

information, and sought irrelevant information. (ECF No. 86 p. 4.) After Plaintiffs redrafted their discovery requests more narrowly, Defendants were ordered to then produce a privilege log.

Subsequent to the court's order the parties moved forward, however, Defendant Snow Christensen & Martineau, P.C. experienced a "cybersecurity incident ... that disabled the law firm's access to its electronic files and data, including files related to this case." (ECF No. 101 p. 1.) This necessitated Defendants' Motion for an Extension of Time. Defendant noted that it experienced a ransomware attack restricting access to its files unless money was paid to the attackers. Defendant is unaware of any loss or manipulation to their data and is working with cyber security experts to resolve the issue. Defendant also represented that it will produce the documents and a privilege log once systems are restored to normal.

Plaintiffs became frustrated with the delay this cybersecurity incident caused and filed a motion for sanctions. Plaintiffs assert Defendant has refused to produce a privilege log and has failed to "take reasonable steps to preserve electronically stored information." (ECF No. 106 p. 3.) These arguments are not supported by the record. There is no evidence at this time that data has been lost. And contrary to Plaintiff's unsupported assertions, Defendant has not refused to produce a privilege log.

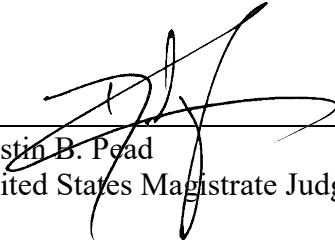
Rule 37(e) provides for sanctions if electronically stored information that should have been preserved is "lost because a party failed to take reasonable steps to preserve it." [Fed. R. Civ. P. 37\(e\)](#). Plaintiffs request "default judgment, or at the very least an Order precluding the defense from entering into evidence any evidence they have not yet disclosed and ... attorneys' fees and costs." (ECF No. 106 p. 3.) Yet, such severe sanctions require a court "finding that the party acted with the intent to deprive another party of the information's use in the litigation" [Fed. R. Civ. P. 37](#). There is simply no evidence of malicious intent by Defendant to avoid their

discovery obligations. Rather, Plaintiffs' motion is more akin to that which is sanctionable under 28 U.S.C. § 1927 for "unreasonably and vexatiously" multiplying proceedings.¹ The facts before the court are not remotely close to those found in *Klein-Becker USA, LLC v. Englert*, 711 F.3d 1153 (10th Cir. 2013), where the imposition of default judgment was upheld as a sanction. Unfortunately, in the modern world cybersecurity attacks are far too common. The court finds no need on the facts before it to needlessly multiply the unfortunate events that have already transpired by entering unwarranted sanctions.

ORDER

Accordingly, Defendants' Motion for an Extension of Time is GRANTED. Plaintiffs' Motion for Sanctions is DENIED. The court further orders Defendant to provide an update to the court and Plaintiffs on the status of recovering any data that was subject to the cybersecurity attack within fourteen (14) days from the date of this order.

DATED this 4 March 2021.



Dustin B. Pead
United States Magistrate Judge

¹ 28 U.S.C. § 1927 provides: "Any attorney or other person admitted to conduct cases in any court of the United States or any Territory thereof who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct." Plaintiffs' motion comes dangerously close to warranting sanctions.