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 **OPINION AND ORDER**
This Document Relates to All Actions.	

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 STOLL BERNE LOKTING & SHLACHTER PC, 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.

Plaintiffs bring this putative class action against Defendant Premera Blue Cross ("Premera"), a healthcare benefits servicer and provider. On March 17, 2015, Premera publicly disclosed that its computer network had been breached. Plaintiffs allege that this breach compromised the confidential information of approximately 11 million current and former

members, affiliated members, and employees of Premera. The compromised confidential information includes 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"). According to Plaintiffs, the breach began in May 2014 and went undetected for nearly a year. Plaintiffs allege that after discovering the breach, Premera unreasonably delayed in notifying all affected individuals. Based on these allegations, among others, Plaintiffs bring various state common law claims and state statutory claims.

Before the Court is Plaintiffs' motion for sanctions. Plaintiffs request sanctions for Premera's alleged discovery misconduct in destroying a computer and data loss prevention ("DLP") logs allegedly containing information that could have shown that the hackers exfiltrated the Sensitive Information of the putative class members. Plaintiffs request an order:
(1) instructing the jury to presume that exfiltration of Sensitive Information occurred;
(2) precluding Premera's expert consulting firm Mandiant or any other expert working for Premera from offering any testimony that the expert found no evidence of data exfiltration; and
(3) precluding Premera from introducing evidence about the spoliated evidence. For the reasons discussed below, Plaintiffs' motion is granted in part and denied in part.

A. Legal Standards

Rule 37(e) of the Federal Rules of Civil Procedure allows for sanctions for failure to preserve electronically stored information ("ESI"). This rule provides:

> If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e).

B. Analysis

1. The Destroyed Computer

There were 35 computers identified as involved in the data breach. Mandiant performed an examination of all 35 computers and recommended that Premera preserve all 35 computers. Premera states that it intended to preserve all 35 computers and concedes that all of those computers are relevant to this litigation and subject to discovery. Premera should have preserved all 35 computers. More than one year after the complaint was filed, however, Premera destroyed the hard drive of one of the 35 computers. Premera asserts that this destruction was accidental. Regardless of whether this destruction was accidental, Premera failed to take reasonable steps to preserve the hard drive and its ESI.

Premera states that it intended to place the computer with the other 34 to be preserved when the computer was accidentally put in a different location for "end of life" storage and then destruction. Premera notes that it was a "hectic" weekend when the computers were moved. The computer at issue, however, remained at this other location for more than a year before its hard drive was destroyed. Apparently, at no time during that year did anyone at Premera ever notice that this computer was not being preserved with the other 34 computers. With a massive data

breach, many lawsuits, including putative class actions, and federal and state investigations, it was not reasonable for Premera not to track all 35 affected computers and confirm that they all were being adequately preserved.

Premera also argues that the information lost can be replaced through Mandiant's investigative report. The Court disagrees. The expert report of the opposing party is not an adequate substitute for the underlying object. See, e.g., PacificCorp v. Nw. Pipeline GP, 879 F. Supp. 2d 1171, 1190 (D. Or. 2012) ("[F]orcing a party to rely on evidence selected by an opposing party's expert creates prejudice, because such evidence generally supports that party's case.").

Premera also argues that Plaintiffs are not prejudiced by the loss of this computer because it did not contain relevant information. Premera bases this argument on the fact that its experts at Mandiant did not image the hard drive from this computer, supporting a conclusion that the computer must not have contained critical information. Mandiant, however, had the opportunity forensically to examine the computer, which Plaintiffs' expert does not. The mere fact that Mandiant chose not to image the hard drive during the initial investigation does not establish a lack of prejudice.

Premera also contends the computer did not contain useful information because the FBI did not image this hard drive, although Premera does not offer evidence to support this assertion. Premera does not discuss whether the FBI imaged other hard drives from Premera's computers, to provide any context to the FBI's purported decision not to image the hard drive of this computer. From this evidence, the Court cannot determine that the computer did not contain relevant information simply because the FBI purportedly chose not to image the hard drive.

Finally, Premera argues that the computer did not contain useful information because it did not contain any .RAR files, which are critical files to determine whether data has been exported or exfiltrated. Plaintiffs, however, argue that this computer is the only computer out of all 35 that contained malware called "PHOTO." Plaintiffs assert this malware can manipulate files, processes, the registry, and can upload and download files. Plaintiffs maintain that the hackers configured PHOTO on this computer to communicate with an outside website and that Mandiant found hundreds of communications between this particular computer and that outside website during the relevant hacking period. Plaintiffs contend that only this computer's destroyed hard drive could show what the hackers left behind during those hundreds of contacts. Thus, it is not .RAR files that Plaintiffs contend are important with respect to this particular computer. The Court rejects Premera's argument that this computer necessarily contained no relevant information and thus Plaintiffs' could not have been prejudiced by the loss of this computer.

The Court, however, does not find that Premera acted with the intent to deprive Plaintiffs of the use of the computer in the litigation. The Court thus considers "measures no greater than necessary to cure the prejudice" to Plaintiffs from the loss of the computer. Fed. R. Civ. P. 37(e)(1). The Court finds that allowing Plaintiffs (or the Court) to inform the jury of the destruction of this computer's hard drive[1] and allowing Plaintiffs to argue to the jury about the implications of that destruction is an appropriate measure. The Court, however, will not instruct the jury that it must or even may make certain "adverse inferences" against Premera or about what may have been contained on this computer, although Plaintiffs will not be precluded from making that argument to the jury. Further, the Court will preclude Mandiant or any other expert

[1] The specifics regarding the notification to the jury, whether by Plaintiffs, the Court, or stipulation of the parties, will be determined not later than the final pretrial conference.

working for Premera from testifying that this computer did not contain evidence of exfiltration. Because Plaintiffs' experts do not have the opportunity to review the hard drive and make any determinations relating to exfiltration on this device, no expert can testify that there was no exfiltration from this computer. This ruling does not affect the other 34 devices. These measures are sufficient to cure the prejudice to Plaintiffs.

2. DLP Logs

Premera used DLP software Bluecoat or Vontu as part of its information technology security. This software created logs of the activity observed, including certain data traffic in and out of a network. Premera performed necessary upgrades to its servers after this lawsuit was filed and decommissioned the old servers on which the DLP logs were maintained. In doing so, these DLP logs became inaccessible. Premera states that the "database key . . . was lost" during decommissioning. It is unclear why the DLP logs were not properly preserved or backed-up before the upgrade. Premera merely states, without explanation or detail, that it was "unable to back up or preserve" the logs. The Court finds that Premera did not take reasonable steps to the preserve the DLP logs.

Premera argues, however, that the logs need not have been preserved (and that Plaintiffs have suffered no prejudice from their loss) because they would not have contained any relevant information. Premera asserts that the DLP logs would not have tracked any .RAR files because the DLP software was not configured to track .RAR files. Plaintiffs respond that the DLP logs were important because they would have shown whether the hackers had emailed Sensitive Information offsite. Premera admits that the DLP software scanned email.

The Court finds that Plaintiffs are prejudiced by the loss of the DLP logs and the inability to determine whether they show any removal of Sensitive Information during the relevant time through a method tracked by the DLP software. The Court, however, does not find that Premera

acted with the intent to deprive Plaintiffs of the use of the DLP logs in the litigation. The Court thus considers "measures no greater than necessary to cure the prejudice" to Plaintiffs from the loss of the computer. Fed. R. Civ. P. 37(e)(1).

The Court finds that informing the jury of the destruction of the DLP logs and allowing Plaintiffs to make appropriate arguments to the jury about the implications of the destruction of the DLP logs is an appropriate measure. The Court, however, will not instruct the jury that it must or even may make certain "adverse inferences" against Premera or about what may have been in the DLP logs. The Court also orders Premera to collect and produce to Plaintiffs all Vontu Alert email data and other data Premera believes may be relevant to re-create as closely as possible the data lost from the DLP logs. Finally, the Court will preclude Mandiant or any other expert working for Premera from testifying that the DLP logs did not contain evidence of exfiltration. Because Plaintiffs' experts did not have the opportunity to review the logs and make any determinations relating to exfiltration, no expert can testify that there was no exfiltration based on the DLP logs. These measures are sufficient to cure the prejudice to Plaintiffs.

The Court GRANTS IN PART and DENIES IN PART Plaintiffs' Motion for Sanctions for Defendant's Discovery Misconduct (ECF 182) as provided in this Opinion and Order.

IT IS SO ORDERED.

DATED this 5th day of November, 2018.

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