

Procedure (“Rule”) 37, for alleged spoliation of evidence.² “[T]he [2015] amendments to Rule 37(e) limited a court’s discretion to impose sanctions.” *Snider v. Danfoss, LLC*, No. 15 C 4748, 2017 WL 2973464, at *3 (N.D. Ill. July 12, 2017). As noted by another court:

[T]he introductory clause of the current version of Rule 37(e) sets out five prerequisites that must be met before any sanctions may be imposed. First, the information at issue must be electronically stored information (ESI). Second, there must be anticipated or actual litigation. Third, it must be the case that because of the actual or anticipated litigation, the information should have been preserved. Fourth, the ESI must have been lost because a party failed to take reasonable steps to preserve it. And fifth, the lost ESI must be unable to be restored or replaced through additional discovery.

If all of those prerequisites are met, and the Court also determines that one party was prejudiced from the loss of the information, the Court “may order measures no greater than necessary to cure the prejudice.” In addition, if the Court concludes that the offending party acted “with the intent to deprive another party of the information’s use in the litigation,” then it may impose more severe sanctions. These may include presuming that the lost information was unfavorable to the party, instructing a jury that it may or must make that same assumption, and dismissing the action or entering a default judgment.

Worldpay, 2018 WL 5977926, at *3-4 (internal citations omitted).

The magistrate judge recommended denying the motion, finding that Defendants’ version of events was based on speculation and that there was no evidence of intentional destruction of evidence. The magistrate judge noted that Isaac Kohen, Teramind’s Chief Technology Officer, attested that because defendant Dusan Milicevic failed to make the monthly subscription payment for Teramind’s services, Teramind canceled Milicevic’s subscription and deleted the stored screen and audio recordings on July 6, 2018. (Kohen Decl., Dkt. # 162-2, ¶ 7.) According to Kohen, “[w]hen a customer terminates its account, or stops paying for its account, Teramind deletes the customer’s account data” because of the significant amount of storage space that such data requires. (*Id.* ¶¶ 3,4.) In a subsequent declaration, Kohen attested that upon further investigation, he found that an “old server continued to store some of [Defendants’] screen and

² To the extent Defendants also seek relief under the Court’s inherent authority to impose sanctions, at least one court in this district has noted that “this interpretation is at odds with the Advisory Committee Notes to the 2015 amendment to Rule 37(e), which state that the rule ‘forecloses reliance on inherent authority or state law to determine when certain measures should be used.’” *Worldpay, US, Inc. v. Haydon*, No. 17 C 4179, 2018 WL 5977926, at *3 (N.D. Ill. Nov. 14, 2018) (citation omitted). Regardless, the Court will not award relief under its inherent powers, assuming it could do so.

audio recordings from before July 6, 2018,” specifically from November 25, 2017 through January 17, 2018, because the “automated deletion scripts . . . failed to run properly on th[e] old server.” (Kohen Decl., Dkt. # 162-3, ¶ 3.) Kohen’s initial declaration also stated that “[r]ecorded employee monitoring data cannot be deleted by customers or other third parties while an account is still in good standing.” (Kohen Decl., Dkt. # 162-2, ¶ 4.)

The magistrate judge also relied upon Hicks’ declaration that on March 2, 2018, he intended to access Defendants’ Teramind account in order to “remove the account for Ms. Arlene Teller [a Flair call-center employee], because at that time[,] Flair and [Defendants] were no longer working with one another, and as such, [he] did not want Teramind to continue to monitor the activities of a Flair employee.” (Hicks Decl., Dkt. # 162-4, ¶ 5.) Hicks further declared that he did not intend any of his actions on March 2, 2018 “to cause the deletion of any screen or audio recordings from Teramind,” and that he “received no indication from the Teramind interface that any of [his] actions were going to delete, move, or otherwise affect any of the screen or audio recordings stored on the Teramind system.” (*Id.* ¶¶ 8,9.)


In their objections to the R&R, Defendants assert that Flair wanted to delete the audio and screen recordings because they “would demonstrate that Flair executives made the decision to aggressively terminate Flair’s relationship with Defendants without warning, and in turn[,] contradict a sworn Declaration of James Scott, the CEO of Flair, in which he asserts a false narrative of Flair as [a] ‘victim.’” (Defs.’ Obj., Dkt. # 192, at 2.) According to Defendants, Hicks’ assertion that he never intended to delete any recordings is belied by the fact that he simply could have uninstalled the Teramind software from the Flair computer to end any contact between Teramind and Flair, but instead, twice engaged the “delete” commands – “once for the [Flair computer in] Winnipeg and once for the data files of Arlene Teller.” (*Id.* at 5-6.) Defendants argue that “[t]he idea that an IT professional could engage twice in such [delete] commands on an administrative screen and credibly assert that he had no idea that he was deleting data strains reason to the extreme.” (*Id.* at 6.) Defendants also contend that Hicks’ statement that he engaged the delete commands because he was not familiar with the Teramind system is not believable given that Hicks admitted in his deposition that he installed the Teramind system on the Flair computers in Winnipeg and that he was the only person who acted as a troubleshooter for the Teramind program when a problem arose. (*Id.* at 5.) But, as the magistrate judge noted on numerous occasions in his thorough R&R, Defendants’ objections amount to nothing more than speculation and are supported by no specific evidence.

Defendants note further that while Kohen attested that recorded employee data cannot be deleted by customers or other third parties while an account is in good standing, the Teramind user manual, which is unauthenticated, indicates that account administrators like Hicks can “delete everything.” (*Id.* at 6-7.) However, as noted by Flair, Defendants did not depose Kohen or seek to obtain any other testimony from Teramind employees that would elucidate the statements in the user manual or explain a possible contradiction with Kohen’s sworn declaration. The phrase “delete everything” is vague and open-ended and, as such, Kohen’s testimony remains un rebutted.

Defendants also attempt to demonstrate that Flair must have engaged in impropriety by focusing on the timing of the alleged destruction. Defendants ask the Court to attribute a nefarious motive to the fact that Flair’s Chief Executive Officer, James Scott, did not execute the affidavit in support of Flair’s request for an injunction against Defendants in the Canadian litigation until March 5, 2018 (after Hicks’ purported destruction of the audio and screen recordings on March 2, 2018) even though Flair filed suit on February 27, 2018. Defendants ask: “Why such a delay[] if Flair was being damaged day by day?” (Defs.’ Obj., Dkt. # 192, at 11.) According to Defendants, “it is not unreasonable to conclude that Scott could not sign his [a]ffidavit until the Winnipeg recordings, emails and messages were destroyed.” (*Id.* at 12.) Again, however, this is conjecture supported by no competent evidence.

Defendants have set forth no evidence from which the Court can conclude that the audio and screen recordings were lost because Flair failed to take reasonable measures to preserve it (as opposed to Defendants’ failure to pay for Teramind’s services). Accordingly, sanctions are not warranted. For these reasons, the Court overrules Defendants’ objections and adopts the R&R in its entirety, and along with the reasons stated herein, denies Defendants’ motion.

Date: April 3, 2019


Ronald A. Guzmán
United States District