1. An order from the U.S. District Court for the Southern District of New York granting certain spoliation sanctions but denying others where the Plaintiff lost access to two online databases containing relevant electronically stored information (ESI) when its business failed and it could not continue to pay the ongoing costs to host those databases.

In *Medcenter Holdings Inc. v. Web MD Health Corp.*, No. 20 Civ. 53 (ALC) (GWG), 2023 WL 5963616, --- F. Supp. 3d ---- (S.D.N.Y. Sept. 14, 2023), U.S. Magistrate Judge Gabriel W. Gorenstein addressed whether spoliation sanctions were appropriate based on Plaintiff's conduct when Plaintiff determined it could no longer pay for online hosting of the relevant ESI.

Plaintiff, which collects and provides medical and pharmaceutical information, brought this trade secret action against Defendants related to two extensive databases that it had developed and maintained. *Id.* at *1. The first, the "Physicians Database," contained information about physicians and their areas of practice and specialties. The second, the "Salesforce Database," contained unique pharmaceutical drug and medical product project performance data. *Id.* at *2. Plaintiff alleged that Defendants, including Web MD, "conspired together to arrange to poach" an executive named Mariel Aristu from Plaintiff in June 2016 and that, before she left to work for Defendants, she stole "extensive amounts" of data from the Physicians Database and the Salesforce Database and provided this data to Defendants.

Plaintiff filed this action on January 3, 2020, more than two years after its business collapsed. Plaintiff listed documents and information from the Salesforce Database and the Physicians Database in its initial disclosures under Federal Rule of Civil Procedure 26(a). *Id.* at *9. With respect to both databases, Plaintiff informed Defendants that "all or a substantial portion" of the data was stored in a "Microsoft Azure platform" that was "accessible." A year and a half later, on July 23, 2021, however, Plaintiff disclosed that the hosting arrangement for the Physicians Database had been "terminated due to lack of funds," that "[d]ata was backed up from the Microsoft cloud server before that account was terminated, but some portions of the underlying data were not able to be backed up," and that Plaintiff would produce the backed-up data. The Physicians Database was apparently stored across multiple locations, and "once Microsoft terminated" Plaintiff's access to certain storage locations, Plaintiff "was not able to recover" the data it had stored in this fashion.

In addition, Plaintiff's subscription to the Salesforce Database had lapsed by the end of 2018 because "there were no operating funds available to renew the contract" and Plaintiff had gone out of business. This resulted in Plaintiff losing access to the Salesforce Database. But Plaintiff requested and downloaded all of the information it had stored in the Salesforce Database, which information then was maintained in the form of spreadsheets.

Defendants filed a motion for spoliation sanctions under Federal Rule of Civil Procedure 37(e) and to prevent Plaintiff from introducing "any evidence at trial concerning or allegedly derived from the databases that comprised the alleged trade secrets at issue" or an order for "an adverse inference jury instruction."

Magistrate Judge Gorenstein began his analysis with a survey of the legal standards under Federal Rule of Civil Procedure 37(e), which governs spoliation of ESI. *Id.* at *3-4. "Spoliation is the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." He quoted the rule and explained that imposition of spoliation sanctions requires a showing that relevant ESI, which should have been preserved, was lost because a party failed to take reasonable steps to preserve it, that the ESI cannot be restored or replaced through additional discovery, and that the loss prejudiced another party.

Magistrate Judge Gorenstein noted that Rule 37(e) does not define a party's obligation to preserve ESI, but this element requires a showing that the spoliating party "had an obligation to preserve the evidence at the time it was destroyed." He explained that this duty usually "arises when a party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."

Magistrate Judge Gorenstein explained that the determination of "when the duty to preserve evidence arises may, under certain circumstances, be dependent upon the nature of the evidence." He referred to the advisory committee's note to the 2015 amendment of Rule 37(e), which provides that "[c]ourts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant." He further noted that "the standard is an objective one, asking whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation."

Magistrate Judge Gorenstein proceeded to analyze the parties' respective arguments regarding when Plaintiff's obligation to preserve ESI first arose. Defendant argued that Plaintiff's obligations first arose between June and July 2016, when it corresponded internally and with Mariel Aristu regarding her work with Web MD. *Id.* at *4-6. In particular, an employee of Plaintiff's wrote to Mariel Aristu in July 2016 regarding her use of Plaintiff's confidential information, stating that Plaintiff believed that both she and Web MD were in breach of their respective agreements with Plaintiff. Magistrate Judge Gorenstein found that these communications did not give rise to a preservation obligation because they discussed potential misuse of confidential information, not the theft of trade secrets by Mariel Aristu or anyone else. As a result, he found that these communications "do not evince any understanding of the possibility of the trade secrets claims here — that is, claims that allege that defendants acquired proprietary information through Mariel Aristu that was stolen from" Plaintiff. *Id.* at *6.

Magistrate Judge Gorenstein likewise rejected Defendants' argument that a duty to preserve was shown by minutes from a meeting of Plaintiff's board of directors on August

31, 2016, and from a meeting of its shareholders the following day. *Id.* at *6-7. The minutes of the August 31, 2016, meeting reflected discussion of a proposal for "a general meeting to be called to address Mariel Aristu's removal and the filing of civil and criminal proceedings." The minutes of the September 1, 2016, meeting also referenced Mariel Aristu's "possession and utilization ... of sensitive information" and proposed to "initiate the corresponding proceedings for damages and losses" and "the task of selecting the attorneys and immediate filing of the aforementioned proceedings." But Magistrate Judge Gorenstein used other evidence to show that the references to Mariel Aristu's having had access to "secret commercial and corporate information" referred to her "broad knowledge" of Plaintiff's business and that there was no accusation within either set of minutes that Mariel Aristu stole all or part of the relevant databases and provided them to Web MD. Considering this evidence, Magistrate Judge Gorenstein could not conclude that Plaintiff "harbored any belief at this time that Mariel Aristu had shared data from the" relevant databases "or that it should have harbored such a belief."

Magistrate Judge Gorenstein next addressed Defendants' contention that emails from Plaintiff to Mariel Aristu between September and November 2016 showed a duty to preserve, again rejecting this argument. *Id.* at *7-8. The emails accused her of "using information which is confidential to" Plaintiff and breaching her duties to Plaintiff, and they threatened legal action against her. Magistrate Judge Gorenstein again found that these emails did not show by a preponderance of the evidence any specific awareness by Plaintiff that Mariel Aristu had taken trade secrets in the form of data from the relevant databases; instead, they appeared to address potential violations of confidentiality agreements and related duties.

Finally, Magistrate Judge Gorenstein addressed Defendants' argument that Plaintiff's preservation duty arose in 2017, when Plaintiff's information technology administrator investigated Mariel Aristu's use of the Salesforce Database. *Id.* at *8-9. The administrator testified that he generated a report from the Salesforce Database "in early 2017" to see which users had run reports and that this process showed "unusual or strange times and also locations from which the Salesforce [Database] was accessed." Magistrate Judge Gorenstein noted that this "unusual" activity was "directly related to the claims in this case — namely that Mariel Aristu was improperly accessing the Salesforce Database, enabling her to view its data and thus to unlawfully steal trade secrets from" Plaintiff. Accordingly, he found that these reports meant Plaintiff "actually knew or should have known at that time that Mariel had potentially stolen information from" Plaintiff's databases. He thus found that a duty to preserve documents arose in "early 2017."

Magistrate Judge Gorenstein next addressed when spoliation of the relevant databases occurred and whether Plaintiff took reasonable steps to preserve the databases, starting with the Physician's Database. *Id.* at *10. He noted that contact information from the Physician's Database had been maintained, but noncontact data including "granular detail about user engagement with" Plaintiff's website had not been preserved. Magistrate Judge

Gorenstein found that the first element of the spoliation analysis was met as to this data because Plaintiff had an obligation to preserve it at the time it was destroyed in mid to late 2017 when Plaintiff lost access to it.

With respect to the steps Plaintiff took to preserve the data, Magistrate Judge Gorenstein found that Plaintiff provided "no intelligible explanation" as to why the contact data, but not the noncontact data, from the Physician's Database was downloaded and saved. Plaintiff claimed that the data was too expensive to continue hosting with Azure and too voluminous and therefore "impractical" to back up, but Magistrate Judge Gorenstein discounted this argument because in his view the issue was whether the noncontact data "was downloadable and could be preserved without hosting in the same way the contact data was." He found Plaintiff's explanations in this regard "not sufficiently substantiated" and "particularly weak" because Plaintiff had preserved some data.

Having established spoliation of ESI from the Physician's Database, Magistrate Judge Gorenstein turned to an analysis of whether Plaintiff showed a "culpable state of mind" in failing to preserve. He concluded that Defendant had not made such a showing. *Id.* at *11-12. He noted that Rule 37(e)(2) requires a finding of "intent to deprive" before the court 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." Defendants argued that Plaintiff's intent could be inferred from its selective preservation, because contact data had been preserved but noncontact data had not. Magistrate Judge Gorenstein rejected this argument, which he noted was "strongest when the party at issue was specifically aware of an ongoing proceeding for which the data was relevant, which is not the case here." He found that Plaintiff had offered a plausible explanation for why it distinguished between the contact and noncontact data due to the cost and practicality of downloading the data. Considering this explanation, he found that Defendants did not meet their burden of showing intent by clear and convincing evidence.

Magistrate Judge Gorenstein next found that loss of the noncontact information from the Physician's Database prejudiced Defendants, noting "it is axiomatic that in a case concerning the theft of particular trade secrets that spoliation of those very trade secrets is prejudicial to defendants" because the spoliation "deprives defendants of the ability to learn the specific nature of the secrets and to make judgments or hire an expert to opine on what their value might be." *Id.* at *12.

Regarding the appropriate sanction for spoliation of the noncontact information in the Physician's Database, Magistrate Judge Gorenstein noted that Rule 37(e)(1) provides that where spoliation has caused prejudice to the moving party, the court may impose measures "no greater than necessary to cure the prejudice." *Id.* at *13. He concluded that the measure to most directly cure the prejudice would be to preclude Plaintiff from presenting evidence as to the nature or value of the noncontact data because it would be

unfair to Defendants to require them to counter the evidence regarding the data if they have been placed in the position of not having any access to that data.

Magistrate Judge Gorenstein next turned to whether spoliation of the Salesforce Database occurred. *Id* at *13-16. He explained that Plaintiff had access to a "limited version" of Salesforce as of 2018 but discontinued its subscription due to an inability to pay "beyond 2018." But before losing access to the database, Plaintiff's IT administrator had downloaded and saved a backup of all data residing in the Salesforce Database that Salesforce had made available. This backup was saved to a hard drive in table file formats, generally as .csv files, and those files were produced to Defendants. According to Plaintiff, the backup data could be used to show records of in-person meetings and calls between Plaintiff and its clients, including for accounts associated with Mariel Aristu and her use of the Salesforce system.

Defendants argued that Plaintiff's backup of the Salesforce Database resulted in spoliation because the backup data was not "substantially as effective" as "what would have been available had the database been hosted." *Id.* at *15. Magistrate Judge Gorenstein rejected this argument, noting that the requirement of a party to take reasonable steps "does not call for perfection." He explained that "it is not necessarily reasonable to require a company that has lost its revenue and is essentially a nonfunctioning entity to pay for a hosting contract for potentially years when the data at issue can be preserved, even if it is in a less convenient form." He referenced the commentary to Rule 37, which notes that a "court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms." Ultimately he concluded that Defendants did not proffer competent testimony demonstrating what would have been available on the hosted Salesforce Database platform that they needed but did not have based on Plaintiff's production. Accordingly, he found that Plaintiff took reasonable steps to preserve data from the Salesforce Database and that no spoliation of that data occurred.