10,000 per Class Member for reimbursement of proven out-of-pocket damages that can plausibly be traced to the Data Breach, including up to 20 hours of personal time at $20 per hour; (2) a default settlement amount of up to $50 for Class Members who do not have out-of-pocket damages that can plausibly be traced to the Data Breach; (3) up to an additional $50 for Class Members who resided in California as of March 17, 2015, for the CMIA claim; and (4) two years of credit monitoring and insurance services for Class Members, who may choose to delay the start of such services for up to two years if the Class Member already has credit monitoring. Up to $3,500,000

will be set aside for the wholesale purchase of this insurance. If the credit monitoring and insurance services cost less than $3.5 million, the remaining amount will revert to the Qualified Settlement Fund to be distributed to the Class Members on a pro rata basis or to fund additional credit monitoring services.[7]

The Court recognizes that a guarantee of no less than $10 million to be spent on the recovery of a class of potentially 10.6 million people may seem low. The reality, however, is that through the time of the briefing on class certification, it does not appear that the percentage of Class Members who suffered actual identity theft, and therefore would be eligible for the out-of-pocket reimbursement, is very large. The Court also recognizes that even assuming that no Class Member suffered identity theft that could plausibly be traced to the Data Breach, the default settlement of $50 would only allow for recovery by 130,000 Class Members.[8] This is only 1.23 percent of the total potential class of 10.6 million people. This calculation also does not include any recovery for the CMIA claim. The Court assumes that it is likely that there will be some Class Members eligible for CMIA recovery and some eligible for out-of-pocket reimbursement. It is also possible (perhaps even likely) that more than 1.23 percent of the class will submit Claim Forms. Accordingly, it is unlikely that the Class Members will recover the full $50 in default settlement or CMIA recovery if only $10 million is available to fund Class Members' benefits.

[7] The Settlement Agreement and Plaintiffs' motion for preliminary approval do not identify what the wholesale cost is per Class Member for the credit monitoring service, or explain whether there is a possibility that the total wholesale cost of the credit monitoring could exceed $3.5 million (such as if more Class Members choose to enroll in the service than the $3.5 million wholesale payment can cover).

[8] Ten million dollars minus $3.5 million spent on credit monitoring services leaves $6.5 million, which when divided by $50 equals 130,000.

The amount available to fund Class Members' benefits, however, is not necessarily limited to $10 million. That is the minimum amount. The Qualified Settlement Fund begins at $32 million and subtracts the cost of administration, including notice (which is unknown at this time, but includes email service for much of the class), attorney's fees and expenses (which is unknown at this time, although the Settlement Agreement states that Plaintiffs' counsel will request fees and costs of up to $14 million), and Service Awards (which is unknown at this time, but Plaintiffs' counsel has indicated they will request up to $5,000 for each of the 20 Representative Plaintiffs, which totals $100,000). Thus, there is a reasonable possibility that the available amount to fund Class Members' benefits will be greater than $10 million, with funding for the cash reimbursement portion greater than $6.5 million, both because the $10 million figure might be higher and because the $3.5 million figure for credit monitoring and insurance might be lower. It is also difficult to assess Class Member individual benefits without knowing how many Class Members will return their Claim Forms and the type of claims (default recovery versus out-of-pocket reimbursement) that will be claimed. The fact that there is a guaranteed cash component, however, is of value to Class Members.

The credit monitoring and insurance benefit is an additional valuable benefit to Class Members. The ability to delay the start of these services increases its overall value, because Class Members may already have such monitoring provided because of another data breach or through purchasing on their own. Allowing Class Members to add this service two years after the Settlement, and after their current credit monitoring expires, provides added benefit.

Plaintiffs argue that the retail value of credit monitoring, and not the wholesale cost, should be considered as the value of the benefit provided to Class Members. The retail value of the plan being offered to the Settlement Class is $19.99 per month, which equals $479.79 for the two-year period. Plaintiffs argue that equals $50,854,560 for every one percent of the class that

enrolls in this benefit, before subtracting the cost of the credit monitoring. Because Plaintiffs have not provided the Court with the cost of the credit monitoring, the Court cannot at this juncture make this comparison with any precision. The Court accepts, however, that the benefit to Class Members is greater than the initial estimated $3.5 million wholesale cost that will come out of the Qualified Settlement Fund. This benefit, therefore, has a significant value to the Settlement Class.

Plaintiffs also did not provide a calculation of estimated total damages in their briefing on class certification or in their motion for preliminary approval. Plaintiffs' classwide damage theories were that Class Members could claim damages of either the value on the "black-market" of their Sensitive Information (for which Plaintiffs did not provide an estimated value) or the value of the difference between the health insurance premium they paid that was supposed to include robust data security and the value of the health insurance they actually received that allegedly did not include robust data security. The Court does not have specific estimated recovery numbers from which to reach a specific percentage of estimated recovery, but Plaintiffs' expert had used an example figure of $1,000 dollars, although not opining that was the value of Class Members' data. The Court considers the value to the Settlement Class looking at the Settlement as a whole and considering the risks and weakness of Plaintiffs' case and Plaintiffs' damages theories. The Court also considers the fact that this recovery was negotiated with significant assistance from outside mediators.

b. Non-monetary relief

Under the Settlement, Premera also will pay $42 million on improved data security between 2019 and 2022. Improved data security benefits all Class Members, even if they are no longer insured by Premera or a related Blue Cross entity, because Sensitive Information remains

stored on Premera's servers. If Premera has improved data security, it will decrease the chance of a future data breach and future harm to Class Members from such a breach.

Plaintiffs submit the expert witness declaration of Dr. Robert Vigil (ECF 274), in support of the estimated value of this non-monetary benefit to Class Members. Dr. Vigil used the Cost Approach, which is an accepted methodology to value certain types of intangible assets, including where cost information is known, the intangible asset is new, and the type of value being estimated is the value in continued use by the current owner. ECF 274 at ¶ 12. Dr. Vigil opines that the value to the Settlement Class of the increased data security Premera will implement is $11,872,000. Id. at ¶¶ 3, 23-25.

c. Conclusion

Although the cash recovery is a "mere fraction" of what Plaintiffs generally argued they could recover at trial, that does not require a finding that the recovery is not fair, reasonable, or adequate. See In re Mego, 213 F.3d at 459; *see also Linney v. Cellular Ala. P'ship*, 151 F.3d 1234, 1242 (9th Cir. 1998) (noting that "the very essence of settlement is . . . a yielding of absolutes and an abandoning of highest hopes" (citation and quotation marks omitted)). Considering the cash settlement, the value of the credit monitoring services, the additional non-monetary relief, the risks and weaknesses of Plaintiffs' case, and all of the other circumstances of this Settlement and how it was reached, the recovery is fair, reasonable, and adequate. This factor thus supports approval of the Settlement.

3. The extent of discovery completed and the stage of the proceedings

This factor is concerned with whether "the parties have sufficient information to make an informed decision about settlement." In Re Mego Fin. Corp., 213 F.3d 454, 459 (9th Cir. 2000) This case has been pending for four years. The parties have litigated two motions to dismiss, fully briefed and argued the motion for class certification and motions to exclude expert

testimony, and Premera filed a motion for partial summary judgment. The parties and their counsel have exchanged 1.5 million pages in document discovery, which they have extensively reviewed. The parties have also conducted more than 50 depositions, including those of eight experts, filed and argued numerous discovery motions, and Plaintiffs filed and argued a motion for sanctions for the spoliation of evidence, which the Court granted in part. Plaintiffs' counsel also retained four experts to measure damages, investigate the Data Breach, and conduct forensic analyses of Premera's computers and data systems. The parties "carefully investigated the claims before reaching a resolution." Ontiveros v. Zamora, 303 F.R.D. 356, 371 (E.D. Cal. Oct. 8, 2014). This factor, therefore, supports approval.

4. The experience and views of counsel

Lead Plaintiffs' Counsel and Liaison Plaintiffs' Counsel are experienced class action litigators. Premera is also represented by experienced counsel. This factor supports approval.

5. The reaction of the class

Because there has not yet been notice or a response to the Settlement, this factor is not applicable at this stage of the Court's review.

6. The absence of collusion or other conflicts of interest

The Court finds that the Settlement is the product of extensive arm's-length negotiations, with assistance from experienced mediators Judge Gandhi and Mr. Rosen in multiple mediation sessions. There is no evidence of collusion or any other conflict of interest. Premera has and continues to dispute the claims against it and the Action was litigated for nearly four years before the parties reached their proposed Settlement Agreement.

Moreover, none of the three "subtle" signs of collusion are present here. The Settlement Class is to receive significant monetary and non-monetary benefits that are not

disproportionately low compared to the requested attorney's fee award, the payment of attorney's fees is not separate from class funds, and the Settlement Fund is non-reversionary.

7. Conclusion

After considering the relevant factors and circumstances, the Court finds that the Settlement is fair, reasonable, and adequate to the Settlement Class, and that each Class Member (except those who submit a timely and valid request for exclusion) shall be bound by the Settlement. The persons who timely request exclusion from the Settlement Class will not be members of the Settlement Class, shall have no rights or interests with respect to the Settlement, and shall not be bound by any orders or judgments entered in respect to the Settlement.

C. Order Establishing Notice and Other Settlement Procedures

The Court has read and considered the Settlement Agreement, the proposed Notice of Premera Blue Cross Security Incident Settlement ("Long Form Notice"), the proposed Summary Notice, the proposed Publication Notice, and the proposed Claim Form for Premera Blue Cross Security Incident Benefits ("Claim Form"), and finds that substantial and sufficient grounds exist to grant preliminary approval of the Settlement.

Accordingly, IT IS HEREBY ORDERED:

1. Defined Terms. Unless otherwise defined, all capitalized terms herein have the same meanings as set forth in the Settlement Agreement;

2. Stay of the Action. Pending the Final Fairness Hearing, all proceedings in the Action, other than proceedings necessary to carry out or enforce the terms and conditions of the Settlement Agreement and this Opinion and Order, are hereby stayed.

3. Provisional Class Certification for Settlement Purposes Only. For purposes of the Settlement only, the Court finds and determines that the Action may proceed as a class action under Rule 23(b)(3) of the Federal Rules of Civil Procedure, and that: (a) the Class certified

herein numbers more than 10.6 million people and joinder of all such persons would be impracticable, (b) there are questions of law and fact that are common to the Class and those questions of law and fact common to the Class predominate over any questions affecting any individual Class Member; (c) the claims of the Plaintiffs are typical of the claims of the Class they seek to represent for purposes of settlement; (d) a class action on behalf of the Class is superior to other available means of adjudicating this dispute; and (e) as identified below, the Representative Plaintiffs and Class Counsel are adequate representatives of the Class. Premera retains all rights to assert that this action may not be certified as a class action, other than for settlement purposes.

4. Class Definition. The Court hereby certifies, for settlement purposes only, a Settlement Class consisting of: all persons in the United States whose Personal Information was stored on Premera's computer network systems that was compromised in the Security Incident as publicly disclosed on March 17, 2015. Excluded from the Settlement Class are: (1) the Judge presiding over the Action, and members of his family; (2) Premera, its subsidiaries, parent companies, successors, predecessors, and any entity in which Premera or its parents have a controlling interest and their current or former officers and directors; (3) Persons who properly execute and submit a request for exclusion prior to the expiration of the Opt-Out Period; and (4) the successors or assigns of any such excluded Persons.

5. Representative Plaintiffs. For purposes of the Settlement only, the Court finds and determines, pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, the Representative Plaintiffs[9] will fairly and adequately represent the interests of the Class in enforcing their rights

[9] The Representative Plaintiffs consist of Elizabeth Black, Catherine Bushman, Krishnendu Chakraborty, Maduhchanda Chakraborty, Ralph Christopherson, Anne Emerson,

in the Action and appoints them as Representative Plaintiffs. The Court preliminarily finds that they are similarly situated to absent Class Members and have Article III standing to pursue their claims, and are therefore typical of the Class, and that they will be adequate class representatives.

6. Class Counsel. For purposes of the Settlement, the Court appoints Kim D. Stephens of Tousley Brain Stephens PLLC; James Pizzirusso of Hausfeld LLP; Tina Wolfson of Ahdoot & Wolfson, PC; Karen Hanson Riebel of Lockridge Grindal & Nauen PLLP; and Keith Dubanevich of Stoll Berne as Class Counsel to act on behalf of the Class and the Representative Plaintiffs with respect to the Settlement. The Court authorizes Class Counsel to enter into the Settlement on behalf of the Class Representatives and the Class, and to bind them all to the duties and obligations contained therein, subject to final approval of the Settlement by the Court.

7. Administration. The firm of Epiq is appointed as Settlement Administrator to administer the notice procedure and the processing of claims, under the supervision of Class Counsel.

8. Class Notice. The form and content of the proposed Summary Notice, Long Form Notice, Publication Notice, and Claim Form, submitted by the Settling Parties as Exhibits B, C, D, and E, respectively, to the Settlement Agreement, are hereby approved. Before the dissemination of Class Notice, the Settlement Administrator shall establish a dedicated Settlement Website and shall maintain and update the website through the Claims Period ("Settlement Website"). The Settlement Website shall include, and make available for download, copies of the Settlement Agreement, Long Form Notice, Summary Notice, and Claim Form, in forms available for download.

William Fitch, Eric Forsetter, Mary Fuerst, Debbie Hansen-Bosse, Stuart Hirsch, Ilene Hirsh, Howard Kaplowitz, Barbara Lynch, and Kevin Smith.

9. Notice Date. The Court directs that the Settlement Administrator cause a copy of the Publication Notice to be published in a manner to be agreed upon by the parties. This publication shall be done as soon as practicable, but not later than August 29, 2019. The Court also directs the Settlement Administrator to cause a copy of the Summary Notice to be mailed and emailed to all members of the Class who have been identified by Premera through its records and who are included in the Class Member List, which Premera is to provide to the Settlement Administrator on or before August 29, 2019. The mailing is to be made by first class United States mail and by email for Class Members for whom Premera has an existing email address, from between September 13, 2019 and November 13, 2019. The "Notice Date" under the Settlement Agreement shall be October 29, 2019, 60 days from the Publication Notice deadline.

10. Findings Concerning Notice. The Court finds and determines that: (a) publishing the Publication Notice; (b) mailing and emailing the Summary Notice; (c) sending reminder emails to Settlement Class Members (if possible); and (d) publishing the Settlement Agreement, Long Form Notice, Summary Notice, and Claim Form on the Settlement Website, all pursuant to this Opinion and Order, constitute the best notice practicable under the circumstances, constitute due and sufficient notice of the matters set forth in the notices to all persons entitled to receive such notices, and fully satisfies the requirements of due process, Rule 23 of the Federal Rules of Civil Procedure, 28 U.S.C. § 1715, and all other applicable laws and rules. The Court further finds that all of the notices are written in simple terminology, and are readily understandable by Class Members. The Court also appoints Cameron Azari as Notice Specialist.

11. Proof of Notice. On or before December 30, 2019, Plaintiffs shall cause to be filed with the Court Proof of Notice, in compliance with ¶ 6.2.12 of the Settlement Agreement.

12. Deadline to Submit Claim Forms. Class Members will have until March 30, 2020 (150 days from the Notice Date) to submit their Claim Forms ("Claims Deadline"), which is due, adequate, and sufficient time.

13. Exclusion from Class. Any person falling within the definition of the Class may, upon request, be excluded or "opt out" from the Class. Any such person who desires to request exclusion from the Class must submit a fully-completed Request for Exclusion. To be valid, the Request for Exclusion must be (i) submitted electronically on the Settlement Website, or (ii) postmarked or received by the Settlement Administrator on or before the end of the Opt-Out Period, which shall expire January 29, 2020. In the event the Settlement Class Members submit a Request for Exclusion to the Settlement Administrator by U.S. Mail, such Request for Exclusion must be in writing and must identify the case name *In re Premera Blue Cross Customer Data Security Breach Litigation*, Case No. 3:15-md-2633-SI; state the name, address and telephone number of the Settlement Class Members seeking exclusion; be physically signed by the Person(s) seeking exclusion; and must also contain a statement to the effect that "I/We hereby request to be excluded from the proposed Settlement Class in *In re Premera Blue Cross Customer Data Security Breach Litigation*, Case No. 3:15-md-2633-SI." All persons and entities who submit valid and timely Requests for Exclusion as set forth in this Opinion and Order and the Notice shall have no rights under the Settlement, shall not share in the distribution of the Settlement Fund, and shall not be bound by the Settlement or any final judgment entered in this Action.

14. Final Fairness Hearing. The Final Fairness Hearing will be held before the Honorable Michael H. Simon, United States District Judge for the District Oregon, Mark O. Hatfield United States Courthouse, 1000 SW Third Avenue Portland, Oregon, 97204 at 11:00 a.m. on Monday, March 2, 2020, in Courtroom 15B, to determine: (a) whether the Settlement

should be approved as fair, reasonable, and adequate to the Class; (b) whether a Final Approval Order and Judgment should be entered in this case; (c) whether the Representative Plaintiffs' proposed Settlement Benefits as described in Section IV of the Settlement Agreement should be approved as fair, reasonable, and adequate to the Class; (d) whether to approve the application for Service Awards for the Representative Plaintiffs or an award of attorneys' fees and litigation expenses to Plaintiffs' counsel; and (e) any other matters that may properly be brought before the Court in connection with the Settlement. The Final Fairness Hearing is subject to continuation or adjournment by the Court without further notice to the Class. The Court may approve the Settlement with such modifications as the Settling Parties may agree to, if appropriate, without further notice to the Class.

15. Objections and Appearances. Any Class Member may enter an appearance in the Action, at his or her own expense, individually or through counsel. If a Class Member does not enter an appearance, they will be represented by Class Counsel. Any Class Member who wishes to object to the Settlement, the Settlement Benefits, Service Awards, and/or the Attorney's Fee Award and Costs, or to appear at the Final Fairness Hearing and show cause, if any, why the Settlement should not be approved as fair, reasonable, and adequate to the Class, why a final judgment should not be entered thereon, why the Settlement Benefits should not be approved, or why the Service Awards and/or the Attorney's Fee Award and Costs should not be granted, may do so, but must proceed as set forth in this paragraph. No Class Member or other person will be heard on such matters unless they have filed in this Action the objection, together with any briefs, papers, statements, or other materials the Class Member or other person wishes the Court to consider, on or before January 29, 2020. Any objection must include: (i) the Settlement Class Member's full name, current mailing address, and telephone number; (ii) a signed statement that he or she believes himself or herself to be a member of the Settlement Class; (iii) the specific

grounds for the objection; (iv) all documents or writings that the Settlement Class Member desires the Court to consider; and (v) a statement regarding whether they (or counsel of their choosing) intend to appear at the Final Fairness Hearing. Any Class Member who does not make their objections in the manner and by the date set forth in this paragraph shall be deemed to have waived any objections and shall be forever barred from raising such objections in this or any other action or proceeding, absent further order of the Court.

16. Claimants. Class Members who have been identified from Premera's records and who submit by the Claims Deadline a valid Claim Form approved by the Settlement Administrator may qualify to receive Credit Monitoring and Insurance Services, cash payments for Out-of-Pocket Losses or the Default Settlement Payment, and a California Payment. Any such Class Member who does not submit a timely Claim Form in accordance with this Opinion and Order shall not be entitled to receive Credit Monitoring and Insurance Services, cash payments for Out-of-Pocket Losses or the Default Settlement Payment, and a California Payment, but shall nevertheless be bound by any final judgment entered by the Court. Class Counsel shall have the discretion, but not the obligation, to accept late-submitted claims for processing by the Settlement Administrator, so long as distribution of the Net Qualified Settlement Fund to Claimants is not materially delayed thereby. No person shall have any claim against Class Counsel or the Settlement Administrator by reason of the decision to exercise discretion whether to accept late-submitted claims.

17. Release. Upon the entry of the Court's order for final judgment after the Final Fairness Hearing, the Representative Plaintiffs and all Class Members except those who have timely filed an opt-out form pursuant to this Opinion and Order, whether or not they have filed a Claim Form within the time provided, shall be permanently enjoined and barred from asserting any claims (except through the Claim Form procedures) against Premera and the Released

Persons arising from the Released Claims, and the Representative Plaintiffs and all such Class Members conclusively shall be deemed to have fully, finally, and forever released any and all such Released Claims.

18. Funds Held by Settlement Administrator. All funds held by the Settlement Administrator shall be deemed and considered to be in custodia legis of the Court and shall remain subject to the jurisdiction of the Court until such time as the funds are distributed pursuant to the Settlement or further order of the Court.

19. Final Approval Briefing. All opening briefs and supporting documents in support of a request for final approval of the Settlement, the Settlement Benefits, the Service Award, and a motion for Attorney's Fees and Costs must be filed and served on or before January 10, 2020, and must be posted on the Settlement Website. Reply briefs in support of the request for final approval of the Settlement, the Settlement Benefits, the Service Award, and the Attorney's Fees and Costs, and responses to any objections, must be filed and served on or before February 19, 2020.

20. Reasonable Procedures. Class Counsel and Defense Counsel are hereby authorized to use all reasonable procedures in connection with approval and administration of the Settlement that are not materially inconsistent with this Opinion and Order or the Settlement Agreement, including making, without further approval of the Court, non-substantive changes to the form or content of the Long Form Notice, Summary Notice, and other exhibits that they jointly agree are reasonable or necessary, as long as those changes do not make Class Members' rights to object to the Settlement, Attorney's Fees and Costs, or Service Award less noticeable.

21. Extension of Deadlines. Upon application of the Parties and good cause shown, the deadlines set forth in this Opinion and Order may be extended by order of the Court, without further notice to the Class. Class Members must check the Settlement Website regularly for

updates and further details regarding extensions of these deadlines. The Court reserves the right to adjourn or continue the Final Fairness Hearing, or to extend the deadlines set forth in this Opinion and Order, without further notice of any kind to the Class.

22. If Effective Date Does Not Occur. In the event that the Effective Date does not occur, certification shall be automatically vacated and this Preliminary Approval, and all other orders entered and releases delivered in connection herewith, shall be vacated and shall become null and void.

CONCLUSION

Plaintiffs' Unopposed Motion for Preliminary Approval of Proposed Settlement Agreement (ECF 273) is GRANTED. The Court directs the Clerk of the Court to send a copy of this Opinion and Order to the Clerk of the Judicial Panel on Multidistrict Litigation.

IT IS SO ORDERED.

DATED this 29th day of July, 2019.

/s/ Michael H. Simon
Michael H. Simon
United States District Judge