Kim D. Stephens, OSB# 030635
kstephens@tousley.com
Christopher I. Brain
cbrain@tousley.com
Jason T. Dennett
jdennett@tousley.com
Tousley Brain Stephens PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992

Interim Lead Plaintiffs' Counsel

Keith S. Dubanevich
kdubanevich@stollberne.com
Steve D. Larson
slarson@stollberne.com
Yoona Park
ypark@stollberne.com
Stoll Berne
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840

Interim Liaison Plaintiffs' Counsel

[Additional counsel appear on the signature page.]

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.	**PLAINTIFFS' MOTION FOR SANCTIONS FOR DEFENDANT'S DISCOVERY MISCONDUCT** Request for Oral Argument

LR 7-1 CERTIFICATION

Counsel for Plaintiffs hereby certifies that the parties have conferred in good faith regarding the subject matter of this motion and have been unable to reach a resolution.

MOTION

Pursuant to the Court's inherent discretionary power, Plaintiffs move for sanctions against Defendant Premera for discovery misconduct. By willfully destroying: (a) a computer that the hackers used in the data breach and which may have held evidence of data exfiltration; and (b) data loss prevention software logs that may have shown evidence of data exfiltration, Premera spoliated key evidence and prejudiced Plaintiffs' ability to achieve a rightful decision in this case. Consequently, Plaintiffs move this Court for sanctions in the form of:

1. An adverse jury instruction at trial stating that given the spoliation, the jury is to presume that exfiltration occurred;

2. An order preventing Mandiant,[1] or any other expert relying on Mandiant's investigation, from offering an expert opinion that it found no evidence of data exfiltration; and

3. An Order prohibiting Premera from introducing any evidence regarding the spoliated evidence.

MEMORANDUM

I. INTRODUCTION

Since before this case was filed, Premera has claimed that no evidence exists that the hackers removed or "exfiltrated" any of Plaintiffs' data from Premera's systems. *See, e.g.*, ECF No. 60 at 54:20-56:2 ("The notice that was sent to affected persons says very specifically that

[1] Mandiant is a third party information technology consultant that Premera hired to investigate the data breach.

there is no evidence that any information was taken out of the systems."). Essentially, Premera maintains a "no harm, no foul" defense, contending there can be no damage to any Plaintiff unless he or she can prove confidential information was exfiltrated from Premera's system. *Id.* Plaintiffs dispute Premera's theory, and allege that harm was done to every member of the Class when their sensitive information was exposed to an unauthorized third party—namely, the hackers. At trial, Plaintiffs intend to offer direct and circumstantial evidence of exfiltration.

Plaintiffs sought evidence of exfiltration through various discovery methods. In particular, Plaintiffs asked Premera for two categories of evidence: (1) files contained on the hard drives of computers compromised by the hackers; and (2) log files from Premera's various types of data security software—both of which can show evidence of exfiltration and both of which Premera destroyed well after Plaintiffs filed their complaints.

II. FACTS

A. Plaintiffs sought evidence that was left behind on the 35 computers the hackers compromised, but Premera's 2016 destruction of an important computer thwarted that effort.

1. Computer hard drives can contain evidence of exfiltration.

One of the ways to look for evidence of exfiltration is by examining the files left behind on the affected computers to see if the hackers left any clues. Declaration of Matthew Strebe ("Strebe Decl.") ECF No. 166 at ¶ 73. To look for such files, one needs either the computer's original hard drive or a copy of all the data on that drive, which is called a forensic image. *Id.* From the hard drive or its forensic image, a forensic expert can examine file remnants, logs, or other indicators to determine where the hackers went, when they went there, and what they did. Strebe Decl. at ¶¶ 73-79; 225-229.

Mandiant identified 35 computers affected by the breach. *See* Declaration of Jason T.

Dennett ("Dennett Decl.")[2] Ex. 1 at 49 , June 26, 2015 Mandiant Intrusion Investigation Report ("Mandiant Report"). Premera's data breach expert Mandiant examined the files within the 35 computers compromised by the hackers soon after it discovered the breach in January 2015, and rendered conclusions about exfiltration based on the data contained therein. Ex. 1. On November 8, 2017, Plaintiffs served a request for inspection on Premera asking for forensic images of all 35 of the affected computers for the purpose of conducting their own forensic examination of the breach. Ex. 2. Premera responded that it could only produce images for 34 of those 35 computers; the 35th computer had been destroyed.

2. Mandiant found unusual activity, but reached conflicting conclusions.

During its forensic investigation, Mandiant found evidence of unusual .RAR[3] files. Ex. 1 at 49. Initially, Mandiant's investigators told Premera that the .RAR files were evidence of exfiltration. *See* Ex. 3, February 5, 2015 Mandiant Status Report from Mr. Foscue to Premera ("Began sweeping servers for evidence of large file archives (.RAR), which could indicate data staging and theft.") and Ex. 4, March 3, 2015 Mandiant Status Report from Mr. Foscue to Premera ("I have some unfortunate news for you . . . searches . . . identified [.RAR] files . . . . I believe this new evidence suggests that the files were more than likely created by the attacker."). But later, after Baker Hostetler took over all of Premera's communication with Mandiant, Mandiant changed its story. *See* Ex. 1 at 49, June 26, 2015 Mandiant Report, also written by Mr. Foscue ("Mandiant did not identify attacker access to sensitive or protected information . . . Mandiant and Premera could not determine the nature or contents of the [.RAR] files nor determine whether they were created by the attacker or Premera employees."). Plaintiffs sought

[2] Except where noted, all exhibits cited are attached to the Dennett Decl.

[3] A .RAR file is a piece of software designed to compress files and commonly used by hackers to extract data from their targets. Strebe Decl. at ¶ 76.

to conduct the same type of forensic examination done by Mandiant to test Mandiant's opinions on which Premera intends to rely.

3. A23567-D showed indications of heavy hacker activity.

The 35th computer, called A23567-D, was a "developer" computer—loaded with robust software and afforded security clearance to Premera's most sensitive databases. Ex. 7. Mandiant found that A23567-D contained a unique piece of hacker-created malware that Mandiant called PHOTO. Ex. 3, February 5, 2015 Mandiant Status Report from Mr. Gowan to Premera. Mandiant found PHOTO only on A23567-D. Ex. 1. PHOTO malware had the capability to upload and download files, and to exfiltrate data. Ex. 5 at PBC00264273 ("The malware has the ability to manipulate files, processes, the registry, and services and can also upload and download files and execute programs."). Hackers accessed PHOTO on A23567-D between May 12, 2014 and February 2015. Ex. 8.

The hackers configured PHOTO on A23567-D to communicate with an outside website named "www[.]presecoust[.]com." Ex. 3 at PBC_TAR00845898. Mandiant's analysis of proxy logs[4] found hundreds of thousands of almost daily contacts between A23567-D, the only Premera computer containing PHOTO, and www.presecoust.com between July 23, 2014 and January 9, 2015. Dennett Decl at ¶ Ex. 9, FIREEYE003181. Only A23567-D's destroyed hard drive could show what the hackers left behind during those contacts.

4. Premera destroyed the 35th computer after Plaintiffs filed their complaints.

Plaintiffs requested an image of A23567-D for purposes of conducting their own forensic investigation of the hacker activity. In its discovery responses, Premera confirmed that it destroyed this computer *after* the filing of the complaints in this case:

[4] Premera's proxy logs recorded the requests made by outside users to access Premera's network.

> In early February 2015, Mandiant identified A23567-D as a compromised asset. Mandiant noted that A23567-D seemed to contain files related to PHOTO Malware, and at that time recommended that Premera keep A23567-D *in situ*, ostensibly as part of Premera's plan to avoid alerting any potential intruders on Premera's network that Premera was in the process of investigating and remediating its IT network.
>
> On March 4, 2015, likely as part of its Remediation Weekend strategy, Premera issued a COSMOS ticket for the collection of A23567-D . . .
>
> While the other 34 systems identified by Mandiant were sent to sequestration together, A23567-D was instead unintentionally filed, as End of Life ("EoL") already-configured equipment, with Premera's Client Technology Services ("CTS") facility, where it remained, offline and unused, for more than a year. On September 28, 2016, that facility then separately identified it as a device that no longer served a Premera purpose; it was sent to Premera's Personal Computer Distribution Center ("PCDC") on September 29, 2016 and was listed as destroyed on December 16, 2016.

Ex. 7, Premera's Response to Plaintiffs' Interrogatory 14.

The destroyed computer was perfectly positioned to be the one-and-only staging computer hackers needed to create vast staging files for the purpose of shipping even more data outside of Premera's network. This computer functioned as the development machine for a software programmer, and as such was pre-loaded with a vast array of legitimate utilities that could be turned to any purpose. Strebe. Decl. ¶¶ 44, 225-227. Only A23567-D itself, or a forensic image of it,[5] would contain the files left behind by the hackers showing their activity. *Id.* ¶¶ 73-74, 225-229. Any files or remnants the hackers left on A23567-D during those contacts are now permanently lost, along with Plaintiffs' chance to show evidence of exfiltration though

[5] Premera created forensic images of at least 10 of the 35 computers, preserving their contents for Mandiant's use in its investigation of the breach. Ex. 6, Gowan Deposition Transcript at 152:24-155:9. Mandiant also had the ability and option to create a digital image of each computer on which it looked for clues of exfiltration. Ex. 10, 30(b)(6) Deposition of FireEye, Inc. at 185:4-186:22; 270:2-17. Both deliberately chose not to preserve the contents of A23567-D with a forensic image at the time of Mandiant's investigation in 2015. Ex. 11, May 28, 2018 email from Premera's counsel.

the logs stored on the device. While Mandiant had a chance to analyze its contents and draw conclusions from that data, Plaintiffs will not be able to do so, and have been deprived of the ability to review and rebut Mandiant's conclusions based on that data. Without access to that hard drive, trying to prove that the hackers removed Plaintiffs PII and PHI through that computer is impossible. *Id.* ¶ 229.

B. Premera destroyed the logs from its data loss prevention software.

Premera used a data loss prevention ("DLP") software called Bluecoat or Vontu as part of its IT security system. Ex. 12, Vergeront Deposition Transcript at 88:17-89:20. DLP software monitors certain types of data traffic in and out of a network, and can be programmed to alert if someone within Premera's network attempts to transmit sensitive information, including customers' personal information, outside of the network. *Id*. at 115:15-116:24. Premera's DLP created logs of the activity it observed. *Id.* at 129:7-130:5.

These DLP logs contain critical evidence necessary for a full assessment of the hacker's activity. The logs can show exfiltration because they capture evidence of customers' information leaving Premera's system. *Id*. at 88:3-89:5, 90:4-14. While Premera produced various log files, those logs contained very little information from the DLP system during the time of the breach. Strebe Decl. ¶ 160. In response to a formal discovery request for all DLP logs from January 1, 2014 through December 31, 2015, Premera admitted that (1) it no longer has DLP logs from that period, (2) the logs from that period existed until June or July of 2015, and (3) Premera failed to preserve DLP logs after Plaintiffs filed their complaints. Ex. 13 (Premera's Response to Plaintiffs' Request for Production No. 268).[6]

[6] Premera's offer of a forensic image of one of two servers containing 2014-2015 DLP log data (the other was destroyed) that "may contain remainder data predating the server's commission

Premera knew its DLP logs were relevant to the data breach. Premera's Deputy General Counsel, Kitti Cramer, included an analysis of DLP logs data from 2014 in a March 4, 2015[7] memorandum to the boards of directors of its affiliates about Premera's privacy program. Ex. 14 at PBC_TAR00034590. Premera touted that its DLP software blocked malware at the web gateway and explained how the security team investigated 2,960 DLP alerts Q3 2014, at which time the hackers had unfettered and undetected access to Premera's network. *Id.* No other source of data will show what a DLP log would: hackers transferring customers' personal information out of Premera's network. Ex. 12 at 88:3-89:5, 90:4-14, 115:15-116:24, 129:7-130:5 (Vergeront Dep. Tr.).

III. LEGAL STANDARDS

As part of its inherent power "to make discovery and evidentiary rulings conducive to the conduct of a fair and orderly trial," a district court has the discretion to impose sanctions to address the harm resulting from a party's destruction of evidence. *PacificCorp v. Nw. Pipeline GP*, 879 F. Supp. 2d 1171, 1187-88 (D. Or. 2012); *Glover v. BIC Corp.*, 6 F.3d 1318, 1328 (9th Cir. 1993). Sanctions are appropriate if the party destroying evidence knew or had notice that "the evidence in dispute was 'potentially relevant' to probable litigation" and the moving party was prejudiced by the destroying party's conduct. *U.S. ex rel. Berglund v. Boeing Co.*, 835 F. Supp. 2d 1020, 1051 (D. Or. 2011). Sanctions for spoliation may include "dismissal of claims, exclusion of evidence, and adverse jury instructions permitting a jury to draw an inference that the destroyed evidence would have been adverse to the party responsible for its destruction." *PacificCorp*, 879 F. Supp. 2d at 1187-88.

---

within the server's unallocated or slack space" is no substitute for a complete log set. *Id.*

[7] Premera discovered the data breach in January 2015. Ex. 1 at PBC00023944.

IV. ARGUMENT

Premera destroyed both computer A23567-D and its DLP logs after Premera knew or should have known of their relevance to probable or pending litigation. Sanctions are warranted as this destruction has harmed Plaintiffs' ability to analyze these relevant, critical pieces of evidence.

A. Premera's destruction of A23567-D and DLP logs was willful.

To merit sanctions, regardless of the type of sanction levied, a court must find that the evidence was destroyed "willfully." *PacificCorp*, 879 F. Supp. 2d at 1188 (citing *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982 F.2d 363, 368 (9th Cir. 1992)). Destruction is "willful" if, at the time of destruction, the destroying party had some notice that the evidence was "potentially relevant to the litigation." *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 959 (9th Cir. 2006).

Here, Premera acted willfully because at the time that Premera destroyed A23567-D and its DLP logs, it knew that this evidence was critically relevant[8] to the litigation. Premera knew that A23567-D was one a few machines the hackers used during the breach, and for that reason, Premera was aware that the computer contained data relevant to exfiltration.[9] And because DLP is designed to log sensitive information leaving Premera's system, DLP logs were critically relevant to exfiltration and Premera's data security, as shown by Ms. Kramer's inclusion of DLP

[8] Having destroyed the evidence, Premera cannot now argue that there is no prejudice to Plaintiffs because any destroyed information was irrelevant to this case. "A party cannot rely on a 'presumption of irrelevance' to defeat a motion for sanctions on the basis of spoliation because 'the relevance of destroyed documents cannot be clearly ascertained.'" *Grove City Veterinary Service, LLC v. Charter Practices Int'l, LLC*, No. 3:13–cv–02276–AC, 2015 WL 4937393 at *3 (D. Or. Aug. 18, 2015) (citing *Leon*, 464 F.3d at 959).

[9] Mandiant identified A23567-D as one of the computers accessed and used by the hackers prior to Premera destroying it. Ex. 1 at 49.

log results in her board presentation. Ex. 12. Premera destroyed both of these pieces of evidence *after* the filing of this lawsuit. There can be no serious argument that Premera was unaware that the computer and logs contained evidence that was crucial to this case.

B. Premera's spoliation of key evidence has prejudiced Plaintiffs.

In assessing prejudice, the Court must determine whether Premera's actions have impaired Plaintiffs' ability to "go to trial, threatened to interfere with the rightful decision of the case, or forced the non-spoiling party to rely on incomplete and spotty evidence." *Berglund*, 835 F. Supp. 2d at 1051 (citing *Leon*, 464 F.3d at 959). Premera destroyed key evidence that could show exfiltration and yet intends to argue that Plaintiffs cannot show exfiltration of data. Premera cannot be allowed to destroy evidence and point to its absence as a defense; such a defense would be highly misleading and unfairly prejudicial. While secondary evidence can reduce prejudice caused by the destruction of evidence, the prejudice to Plaintiffs is not mitigated by the existence of other sources of evidence relating to exfiltration. *See PacifiCorp*, 879 F. Supp. 2d at 1190. No other evidence can show what files the hackers may have left behind on A23567-D. Strebe Decl. ¶¶ 73-74, 225-229. No other evidence can show transfers of customers' personal information logged by Premera's DLP software. Ex. 9 at 88:3-89:5, 90:4-14, 115:15-116:24, 129:7-130:5 (Vergeront Dep. Tr.).

Even assuming that Premera or Mandiant witnesses exist who could testify about the specific contents of A23567-D and the DLP logs, such deposition testimony is an inadequate substitute for an expert's direct examination. *See PacifiCorp*, 879 F.Supp.2d at 1193 (photographs of damaged machine and destroying party's consultant's analysis of damaged machine "hardly an adequate substitute for the thing itself"). Consequently, Plaintiffs' ability to present its case at trial and to achieve a rightful outcome have been critically impaired by the

destruction of the evidence, and Premera should be sanctioned.

C. An adverse jury instruction is an appropriate sanction for Premera's destruction of evidence related to facts that Plaintiffs want to present to the jury.

In deciding on the appropriate sanction, courts generally weigh three factors: "1) the degree of fault of the party who altered or destroyed the evidence; 2) the degree of prejudice suffered by the opposing party; and 3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party." *Dallas Buyers Club, LLC v. Huszar*, No. 3:15–cv–907–AC, 2017 WL 481469, at *2 (D. Or. Feb. 6, 2017) (citing *Nursing Home Pension Fund v. Oracle Corp.*, 254 F.R.D. 559, 563 (N.D. Cal. 2008)) (additional internal citations omitted).

Plaintiffs request an adverse jury instruction establishing a rebuttable presumption that the destroyed computer and DLP logs contained evidence that Plaintiffs' sensitive data had been exfiltrated by the hackers. A trial court has the "broad discretionary power to permit a jury to draw an adverse inference from the destruction or spoliation against the party or witness responsible for that behavior." *Glover*, 6 F.3d at 1329. Although a showing of bad faith is required for dispositive sanctions, bad faith on the part of the destroying party is not a prerequisite for an adverse jury instruction sanction, and a simple showing of willfulness will suffice. *See id.* (citing *Akiona v. United States*, 938 F.2d 158 (9th Cir. 1991)).

Judge Papak issued an adverse inference sanction in a similar situation in the *PacifiCorp* case. There PacificCorp claimed that oil leaking from defendant GTN's compressor damaged its fuel nozzles, causing power plant outages on which PacificCorp based its damages. PacificCorp preserved only 11 of the 350 nozzles. *PacificCorp*, 879 F. Supp. 2d at 1191. While the 350 nozzles were damaged during three different outage events in July, August, and September of 2007, the 11 preserved nozzles related only to the July outage. *Id.* PacificCorp provided the remaining nozzles to its expert Dr. Kemal to determine whether GTN's leak caused the damage

to the nozzles and therefore the three outages. *Id.* Dr. Kemal concluded based on his inspection of the July nozzles that oil leaks caused all three outages. *Id.* In addition to imposing sanctions barring expert testimony (discussed below), because the despoiled nozzles could not be inspected, the Court also imposed a sanction of an "adverse inference instruction establishing a rebuttable presumption" that the refurbished fuel nozzles did not exhibit signs of compressor oil contamination, a key element of Plaintiff's case. *Id.* at 1194-95.

Here, regardless of whether such actions were made in bad faith, Premera isolated and destroyed a piece of hardware that contained evidence of probable relevance to this case. As in *PacificCorp*, a lesser sanction will not resolve the prejudice to Plaintiffs resulting from loss of the spoliated evidence, as there is no other discovery that can replace an expert's direct inspection of the information that was stored and potentially removed from the spoliated computer. Consequently, an adverse jury instruction establishing a rebuttable presumption that A23567-D and the DLP logs contained evidence that Plaintiffs' sensitive data had been exfiltrated by the hackers is the appropriate sanction. *See Dallas Buyers Club*, 2017 WL 4814469, at *4 (ordering adverse inference instruction where the defendant failed to preserve computer hard drives that may have contained relevant evidence).

D. Exclusion of Premera's expert's opinion on exfiltration is an appropriate sanction.

Plaintiffs expect that in support of its "no harm, no foul" defense, Premera will offer expert testimony from Mandiant (or some other expert repeating Mandiant's conclusion) that it found no evidence of exfiltration. That conclusion rests on Mandiant's investigation of each of the 35 computers, including A23567-D, which contained a large volume of hacker activity, and which Premera has now destroyed. Premera should not be permitted to offer expert testimony about whether it found evidence of exfiltration, while willfully depriving Plaintiffs and their

expert of the opportunity to perform the same analysis. Excluding such testimony is within this Court's inherent power.

Once again, a similar sanction was issued in the *PacifiCorp* case. In addition to an adverse inference sanction, Judge Papak also excluded expert testimony. PacificCorp's expert Dr. Kemal reviewed the 11 remaining nozzles from July and concluded that oil leaks caused all three outages in July, August, and September. *Id.* As a sanction for destruction of the remaining 339 nozzles, the court excluded Dr. Kemal's testimony about causation of the August and September outages:

> Because the despoiled fuel nozzles are at the heart of this case and absolutely no physical evidence remains of the parts damaged in the August and September 2007, the most appropriate sanction is exclusion of all expert testimony concerning those damaged parts and whether compressor oil caused their damage. . . . This includes Dr. Kemal's testimony concerning causation of the August and September outages, plus any other expert's testimony relying on those conclusions. The Ninth Circuit has affirmed imposition of a somewhat similar sanction in *Unigard*, where the district court excluded testimony of an expert about the cause of damages where plaintiff destroyed the instrumentality allegedly causing its damages, reasoning that plaintiff's introduction of the expert testimony would unfairly prejudice defendant and preclude a fair trial.

Id. at 1193-94 (citing *In re Napster, Inc. Copyright Litig*., 462 F.Supp. 2d 1060, 1068 (N.D. Cal. 2006) and *Unigard*, 982 F.2d at 368).

Similarly, although 34 of the 35 computers still exist, and Plaintiffs' expert was able to examine them, A23567-D is unique. Not only is its hard drive the only place to discover any evidence that the hackers may have left there, A23567-D was the only one of the 35 computers on which the hackers installed exfiltration-capable PHOTO malware. "Destruction that precludes a party from inspecting physical evidence can create prejudice . . . . Similarly, forcing a party to rely on evidence selected by an opposing party's expert creates prejudice, because such evidence generally supports that party's case." *Id.* at 1190. Plaintiffs are prejudiced if forced to rely on Mandiant's analysis of A23567-D.

As the *PacificCorp* court recognized, the existence of the other 34 computers does not mitigate the destruction of A23567-D because it deprives Plaintiffs of the ability to conduct its own investigation and investigate the plausibility of other causation conclusions. *Id.* at 1193 ("[T]he prejudice from PacifiCorp's conduct is overwhelming. . . . PacifiCorp's refurbishment prevents GTN's experts from examining any damaged turbine nozzles . . . to investigate the plausibility of alternate causes of damages besides oil contamination—causes such as design defects, plant operation error, or other mechanical error that defense experts raise.").

Moreover, allowing Premera to support its "no harm, no foul" defense with Mandiant's conclusion that it found no evidence of exfiltration would quickly render useless the adverse inference requested above. In *UniGard*, the Ninth Circuit upheld the district court's exclusion of expert testimony because a rebuttable presumption was insufficient to cure the prejudice of destruction of evidence. 982 F.2d at 369 (citing *Fire Ins. Exch. v. Zenith Radio Corp*., 103 Nev. 648, 747 P.2d 911, 914 (1987) (exclusion of expert testimony for plaintiff's destruction of evidence, rather than imposition of a rebuttable presumption, was not an abuse of discretion because "[a]ny adverse presumption which the court might have ordered as a sanction for the spoliation of evidence would have paled next to the testimony of the expert witness")).

E. Premera Should Not Be Allowed to Offer Evidence Regarding A23567-D or the DLP Logs.

An order providing for an adverse inference is appropriate as is barring Premera's expert from opining on exfiltration. But the Court should go further and prohibit Premera from introducing any evidence regarding the spoliated items. Were Premera allowed to offer such evidence, Plaintiffs would be unable to offer any rebuttal evidence as a direct result of Premera's spoliation.

V. CONCLUSION

A rebuttable presumption is an appropriate remedy for Premera taking away Plaintiffs' ability to use the evidence in A23567-D and in the DLP logs in furtherance of their claims. The exclusion of expert testimony prevents Premera from capitalizing on its destruction of evidence to support one of its own defenses, and barring evidence regarding the spoliated items would level the evidentiary field. All three sanctions are necessary to prevent prejudice to the Plaintiffs. For the foregoing reasons, Plaintiffs respectfully request that this Court grant its Motion for Sanctions for Defendants' Discovery Misconduct.

Dated: August 30, 2018

Respectfully Submitted,

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Kim D. Stephens*
Kim D. Stephens, P.S., OSB No. 030635
Christopher I. Brain, *admitted pro hac vice*
Jason T. Dennett, *admitted pro hac vice*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com
cbrain@tousley.com
jdennett@tousley.com

Interim Lead Plaintiffs' Counsel

STOLL BERNE

By: *s/ Keith S. Dubanevich*
Keith S. Dubanevich, OSB No. 975200
Steve D. Larson, OSB No. 863540
Yoona Park, OSB No. 077095
209 SW Oak Street, Suite 500
Portland, OR 97204
Tel: (503) 227-1600
Fax: (503) 227-6840
Email: kdubanevich@stollberne.com
slarson@stollberne.com
ypark@stollberne.com

Interim Liaison Plaintiffs' Counsel

Tina Wolfson
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
Tel: (310) 474.9111
Fax: (310) 474.8585
Email: twolfson@ahdootwolfson.com

James Pizzirusso
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540.7200
Fax: (202) 540.7201
Email: jpizzirusso@hausfeld.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 596-4097
Email: khriebel@locklaw.com

Plaintiffs' Executive Leadership Committee

CERTIFICATE OF SERVICE

I hereby certify that on this day I served the foregoing on all parties by causing a true and correct copy to be filed with the court's electronic filing system, which automatically sends a copy to all counsel of record.

s/ Kim D. Stephens
Kim D. Stephens