UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 23-CV-24868-ELFENBEIN

PLITEQ, INC., *et al.*,

Plaintiffs,

v.

MAGED MOSTAFA,

Defendant.
_____/

ORDER DENYING PLAINTIFFS' VERIFIED MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

THIS CAUSE is before the Court on Plaintiffs' Verified Motion for Temporary Restraining Order and Preliminary Injunction (the "Motion" or "Motion for Preliminary Injunction"), ECF No. [50]. For the reasons explained below, the Motion for Preliminary Injunction, **ECF No. [50]**, is **DENIED**.

I. BACKGROUND

This lawsuit involves a dispute between the Plaintiffs, Pliteq, Inc. ("Pliteq") and Pliteq Building Materials, LLC ("PBM") (collectively "Plaintiffs"), and Defendant Maged Mostafa ("Mostafa" or "Defendant") regarding Mostafa's alleged trade secret misappropriation and breach of contract shortly before his employment termination. Specifically, in the Amended Complaint, Plaintiffs sued Mostafa for misappropriation of trade secrets pursuant to the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836 (Count I), unfair competition (Count II), injunctive relief (Count III), breach of employment contract (Count IV), breach of confidentiality agreement (Count V), breach of fiduciary duty (Count VI), and conversion (Count VII). *See* ECF No. [120] at 10–20.

In the Motion, Plaintiffs seek a preliminary injunction enjoining Defendant "from possessing, transferring, using, or disclosing any Information, for his benefit or the benefit of any third party[and] ordering the seizure of Defendant's DropBox and Microsoft OneDrive Accounts" *See* ECF No. [50] at 20. Following the filing of the Motion, Defendant submitted a timely Response in opposition and Plaintiffs thereafter filed a timely Reply. *See* ECF Nos. [72] and [82]. In support of their respective positions, the Parties also filed numerous exhibits and multiple declarations. *See* ECF Nos. [72] at 19-30, [74], [78], [82-1]-[82-5]. The Court then held an evidentiary hearing (the "Hearing") at which time the Parties presented documentary evidence as well as the live testimony of Santiago Ayala and Matthew Pulcine and excerpts of Mostafa's deposition testimony. *See* ECF Nos. [77], [81], [83], [93], [96], [98], [100], [101], [102], and [134]. At the Hearing, Plaintiffs also made an *ore tenus* Motion for Sanctions against Defendant for spoliation of evidence. *See* ECF No. [88].

Following the conclusion of the Hearing, Plaintiff filed an Amended Complaint adding new claims for relief. *See* ECF No. [120]. Because one of the factors in a preliminary injunction analysis is the likelihood of success on the merits, the Court required supplemental briefing from the Parties regarding the impact of new claims in the Amended Complaint on the pending Motion. *See* ECF No. [126]. Both Parties timely submitted their supplemental briefing. *See* ECF No. [127] and [135]. While the Motion was pending, Defendant moved to strike portions of Plaintiff's expert witness report that discussed evidence from Mostafa's laptop and to exclude evidence contained in the laptop, arguing that it was obtained illegally and was, therefore, inadmissible (the "Motion to Strike"). *See* ECF No. [150]. Given that Plaintiffs introduced a significant amount of evidence at the Hearing about the forensic analysis of Mostafa's laptop, the Court needed to first rule on the

Motion to Strike, which it ultimately denied. *See* ECF No. [214]. The Motion for Preliminary Injunction is now ripe for review.

II. TESTIMONY

a. Matthew Pulcine[1]

Plaintiffs called Matthew Pulcine ("Mr. Pulcine"), the Chief Financial Officer of Pliteq and member of its Executive Council, as a witness during the Hearing. *See* ECF No. [100] at 91-92. Mr. Pulcine explained that, over the years, Pliteq has developed patented products made of recycled rubber used in building construction projects to isolate vibration and reduce noise, such as Pliteq's GenieMat RST, which is used in multi-family high-rise buildings underneath the finished floor. *Id.* at 92-93. Approximately 65% of Pliteq's business is in the United States. *Id.* at 94. PBM, on the other hand, is an affiliate of Pliteq based out of Dubai, United Arab Emirates ("UAE"). *Id.*

Relevant to the trade secret issues in the Motion, Pliteq[2] operates using a cloud-based computer system, meaning all its computing services are over the Internet using Google Cloud, Google Workspace, and Google Drive. *Id.* at 95. Dino Bozzo ("Bozzo"), Pliteq's director of Business IT, oversees all the IT systems at Pliteq, including Google Cloud and Google Workspace. *Id.* Regarding trade secrets, Mr. Pulcine testified that Plaintiffs consider their factory and manufacturing process to be trade secret because the design of the product is unique to Pliteq and is proprietary. *Id.* at 96. The same is true for their manufacturing equipment as it is specifically designed for Pliteq's sole use. *Id.* Pliteq has recipes for its products, including the amount of raw

[1] Although Plaintiffs called their expert, Santiago Ayala, as their first witness, the Court takes the testimony out of order as Mr. Pulcine provided much of the necessary background information to understand the context of Mr. Ayala's testimony.

[2] Throughout the Hearing, Plaintiffs used the term Pliteq to refer to both Plaintiffs unless noted otherwise.

material used in each manufactured product, and it likewise considers its recipes to be trade secret. *Id.* In terms of marketing, Plaintiffs rely on their architect and acoustic consultants to specify the products in a particular building's design drawings. *Id.* at 96-97. Pliteq has targeted global firms and individuals within those firms, maintaining a database called NetSuite containing the contact information for their consultants and customers. *Id.* at 97. NetSuite also contains their sales and future sales as well as potential sales opportunities. *Id.* Pliteq is continually investing in research and development, targeting the consultants and architects, to ensure they meet the building code, which gives Pliteq a competitive advantage. *Id.* at 98. Pliteq likewise considers these test reports to be trade secret. *Id.*

As it relates to Defendant, Mr. Pulcine testified that he was the general manager of PBM in Dubai, an officer of Pliteq in North America, and a member of the Corporate Executive Council, which sets the strategy for Pliteq. *Id.* PBM terminated Defendant in November 2023. *Id.* In 2018, Defendant previously signed a Contract of Employment with PBM that, among other provisions, contained a Confidential Business Information clause, requiring that, at the termination of the contract, Defendant return all company documents in his possession, whether in paper or electronic form, relating to the company's affairs. *Id.* at 99; ECF No. [96-2]. Pliteq considered the Confidential Business Information clause important because its data is confidential and trade secret. ECF No. [100] at 99. In addition, Pliteq required that Defendant sign an additional agreement, entitled "Confidentiality, Assignment of Intellectual Property, Non-Competition and Non-Solicitation Agreement" (the "Confidentiality Agreement"), ECF No. [96-3], which Defendant and Pliteq CEO Paul Downey ("Mr. Downey") signed on February 18, 2021. ECF No. [100] at 100. The Confidentiality Agreement contains restrictions on how Pliteq employees may use its information, including restricting a mass download of information onto a personal cloud

account. *Id.* And, the Confidentiality Agreement contains a stipulation to injunctive relief to protect its confidential and trade secret information. *Id.* Pliteq also required that Defendant sign a document entitled "Additional Agreement Terms," ECF No. [96-4], which covered additional responsibilities as the vice president in corporate development and marketing for Pliteq and all its affiliated entities. ECF No. [100] at 101.

Mr. Pulcine testified that, in Fall 2023, Defendant received a negative performance review and sometime thereafter, on October 26, 2023, Pliteq Finance Manager, Olivia Baker, received a concerning email from Defendant referencing unpaid compensation items that Pliteq owed him per his employment agreements, including commissions, stock options, annual tickets, and unpaid vacation days. *Id.* at 106-107; ECF No. [96-6]. Pliteq responded by looking into Defendant's work-related emails in his @pliteq.com account around October 30 or 31, 2023 at which time they discovered an email that contained two download links from Google Takeout with many Pliteq files. ECF No. [100] at 107-108; ECF No. [96-7]. This email concerned Pliteq because it was unauthorized and highly unusual, so Pliteq began shutting down Defendant's permissions and log ins. *Id.* at 108. The first link included a 4.8 gigabyte zip file. *Id.* at 109.

As explained below in the testimony of Plaintiffs' forensic expert, Santiago Ayala ("Mr. Ayala"), this zip file was discovered on an Acer laptop that Defendant used for work. Mr. Pulcine testified that Defendant originally purchased the laptop and later received a reimbursement from Pliteq for the laptop purchase. *Id.* at 101-106; ECF No. [96-5]. At the time of the investigation, Pliteq took possession of the laptop and sent it to Mr. Ayala in Florida, but the Dubai police thereafter requested the laptop for ongoing legal proceedings, and Pliteq provided it as requested. ECF No. [100] at 109. Given that Defendant may receive the return of the laptop at some future time, Pliteq requested the return of the laptop as part of the relief sought in the Motion. *Id.* On

October 31, 2023, Pliteq sent a letter to Defendant in which it instructed him to return the laptop as company property, but Defendant did not comply. *Id.* at 110, ECF No. [96-12]. And in an email dated October 31, 2023, Pliteq also included an instruction for Defendant to return company property, but he did not. ECF No. [100] at 110-111; ECF No. [96-13]. Defendant responded to the emails explaining that the laptop was a personal laptop, which worried Pliteq because he cannot download confidential and trade secret information belonging to the company on a personal laptop. ECF No. [100] at 112; ECF No. [96-16]. In the email, Defendant also explained that this download was part of a backup functionality that Defendant employed on behalf of Pliteq, but Pliteq disputed this was done in good faith as it stores and backs up its own data in the Google Cloud, and Defendant lacked the authorization to download a massive amount of confidential and trade secret information. ECF No. [100] at 112-113. Pliteq was also concerned about the security of its data given that it could no longer control what Defendant did with the information. *Id.* at 114. Regarding the laptop, Mr. Pulcine testified that Pliteq needs it back because it is "unsure" what will happen if the laptop is turned on at some future point in time. *Id.* a 145-146.

In response, Pliteq's lawyers sent a letter to Defendant disputing the need to download company information onto the laptop and asking Defendant to provide an undertaking letter in which he would delete the downloaded information, agree that he would not disclose the information, and allow them to verify that the information was actually deleted, but Defendant did not provide the letter or otherwise allow Pliteq to verify the deletion. *Id.* at 115; ECF No. [96-17]. On November 6, 2023, Pliteq's Dubai lawyers sent Defendant another follow up letter, but Defendant did not respond, and another group of Pliteq lawyers sent him a third letter inviting him to attend a disciplinary hearing, but Defendant did not attend. *Id.* at 116; ECF Nos. [96-18], [96-19]. Finally, on November 21, 2023, Pliteq sent Defendant a termination letter with a further

instruction that Defendant return company information, including electronically stored information and the download of the Google Takeout file, but Defendant did not do so. *Id.* at 117; ECF No. [96-20].

Instead, in response, Defendant's lawyers sent a letter to Pliteq explaining that Defendant had full access to the information on Google Drive without any restrictions throughout his employment, a statement with which Mr. Pulcine agreed, explaining that Defendant had broad access as part of the Executive Council. ECF No. [100] at 117-118. In the same letter, Defendant's lawyer explained that Defendant was involved in data management practices, including conducting security backups of the company data, *see* ECF No. [96-21], but Mr. Pulcine disputed that, explaining that Mr. Bozzo, as the Director of IT, was in charge of doing so and that security backups could take place through Google Takeout and through their service in Google Cloud, *see* ECF No. [100] at 119. Mr. Pulcine further testified that Defendant had never, in fact, performed a Google Takeout for a massive data download like the one in October of 2023, which Plaintiffs investigated by looking for a replica of other Google Takeout emails in Defendant's inbox and finding none. *Id.* at 120. As Pliteq understood the letter received from Defendant's attorney, Defendant was confusingly taking the position that he did not download Pliteq's information, which Defendant acknowledged may be against the company's internal policies, and that Defendant had not deleted the information in his custody. *Id.* at 120-121. In response, Pliteq's lawyers sent another letter to Defendant, this time through his lawyers, demanding the return of company confidential information, deleting any confidential information, and providing an

undertaking letter, but Defendant did not comply. *Id.* at 121-122; ECF No. [96-22]. Plaintiffs thereafter filed this lawsuit. ECF No. [100] at 122.

As part of its investigation, Pliteq verified whether Defendant downloaded its confidential and trade secret information by clicking and downloading the information in the Google Takeout file emailed to him. *Id.* In doing so, it confirmed that Exhibits 29, 30, 32, and 35 were in the Google Takeout file while Exhibits 29, 30, 32, 34, and 35 were all downloaded onto Defendant's OneDrive folder, which was synched to the Acer laptop. *Id.* at 132-135, 138. Exhibit 29, in particular, was a plant capacity exhibit showing the volume Pliteq can produce in its plant during any given period as well as volume by product line. *Id.* at 135-136. This document contains information about capital expenditures needed to meet these volumes, information about new unreleased products, and projected revenue for one of its regions. *Id.* at 136-137. If released, Mr. Pulcine testified that Plaintiffs' competitors would have access to their pricing strategy and can then undercut them in a competitive market. *Id.* at 137. Exhibit 29 also contains Pliteq's recipes by product line, meaning the amount and ingredients needed for each particular product, which Pliteq considers to be a trade secret. *Id.* at 138.

As for Exhibit 30, this is a listing of Pliteq consultants and customers included in the Google Takeout download. *Id.* at 138. Pliteq also considers this information trade secret because it has Plaintiffs' contacts who specify Pliteq products in construction projects, listed by firm and the individuals at those firms. *Id.* Mr. Pulcine explained that it is key to know contacts at specific firms because they prepare the specifications for the design plans in certain buildings. *Id.* at 138-139. Regarding Exhibit 31, this is a product roadmap for Pliteq to reach $140 million in revenue, which was information circulated to the Executive Council as of June 12, 2023. *Id* at 139. Included in the information in Exhibit 31 are Pliteq's new, unreleased products, which Pliteq

considers to be trade secret. *Id.* at 140. More broadly, Pliteq considers all its research and development to be trade secret. *Id.*

Next, Exhibit 32 contains a financial forecast for the Middle East and North Africa region, but Mr. Pulcine explained that this also related to the North America market because all Pliteq products are manufactured at the Canadian facilities. *Id.* at 141. This document contains product cost information for each individual product, all of which Pliteq considers to be trade secret. *Id.* Exhibit 34 contains Pliteq's orders to ship as of October 2023, including revenue booked to date, future orders, customer names, project names, pricing, quantities, and expected shipment dates. *Id.* at 142. In short, this is a roadmap for specific projects in the pipeline, which Pliteq believed could help competitors take those specific projects if released. *Id.* Finally, Exhibit 35 is a testing report that compares Pliteq's products to a competitor's products. *Id.* at 143-144.

On cross-examination, Mr. Pulcine was asked about the December 6, 2023 letter from Defendant's counsel to Pliteq, and he agreed that, according to the letter, Defendant had not done anything to prejudice or jeopardize Pliteq's information, had never shared any data, and guarded Pliteq's interests and information with the utmost care and diligence. *Id.* at 164; ECF No. [96-21]. He also agreed the letter represents that, as of that date, Defendant did not possess any confidential information belonging to Pliteq and that Defendant acknowledged he was aware of his obligations to preserve Pliteq's confidential information, even after his termination. *Id.* Mr. Pulcine also agreed there was evidence that Defendant deleted records between November 2023 and February 2024, and Mr. Pulcine did not know whether the exhibits containing Pliteq trade secrets had

already been deleted. ECF No. [100] at 164-165. And he also agreed that not all Pliteq documents are trade secret. *Id.* at 165-166.

Mr. Pulcine further testified on cross-examination that Defendant was not prohibited from downloading Pliteq documents or information on the Acer laptop because it was an office computer. *Id.* at 169-170. When asked specifically whether the language in the Confidentiality Agreement prohibited Defendant from downloading company information onto the Acer laptop, Mr. Pulcine agreed that this agreement did not prohibit it. *Id.* at 171-172; ECF No. [96-3]. And he agreed that Pliteq was aware that Defendant would receive confidential information given his role on the Executive Council. ECF No. [100] at 170-171. Finally, Mr. Pulcine agreed that Pliteq had presented no evidence that Defendant had disclosed any trade secrets or confidential information to any third party. *Id*. at 172.

On redirect, Mr. Pulcine clarified that while a download onto a company laptop may be permitted, syncing that data with a personal cloud account was not allowed. *Id.* at 173.

b. Santiago Ayala

At the Hearing, Plaintiffs presented the testimony of their expert in digital forensics, Santiago Ayala, who Plaintiffs retained to perform a forensic image and analysis of an Acer laptop computer that Defendant used for work. *See* ECF No. [100] at 11-12, 14. In particular, Mr. Ayala was asked to perform an analysis involving a potential download of data on that computer, which required him to first make a forensic image of the laptop. *Id.* at 14, 16. Turning to his analysis, Mr. Ayala testified that the computer had a user profile named "Maged," the user last shut down the computer on October 13, 2023, and it last went into sleep mode on October 30, 2023 at 7:24 p.m. *Id.* at 18, 20. The computer then remained in a sleep state on standby mode until November 2, 2023 at 7 a.m. *Id.* at 21. The user of the laptop also had, at one point, a USB device and a

Samsung Galaxy 45 cell phone connected to the computer system. *Id.* Importantly, Mr. Ayala found evidence of a Google Takeout request through an internet browser using a login of mmostafa@pliteq.com. *Id.* at 22. After the request was made, the user for this laptop profile then received an email, downloaded the file, which was 4,881,172,262 bytes, moved it to another folder about three minutes later with the following file path: Mag > OneDrive > Dropbox > Work > Pliteq > Mag > Backup. *Id.* at 23-25. Mr. Ayala explained that the OneDrive account was linked to an account called maged10@hotmail.com while the Dropbox account was linked to mag@mostafa.ca, and the file path was "likely synced" to both the OneDrive and Dropbox accounts, meaning the file was stored locally and in the cloud. *Id.* at 29-30.

Mr. Ayala also received a CSV file from Dropbox, which revealed that it contained a file transfer exactly matching the number of bytes added to the laptop from the Google Takeout file. *Id.* at 36. Based on his review of the Dropbox CSV file, Mr. Ayala determined that there were some deletions of records from the Dropbox account in late November to early December, but these were not significant in number. *Id.* at 37. By comparison, most of the deletion activity occurred on January 24 and February 2, 2024, and in particular, an email from Dropbox revealed that 8,105 files named producttestreports.xlsx were deleted on the earlier date. *Id.* at 38, 40, ECF No. [96-24]. The laptop, however, remained in the custody of the Dubai Police Department, but according to Mr. Ayala, if the laptop were powered on and if the applications are still syncing to the cloud storage, then the computer will "most likely" attempt to upload data onto the cloud again. ECF No. [100] at 41-45. Based on his review of information, Mr. Ayala was unable to determine

whether all files from the Google Takeout file were deleted from Dropbox, OneDrive, or other electronic devices. *Id.* at 45.

On cross-examination, Mr. Ayala testified that he completed his forensic image of the laptop on November 20, 2023. *Id.* at 53, ECF No. [78-1] at 3. Mr. Ayala could not testify whether the folder where the Google Takeout file was stored on the computer had been accessed prior to October 30, 2023 nor was he provided any information for the Dropbox account pre-dating October 28, 2023. *Id.* at 57-58. A review of the internet browsing history on the laptop for October 30, 2023 revealed that Defendant searched the following: UAE Labor Law 2023, Employment Laws and Regulations in the Private Section, the Official Portal of the UAE Government, Gratuity Calculator Dubai, Official Gratuity Calculator Dubai, and Online Gratuity Calculator Dubai Development Authority. *Id.* at 67-68.

When asked questions about his hypothesis that an auto sync of documents could occur if the laptop were turned on, Mr. Ayala twice stated that is "a possibility." *Id.* at 68. And for this possibility to arise, he explained that "[t]here are a lot of things that have to happen," including the laptop "has to be powered on, it has to be connected to the Internet and the applications have to be still syncing to the cloud accounts." *Id.* And for the applications to sync, the passwords or access credentials must be the same.[3] *Id.* at 68-69. Mr. Ayala could not testify to any degree of forensic probability that the laptop was still syncing to these applications and could, at best, testify that there was a "risk" that such an upload could happen. *Id.* at 70.

c. Maged Mostafa

Both sides designated portions of Defendant's deposition testimony to be considered on the issue of sanctions for spoliation of evidence and for the preliminary injunction. Defendant

[3] Defendant testified during his deposition that he changed his password to his Dropbox account on October 31, 2023. *See* ECF No. [77-2] at 91.

testified that he was terminated from Pliteq on November 21, 2023, but he was entitled to three months' notice under UAE law, so his last date of employment was effectively February 21, 2024. ECF No. [77-2] at 12, 17-18. His access to Pliteq's systems though was suspended as of October 31, 2023. *Id.* at 18. Upon review of his employment contract with Pliteq dated January 16, 2018, Defendant agreed to the provisions defining "confidential information," requiring that he return to the company all documents in his possession relating to company affairs by the end of his employment, which he calculated as February 21, 2024. *Id.* at 18-22. When asked what sort of documents he had on his laptop at the time of his termination, he explained that the vast majority were in the public domain, but he also had sales training, market research, product collateral specification sheets, product tests, product descriptions, videos for installation from customer sites, distribution agreements, request letters, memos or letters sent to customers for collections, planning documents, presentations, and normal operating files. *Id.* at 25-27. He estimated that 80 to 90 percent of the materials on his laptop related to his work in sales, marketing, and the administrative roles he played. *Id.* at 27.

Relevant to the issue of spoliation, during Defendant's first deposition taken on June 14, 2024, Defendant testified that it "could be" that some sources of responsive documents from the date of his termination with Pliteq were not searched because they had been deleted. ECF No. [77-1] at 75-76. During his June 21, 2024 deposition, he explained that, after he received a legal notice from PBM's counsel asking him to delete all Pliteq documents (otherwise he could be subject to criminal charges), Defendant began to delete documents starting with confidential information and eventually, all other Pliteq documents. ECF No. [77-2] at 23. He did not, however, return any company documents to Pliteq after his termination. *Id.* As his laptop had already been taken, he instead went online to check whether any documents were synced on a

backup service, and he had the option to return them or delete them, so he opted to delete them. *Id.* at 24. When he searched for confidential documents for deletion, Defendant explained that there were a few documents for business planning or involving financials that were marked as "confidential," so he deleted those. *Id.* at 28. He started deleting information in late November 2023, starting with the information marked as "confidential" or protected in a special password-protected folder. *Id.* at 28-29. By December 6, 2023, he had deleted anything that would be confidential under UAE law. *Id.* at 29. Thereafter, by late January, Defendant testified that he deleted everything related to Pliteq, such as public domain, collateral, or marketing information, except for anything that was publicly available like the public prosecution in Dubai and information from the Dubai police. *Id.* at 29-31. He clarified that these were thousands of files from six years of employment. *Id*. at 31. When asked how long it took him to delete records when he started in late November 2023, he testified he did not know but estimated it was maybe an hour or two. *Id.* at 33. Defendant explained that the deletion process was an ongoing process, but he could not provide the exact dates or the timing of the deletions, estimating that between late November 2023 and January 2024, he spent hours looking into his files and deleting them. *Id.* at 35. When shown the February 2, 2024 Dropbox email indicating that 8,105 files had been deleted, Defendant denied that this email stated the files were deleted in February 2024, but this email was merely a reminder that files were "recently" deleted and that he had until February 23, 2024 to restore them, which he did not do. *Id.* at 36-37, 155; ECF No. [96-24]. When asked whether he deleted any files on or about February 2, 2024, Defendant testified "no." ECF No. [77-2] at 37. Defendant was also asked about the December 6, 2023 letter from his attorney to Pliteq's lawyers, and he agreed that, as of that date, he no longer had any confidential or proprietary trade secret information and that the letter does not explain that he deleted the files but instead explains he no

longer has anything of concern[4]. *Id.* at 54-55. Defendant also denied that any of the Pliteq information was moved or copied anywhere else before he deleted it from his Dropbox folder, and he denied ever disclosing or transferring any portion of the 4.8 gigabyte file to anyone. *Id.* at 111, 138.

As far as data management practices, Defendant testified that he was responsible for those under the law of Dubai for PBM, a corporation incorporated under the laws of UAE, because as the sole manager, under the memorandum of incorporation, he is responsible for data and financials. ECF No. [77-2] at 42. But, Defendant agreed that he had no such responsibility for Pliteq, a Canadian company. *Id.* at 43.

Turning to the Confidentiality Agreement, Defendant agreed that he was bound by its terms based on the promise that he would receive shares under the laws of Canada and Ontario. *Id.* at 45. As for his compliance with the terms of the Confidentiality Agreement, Defendant denied ever disclosing any confidential or proprietary information and denied ever threatening to disclose such information. *Id.* at 45-46.

On the subject of the ownership of the laptop, Defendant disputes that the laptop belonged to Pliteq, explaining that he purchased the computer with his own credit card, it was delivered to his apartment, there was no transfer in ownership, the company never told him it was a company laptop, and he treated it like his personal laptop, using it for personal reasons and saving his personal banking information on it. *Id.* at 58-61. Defendant also testified about his employment-related dispute with Plaintiffs, explaining that he informed Plaintiffs that he had not been provided with his company shares, his commissions were not accurately calculated, and by the end of

[4] Consistent with this testimony, Defendant's Affidavit attached to the Response states that pursuant to a written request from Pliteq's counsel, "I have since deleted all data back ups and am in possession of no information belonging to Plaintiffs." ECF No. [72] at 23.

October 2023, Defendant believed Pliteq owed him about $150,000. *Id.* at 67-69. When asked about downloading the information in the Google Takeout file, Defendant explained that he planned to report the employment dispute about compensation discrepancies to the Ministry of Labor in Dubai, and to do so, he was required to provide proof of the discrepancy. *Id.* at 71. He noted that he downloaded the information through Google Takeout so that it would be transparent with the IT department. *Id.* at 72. Defendant admitted that he was able to download one of the 4.8 gigabyte files onto the Acer laptop, which then synced and uploaded to his Dropbox folder. *Id.* at 75-76. Also within his Drobox account was Defendant's personal data, such as family photos and videos, as well as his work for Pliteq when he created documents from scratch and templates. *Id.* at 96-97.

III. LEGAL STANDARDS

A. Spoliation of Evidence

Federal Rule of Civil Procedure 37(e)(2) provides:

> [i]f electronically stored information that should have been preserved in the anticipation 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:
>
> (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)(2).

Sanctions under Rule 37(e)(2) do not require a finding of prejudice on the non-spoliating party. *Skanska USA Civil Southeast, Inc. v. Bagelheads, Inc.*, 75 F.4th 1290, 1311 (11th Cir. 2023). No such finding is required "because the finding of intent required by the subdivision can support

not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position." *Id.* The level of intent required under this subdivision is "the equivalent of bad faith in other spoliation contexts," meaning "the destruction [of evidence] for the purpose of hiding adverse evidence." *Id*. (citations omitted, alterations in original). Before a court can dismiss a case under Rule 37(e)(2), a district court must find (1) the spoliating party acted with the intent required under the rule and (2) that "lesser sanctions are insufficient to address the loss of the ESI." *Jones v. Riot Hospitality Group LLC*, 95 F.4th 730, 735 (9th Cir. 2024).

B. Preliminary Injunction Standards

"A preliminary injunction is an 'extraordinary and drastic remedy.'" *Citizens for Police Accountability Political Committee v. Browning*, 572 F.3d 1213, 1216 (11th Cir. 2009) (quoting *McDonald's Corp. v. Robertson*, 147 F.3d 1301, 1306 (11th Cir. 1998)). "To secure an injunction, a party must prove four elements: (1) a substantial likelihood of success on the merits; (2) irreparable injury absent an injunction; (3) the injury outweighs whatever damage an injunction may cause the opposing party; and (4) an injunction is not adverse to the public interest." *Id.* The moving party must clearly carry the burden of persuasion as to each of these four factors. *Zardui-Quintana v. Richard*, 768 F.2d 1213, 1216 (11th Cir. 1985) (quoting *United States v. Jefferson County*, 720 F.2d 1511, 1519 (11th Cir. 1983)). The first prong of the test is the most important one and requires only a showing of likely or probable success, not certain success. *EyePartner, Inc. v. Kor Media Group LLC*, No. 13-CV-10072, 2013 WL 3733434, *2 (S.D. Fla. July 15, 2013) (quoting *Schiavo ex rel. Schindler v. Schiavo*, 403 F.3d 1223, 1232 (11th Cir. 2005)).

IV. DISCUSSION

A. Motion for Sanctions

As a preliminary matter, Plaintiffs ask the Court to impose sanctions against Defendant for spoliation of evidence relating to Defendant's deletion of the downloaded files from his Dropbox folder. In doing so, Plaintiffs request the most severe form of sanctions — default judgment. Alternatively, if no default judgment is entered, Plaintiffs request an adverse jury instruction or a presumption that the lost information was unfavorable to Defendant. In response, Defendant did not dispute that he deleted the files, but he instead explained he did so in response to letters he received from Plaintiffs' counsel demanding that he delete any trade secret and confidential information in his possession.

To decide this issue, the Court must first determine whether, when deleting the data and information from his Dropbox account, Defendant "acted with the intent to deprive another party of the information's use in the litigation." Fed. R. Civ. P. 37(e)(2). The Court notes that it need not find any prejudice to Plaintiffs to impose sanctions under Rule 37(e)(2), but it must find that Defendant acted with "the equivalent of bad faith in other spoliation contexts," meaning that he destroyed the evidence "for the purpose of hiding adverse evidence." *Skanska USA Civil Southeast, Inc.*, 75 F. 4th at 1311.

In this case, the Court does not find that Defendant acted in bad faith when he deleted the files from his Dropbox folder. Plaintiffs' spoliation argument hinges on the mass deletion of files on January 24, 2024 and February 2, 2024. He points to Exhibit 24, *see* ECF No. [96-24], as evidence that Defendant deleted 8,104 files from Dropbox on January 24, 2024, which is one week after he had notice of this lawsuit. Significantly, Exhibit 24 merely states that a file labeled "producttestreports.xlsx" and "8,104 files" was deleted without any further elaboration. Thus,

Plaintiffs were unable to show that Pliteq files were deleted from his Dropbox account on January 24, 2024, much less that Defendant deleted the files containing the trade secrets on this date. *See* ECF No. [100] at 180-182. As for the February 2, 2024 deletion of files, Plaintiffs provided no information whatsoever as to what these files contained. *Id.* Importantly, Mr. Ayala's forensic examination revealed that Defendant's Dropbox folder was replete with other files unrelated to Plaintiffs' business, which is consistent with Defendant's deposition testimony. For example, Defendant's Dropbox contained a folder with 44.2 gigabytes of data called "Camera Uploads," 72 gigabytes in a folder called "Archives," 1.1 gigabytes in a folder called "Personal," 42.2 gigabytes in a folder called "Photos," and 6.4 gigabytes in a folder called "Quicken," among others. *See* ECF No. [78-1] at 18. In addition, Plaintiff had a "Work" folder with multiple subfolders consisting of: "BYS" (560 MBs), "Dubai South" (6.0 MBs), "Expenses" (6.0 MBs), "IDH" (1.4 GBs), "Jobs" (46.3 MBs), "Pliteq" (33.0 GBs), "Resources" (95 MBs), "TIME" (7.3 GBs), and "Travel" (1.8 GBs). Thus, it appears that even in the "Work" folder, there were routine work-related documents saved. Despite the large number of files deleted after Defendant had notice of this lawsuit, it remains unclear whether the deletions on these days contained any Pliteq materials at all, as opposed to other personal matters Defendant saved on his Dropbox account, and it remains equally uncertain whether the six trade secret files that were misappropriated and identified during the Hearing were among the documents deleted on these two dates.

What's more is that on both January 24, 2024 and February 2, 2024 — the days on which the larger quantity of file deletions occurred — thousands of files were also added to the Dropbox folder. *See* ECF No. [78-1] at 27. Specifically, on January 24, 2024, Defendant added 16,221 files but deleted 24,318 files, and on February 2, 2024, Defendant added 26,445 files but only deleted 24,089 (meaning 2,356 more files were added than deleted that day). *Id.* The Court has

no way of knowing the content of any of these files or whether Defendant simply deleted most, if not all, of the files he had added on that same day. To determine that Defendant acted in bad faith when deleting these files, it is imperative that the Court conclude that he destroyed the evidence to hide it from Plaintiffs. Based on this record, the Court can only guess what Defendant deleted, making it impossible to determine that such evidence was, in fact, adverse to his position and deleted for the purpose of keeping it from Plaintiffs.

Despite this, it was undisputed that Defendant deleted the confidential files and other Pliteq files at some point prior to the commencement of discovery. Defendant has provided a logical explanation as to why and when he deleted these files. According to Defendant, he began deleting the files following his receipt of repeated instructions from Plaintiffs and its counsel asking him to delete confidential information. Starting on November 3, 2023, Plaintiffs' counsel sent a letter "request[ing] that the confidential information that you [referring to Defendant] have downloaded or stored as a back-up be deleted immediately" and suggesting that potential criminal consequences may follow from a failure to comply. ECF No. [96-17] at 3. Thereafter, on November 21, 2023, Plaintiffs terminated Defendant and, in that letter, advised him that he is, "[u]nder no condition," to "reproduce and/or retain a copy of any Company property," including all ESI that he downloaded without Plaintiffs' approval from the October 28, 2023 Google Takeout request. *See* ECF No. [96-20] at 2.

Consistent with these two notices, Defendant testified that, after he received a legal notice from PBM's counsel asking him to delete all Pliteq documents, he began to delete them, starting with confidential information and eventually deleting all other Pliteq documents. ECF No. [77-2] at 23. When he searched for confidential documents for deletion, Defendant explained that there were a few documents for business planning or involving financials that were marked as

"confidential," so he deleted those. *Id.* at 28. He estimated that he started deleting information marked as "confidential" or protected in a special password-protected folder in late November 2023. *Id.* at 28-29. The November 3 and 21, 2023 letters Defendant received support his timeline and explanation. According to Defendant, by December 6, 2023, he had deleted anything that was confidential under UAE law, which was consistent with the letter his attorneys sent to Pliteq on that date. *Id.* at 29.

A review of Mr. Ayala's forensic report corroborates Defendant's deposition testimony that he deleted files in late November 2023. *See* ECF No. [78-1] at 26. He deleted two files on November 20, 2023, six files on November 22, 2023, two files on November 23, 2023, 810 files on November 26, 2023, four files on November 27, 2023, and one file on November 28, 2023. *Id.* By contrast, during the Hearing, Plaintiffs only presented evidence that Defendant downloaded six files containing trade secret information (Exhibits 29, 30, 31, 32, 34, and 35), but they did not present any evidence to dispute Defendant's testimony that he first deleted the trade secret information at the direction of his counsel after Plaintiffs demanded that he do so. And, Mr. Ayala's expert report confirms that Defendant deleted far in excess of six files in late November 2023, making Defendant's explanation that he deleted all confidential information by December 6, 2023 entirely plausible.

Mr. Ayala's expert report also reveals that Defendant continued to delete files, albeit relatively few, on an almost daily basis throughout the month of December 2023. *Id.* Starting in January 2024, Defendant continued deleting files almost daily with a greater number of files deleted on January 3, 2024 (194 files) and January 14, 2024 (1,754 files) — all of which occurred prior to Defendant having any notice of this lawsuit. *Id.* at 26-27. Again, this pattern supports

Defendant's explanation that he continued deleting Plaintiffs' files throughout January 2024 in response to the letters he received from Plaintiffs.

In support of their argument, Plaintiffs argued that Defendant changed his story and testified inconsistently with the evidence. For the reasons explained above, the Court disagrees, but it recognizes that Defendant incorrectly denied deleting the last large batch of documents, consisting of 24,089 files, on February 2, 2024. *Id.* at 27. During his deposition, he testified that he deleted all of Plaintiffs' files between late November 2023 and January 2024, but Mr. Ayala's report reveals that this large deletion occurred a few days later (assuming this was a deletion of Pliteq information as opposed to other information saved on his Dropbox account). The Court does not find this mistake to be an intentional lack of candor. This is because testimony at a deposition is not a memory test, and witnesses often need assistance refreshing recollections with precise dates. To that point, Defendant explained that the "dates and timings are not exact because [he] cannot recall exactly the time that [he] did that." *See* ECF No. [77-2] at 86. And, his recollection was not that far off the mark as he testified he completed his deletions of Pliteq documents in January, and February 2 is a mere two days after the end of January. The Court notes that during the deposition, Defendant did not have the benefit of any documents to refresh his recollection on the precise dates of the deletions.[5] And, given that Mr. Ayala's report had not been disclosed at the time of the deposition, Defendant could not have tailored his testimony to Mr. Ayala's report; yet, his testimony and recollection of events are generally consistent with these forensic findings.

In sum, the Court finds that Defendant did not engage in bad faith when deleting the files in his Dropbox folder, meaning he did not delete the files with the purpose of hiding adverse

[5] Mr. Ayala's report was produced five days after Defendant's June 21, 2024 deposition.

evidence from Plaintiffs. As a result, the intent element of Rule 37(e)(2) has not been satisfied, making sanctions for spoliation against Defendant improper. Plaintiff's Oral Motion for Sanctions is, therefore, **DENIED**.

B. Motion for Preliminary Injunction

a. Whether There is a Substantial Likelihood of Success on the Merits

i. Misappropriation of Trade Secrets pursuant to 18 U.S.C. § 1836 (Count I)

Count I alleges that Defendant violated the DTSA pursuant to 18 U.S.C. § 1836. The DTSA authorizes courts to grant injunctions in the event of "actual or threatened misappropriation" of trade secrets. *Hayes Healthcare Servs. LLC v. Meacham*, No. 19-CV-60112-COHN, 2019 WL 2637053, at *3 (S.D. Fla. Feb. 1, 2019). "The party claiming trade secret protection has the burden to show how the information qualifies as a trade secret." *Pals Grp., Inc. v. Quiskeya Trading Corp.*, No. 16-23905-CIV, 2017 WL 532299, at *3 (S.D. Fla. Feb. 9, 2017) (citing *Hennegan Co. v. Arriola*, 855 F. Supp. 2d 1354, 1360 (S.D. Fla. 2012)). A trade secret" is defined as "all forms and types of financial, business, scientific, technical, economic, or engineering information," provided that:

> (A) The owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

18 U.S.C. § 1839(3). Finally, the DTSA defines the term "misappropriation" as the "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means." 18 U.S.C. § 1839(5)(A). The phrase "improper means," in turn,

includes "theft, bribery, misrepresentations, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." 18 U.S.C. § 1839(6).

Here, the Court has little difficulty concluding that the identified documents consisting of Exhibits 29, 30, 31, 32, 34, and 35 are trade secrets under the DTSA. Exhibit 29 contains information about the volume of products Pliteq can produce in its plant during any given period by product line, information about capital expenditures needed to meet these volumes, information about new, unreleased products, including product recipes, and Plaintiffs' projected revenue for one of their regions. *See* ECF No. [100] at 135-137. As for Exhibit 30, this is a listing of Pliteq consultants and customers that specify Pliteq products in construction projects, listed by firm and the individuals at those firms. *Id.* at 137-139. Regarding Exhibit 31, this is a product roadmap to reach $140 million in revenue, which includes information about Pliteq's new, unreleased products and forms part of its research and development. *Id.* at 140. Next, Exhibit 32 contains a financial forecast for the Middle East and North Africa region, including product cost information for each individual product. *Id.* Exhibit 34 sets forth Pliteq's orders to ship as of October 2023, including revenue booked to date, future orders, customer names, project names, pricing, quantities, and expected shipment dates. *Id.* at 142. Finally, Exhibit 35 is a testing report that compares Pliteq's products to a competitor's products. *Id.* at 143-144. Thus, these documents are "forms and types of financial, business, scientific, technical, economic, [and] engineering information." 18 U.S.C. § 1839(3). And, Mr. Pulcine provided unrebutted testimony that Plaintiffs derive independent economic value from this information, such as their pricing strategies and recipes, not being generally known. Although Defendant's Response argued that Plaintiffs failed to identify the trade secrets at issue with sufficient particularity, *see* ECF No. [72] at 14-14, Defendant stipulated at the Hearing that these exhibits indeed qualified as trade secrets, *see* ECF No. [100] at 215 ("For the

purposes of today, they're trade secrets"); 217 ("We're not going to contest whether those are trade secrets themselves.").

Finally, to determine whether the documents satisfy the definition of "trade secret" under the DTSA, the Court must determine whether Plaintiffs have taken reasonable steps to keep this information a secret. In support of their verified Motion for Preliminary Injunction, Plaintiffs explained that, in addition to requiring Defendant to sign the Confidentiality Agreement that prohibited him from using confidential company information, Plaintiffs also undertook efforts to maintain the secrecy of the information, such as requiring passwords to access their cloud-based servers, giving limited employees access to NetSuite (their proprietary customer information database), and EchoOne (their database of testing information for their products), and enforcing strong passwords and two-factor authentication. *See* ECF No. [50] at 9. In addition, Plaintiffs employ "corporate antivirus and anti-phishing systems" "to prevent unauthorized access," and their "IT personnel are regularly engaged to audit vulnerabilities" in their computer systems. *Id.* Regarding physical access, the use of keycard access restricts Plaintiffs' offices, and upon termination of an employee's employment relationship, "Plaintiffs promptly terminate departing employees' access to their e-mail accounts, customer and testing databases, and work-related software applications." *Id.* At the Hearing, the Court asked Defendant whether it disputed or had any evidence to dispute that Plaintiffs took reasonable measures to keep their information secret. *See* ECF No. [100] at 238-239 ("what evidence, if any, is there in the record to suggest that they weren't taking those measures to try to safeguard their own information?"). Defendant admitted

he had no evidence to contradict that information. *Id.* Based on the foregoing, the Court finds that Exhibits 29, 30, 31, 32, 34, and 35 meet the definition of "trade secrets."

The final issue the Court must address is whether Defendant misappropriated these "trade secrets." Plaintiffs heavily rely on two cases to support their request for a preliminary injunction: *Meachum*, 2019 WL 2637053 at *4, and *Hayes Medical Staffing, LLC v. Eichelberg*, No. 23-CV-60748-GAYLES, 2024 WL 670440, *1 (S.D. Fla. Jan. 23, 2024). In *Meachum*, the district court found there was evidence of misappropriation because the defendant "surreptitiously" retained certain trade secret information in violation of his employment agreement with the intent to use the information for his personal benefit. 2019 WL 2637053 at *4. In *Eichelberg*, the district court found misappropriation by one defendant but not by the other. 2024 WL 670440 at *8. Although both employees retained the trade secrets after they left their employment, one employee intended to misappropriate the trade secret information as evidenced by the timing of the emails sending herself the information (two days before her resignation), how she sent the emails to herself (through a blind copy), and her efforts to delete the evidence of her misappropriation. *Id.* The district court determined the evidence did not support the claim that the other employee misappropriated the trade secrets because he had emailed himself the information years earlier and some of the emails were titled "Backups," which supported his claim that he sent these emails in the event the servers crashed. *Id.*

Here, the evidence is a slightly closer call on the subject of misappropriation. This was not the first time that Defendant had downloaded Pliteq's information onto his Acer laptop and Dropbox folder. Mr. Ayala's expert report reveals that his Dropbox "Work" folder contained 44.1 gigabytes of data. *See* ECF No. [78-1] at 18. The download at issue was only 4.8 gigabytes of data; therefore, another 39 gigabytes of data were previously transferred from Plaintiffs' computer

system to Defendant's Dropbox folder. And, the Dropbox subfolder structure reveals that each subfolder within the "Work" folder was modified prior to the October 28, 2023 download, meaning that information had been saved into the subfolders on prior occasions, such as on April 4, 2023, September 18, 2023, and October 11, 2023. *Id.* at 19. Even the "Pliteq" folder, which contained 33 gigabytes of data, had nearly 28 additional gigabytes of data beyond what Defendant downloaded on October 28, 2023. Thus, this evidence that Defendant had downloaded Pliteq information on prior occasions corroborates Defendant's position that he previously downloaded information, which also makes sense if he was travelling for work.[6] And, unlike in *Meacham* and *Eichelberg*, Defendant did not surreptitiously download the information by sending himself blind copy emails and deleting the evidence or uploading the information onto a USB. Defendant used a Google Takeout request to download the information, knowing this would have been visible to the IT department. The foregoing evidence weighs against misappropriation.

With that said, the timing of this download, the content of the download, and the purpose of the download are all problematic and are strong evidence of misappropriation. Regarding the timing, Defendant downloaded a significant amount of data, including multiple trade secret files, days after he sent an email to Plaintiffs' finance director complaining about Plaintiffs failure to deliver his stock options and failure to pay him his full commissions. By Defendant's own admission, he did not download this information for work-related reasons, but he did so to present a labor dispute against Plaintiffs. In short, he wanted proof to back up his employment claim. This download was not related to his ongoing work for Pliteq. And, there is no indication that his prior downloads of Pliteq information ever contained Plaintiffs' trade secret information as opposed to

[6] The Court notes that, according to Mr. Pulcine, if this were a company-issued laptop, there was no issue with Defendant downloading the information onto the laptop. At this juncture, the Court need not decide the issue of who owned the laptop as there is other evidence of misappropriation regardless of whether Plaintiffs or Defendant owned the computer.

other routine work-related matters. Finally, Defendant contends that Plaintiffs knew about his prior download of Pliteq information, but Defendant was unable to point the Court to any evidence in the record that corroborates Defendant's argument that Plaintiffs knew he was downloading company information onto the computer and his personal Dropbox. *See* ECF No. [100] at 234-237. Here, the timing of the download, the selection of confidential, trade secret information among the information in the download, and Defendant's stated purpose in using the downloaded files (not for any work-related purpose), all support Plaintiffs' claim that Defendant misappropriated the information under the DTSA. Based on the foregoing, the Court finds there is a substantial likelihood that Plaintiffs will succeed on the merits of their DTSA claim.

ii. Unfair competition (Count II)

In their briefing, the Parties have briefed the law of unfair competition under the assumption that Florida common law will apply. Even though the Court ordered supplemental briefing on the impact of various claims added to the Amended Complaint that sounded in common law, neither Party raised choice-of-law issues, which must be addressed as a threshold matter. Rather than require a third round of briefing, the Court addresses the choice-of-law issue *sua sponte. See Rossi v. Pocono Point, LLC*, No. 08-CV-750-ORL-28-KRS, 2009 WL 435064, at *4 (M.D. Fla. Feb. 20, 2009) (raising choice-of-law issue *sua sponte*). "A federal district court sitting in diversity must apply the choice of law rules of the forum state." *Arndt v. Twenty-One Eighty-five, LLC*, 448 F. Supp. 3d 1310, 1315 (S.D. Fla. 2020) (alteration adopted) (quoting *Clanton v. Inter.Net Glob., L.L.C.*, 435 F.3d 1319, 1323 (11th Cir. 2006)); *see also Seven Seas Int'l, LLC v. Frigopesca, C.A.*, 616 F. Supp. 3d 1323, 1328 (S.D. Fla. 2022). The same is true when a federal court hears state law claims under its supplemental jurisdiction. *See, e.g.*, *Palm Beach Golf Ctr.-Boca, Inc. v. John G. Sarris, D.D.S., P.A.*, 781 F.3d 1245, 1260 (11th Cir. 2015).

The first step in conducting a choice-of-law analysis requires a determination of which sovereigns have an interest in applying their laws to the controversy. *See Pycsa Panama, S.A. v. Tensar Earth Techs., Inc.*, 625 F. Supp. 2d 1198, 1218–19 (S.D. Fla. 2008), *aff'd*, 329 F. Appx 257 (11th Cir. 2009) (citing *Judge v. Am. Motors Corp.,* 908 F.2d 1565, 1568 (11th Cir. 1990)). After the court identifies the interested sovereigns, it "must consider the threshold issue of whether there is a 'true conflict' among the jurisdictions with an interest in a particular issue or merely a 'false conflict.'" *Id.* (quoting *Tune v. Philip Morris, Inc.,* 766 So. 2d 350, 352 (Fla. 2d DCA 2000)). A "false conflict" can arise in three different scenarios: if "the laws of the interested jurisdictions are: (1) the same; (2) different but would produce the same outcome under the facts of the case; or, (3) when the policies of one jurisdiction would be furthered by the application of its laws while the policies of the other jurisdiction would not be advanced by the application of its laws." *Id.* (citing *Tune,* 766 So.2d at 352). A true conflict, however, arises when "two or more states have a legitimate interest in a particular set of facts in litigation and the laws of those states differ or would produce a different result." *Id.* (quoting *Walker v. Paradise Hotel, Ltd.,* No. 01–3564, 2003 WL 21361662, *2–3, 2003 U.S. Dist. LEXIS 25660, at *5 (S.D. Fla. April 25, 2003)). If a false conflict exists, the Court applies the law of the forum state. *Id.* In the event of a true conflict, the court must then apply the significant relationships test under the Restatement (Second) of Conflicts of Laws § 145. *Id.*

Here, the Court finds that three sovereigns have an interest in the application of their law: Canada, the UAE, and Florida. Specifically, Canada has an interest because Pliteq is a Canadian corporation and the production of the products at issue takes place in Toronto. The UAE likewise has an interest as Defendant resides in Dubai, PBM is organized under the laws of the UAE, and the alleged misappropriations of trade secrets occurred in Dubai. Finally, Florida as the forum

state has an interest in having its law applied, but it has the fewest contacts with the issues in this litigation. Although the Parties have briefed Florida law on unfair competition, the Parties have not addressed this issue under Canadian law or UAE law. As a result, the Court is unable to determine if there is a false conflict of interest, which would allow it to apply Florida common law, or whether there is a true conflict, requiring a conflict-of-law analysis to determine which law should apply. To the extent the Parties have opted to waive the application of foreign law, neither Party has affirmatively stated as much in any of its briefing to date on the Motion. *See Sun Life Assurance Co. of Canada v. Imperial Premium Fin., LLC*, 904 F.3d 1197, 1208–09 (11th Cir. 2018) (explaining that a party's reliance on and the Court's application of foreign law may be waived). Without this information, the Court cannot analyze the likelihood of success on the merits of Count II of the Amended Complaint. But in any event, the Court has found that Plaintiffs have proven a substantial likelihood of success on the merits of Count I, so it will move on to the next step of the preliminary injunction analysis regardless.

iii. Injunctive Relief (Count III)

Count III simply seeks injunctive relief against Defendant. *See* ECF No. [120] at 15-16. Because the Court addresses each element of a preliminary injunction throughout this Order, it does not rehash the likelihood of success on the merits of injunctive relief here.

iv. Breach of Employment Contract (Count IV)

Count IV is premised upon Defendant's alleged breach of his employment contract with PBM. *See* ECF [120] at ¶21 (attaching the employment agreement as Exhibit A). Paragraph 15 of the employment contract, entitled "Governing law and dispute resolution," states: "This Contract and any dispute, difference, proceedings or claim of whatever nature arising out of or in connection with this Contract shall be governed by the laws of Dubai." *See* ECF No. [121] at ¶15.

As explained above, the Court gave the Parties an opportunity to brief the impact of this new claim in the Amended Complaint on Plaintiffs' request for injunctive relief and asked them to specifically address the likelihood of success on the merits of this claim. Yet, neither Party noted that the law of Dubai governs this claim nor did they provide the Court with any authorities under Dubai law to assist the Court with its analysis of this claim.

"Under Florida's choice-of-law rules, it is well-settled that Florida courts are obligated to enforce choice-of-law provisions unless a showing is made that the law of the chosen forum contravenes strong public policy or that the clause is otherwise unreasonable or unjust." *See Arndt*, 448 F. Supp. 3d at 1315 (quotation marks omitted). A "choice of law provision in a contract is presumed valid until it is proved invalid," and the "party who seeks to prove such a provision invalid because it violates public policy bears the burden of proof." *Id.* (quotation marks omitted). To the extent the Parties have opted to waive the enforcement of the choice-of-law provision, neither Party has affirmatively stated as much in any of its briefing. *See Sun Life Assurance Co. of Canada, LLC*, 904 F.3d at 1208–09. Thus, absent briefing on Dubai contract law and evidence that the choice-of-law provision is invalid or any indication that its enforcement is waived, the Court declines to decide the likelihood of success on the merits on this claim.

v. Breach of Confidentiality Agreement (Count V)[7]

Plaintiffs' request fares no better for Count V of the Amended Complaint. In this Count, Plaintiffs seek to enforce the Confidentiality Agreement signed between Pliteq and Defendant.

[7] According to Plaintiffs' Supplemental Brief, Plaintiffs are not seeking injunctive relief based on the newly added Count VII for breach of fiduciary duty, *see* ECF No. [127] at 2, so the Court need not analyze the likelihood of success of this claim. However, the Court flags that this issue will require a choice-of-law analysis, unless the Parties opt to waive the application of foreign law, and if a true conflict exists, the Court must conduct a choice-of-law analysis under the significant relationship test. *See Trumpet Vine Invs., N.V. v. Union Cap. Partners I, Inc.*, 92 F.3d 1110, 1116 (11th Cir. 1996) (finding that breach of fiduciary duty is more akin to fraud and was, therefore, properly analyzed as a fraud claim under § 145 of the Restatement (Second) of Conflicts rather than a personal injury claim).

See ECF No. [120] at ¶88 (attaching the Confidentiality Agreement as Exhibit B). Paragraph 16 of this agreement, labeled "Governing Law and Covenant to Jurisdiction," states: "This Agreement shall be governed by and interpreted under the laws of the Province of Ontario and the federal laws of Canada applicable therein." ECF No. [121] at ¶16. Again, the Court asked the Parties to brief the impact of the newly added claims in the Amended Complaint on the request for injunctive relief. It appears that neither Party realized that the laws of Ontario and the federal laws of Canada apply to any interpretation of this agreement. Once again, the Court will not speculate as to what the laws of Ontario say or what federal Canadian law says on the topic or which of the two Canadian laws (Ontarian or Canadian federal law) govern over the claim in Count V. To the extent the Parties have opted to waive the enforcement of the choice-of-law provision, neither Party has affirmatively stated as much in any of its briefing. *See Sun Life Assurance Co. of Canada, LLC*, 904 F.3d at 1208–09. Without a framework to analyze the law that applies to Count V, this Court cannot analyze the likelihood of success of this claim.

vi. Conversion (Count VII)

Much like Count II, the Court must conduct a choice-of-law analysis as it finds that three sovereigns have an interest in the matter involving the alleged conversion of the laptop: (1) Canada as Pliteq, a Canadian corporation, alleges it owns the laptop; (2) the UAE, as the Defendant, a Dubai resident, claims he is the rightful owner of the laptop;[8] and (3) Florida, as the forum state. Yet again, the Parties' Supplemental Briefing failed to provide the Court with any authorities discussing the tort of conversion under the laws of the UAE or Canada, its elements, or its viability. They only addressed Florida conversion law. Without such information, the Court cannot

[8] The Court further notes that Dubai launched a criminal investigation and prosecution involving the theft of the laptop, so it certainly has an interest in applying its laws to this claim for relief.

determine whether a true conflict exists, which requires the application of the significant relationship test, or whether there is a false conflict, which allows the Court to apply Florida law. To the extent the Parties have opted to waive the enforcement of the choice-of-law provision, neither Party has affirmatively stated as much in any of its briefing. *See Sun Life Assurance Co. of Canada, LLC*, 904 F.3d at 1208–09. The Court, therefore, declines to reach the merits of the likelihood of success of Count VII.

b. Whether Plaintiffs Will Suffer an Irreparable Injury Without an Injunction

When analyzing this second prong, the key word here is "irreparable." *See Rey v. Guy Gannett Publishing Co.*, 766 F. Supp. 1142, 1147 (S.D. Fla. 1991) (quoting *USA v. Jefferson County*, 720 F.2d 1511 (11th Cir. 1983)). "The possibility [that] adequate compensatory or other corrective relief will be available at a later date, in the ordinary course of litigation, weighs heavily against a claim of irreparable harm." *Id.* at 1148. To satisfy this element, it is well settled that a plaintiff is required to "show potential harm which cannot be redressed by a legal or equitable remedy following a trial" and that the preliminary injunction is "the only way of protecting the Plaintiffs from harm." *Id.* (citing *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797 (3d Cir. 1989)). In addition, Plaintiffs are required to show that irreparable harm is likely, and not merely possible, without the requested injunctive relief. *See Hoop Culture, Inc. v. GAP Inc.*, 648 F. App'x 981, 985 (11th Cir. 2016). They also must show that the irreparable harm is *imminent. See Wreal, LLC v. Amazon.com, Inc.*, 840 F.3d 1244, 1248 (11th Cir. 2016).

In support of injunctive relief, Plaintiff first argues that the harm of use or disclosure of its trade secrets is irreparable because, under the Confidentiality Agreement, Defendant agreed that:

> any breach or threatened breach by [Defendant] could result in irreparable harm to the Company which may not reasonably or adequately be compensated in damages and that, in the event of any such breach or threatened breach, the Company shall

> be entitled to equitable relief, including but not limited to temporary, preliminary and permanent injunctive relief enforcing the specific performance by the [Defendant] or enjoined [sic] or restraining the [Defendant] from any violation or threatened violation of the terms of this Agreement.

See ECF No. [50] at 18 (alterations in original). And the Confidentiality Agreement required that Defendant return all confidential information upon termination of the employment or contractual relationship. *Id.* According to Plaintiffs, Defendant was terminated (and was therefore required to return the information), but he refused to return it or confirm that he would not disclose it and such threat of disclosure to "Plaintiffs' US-based competitors and consultants, for purposes of financial gain to Defendant and retaliatory harm to Plaintiffs" creates irreparable harm. *Id.*

Defendant, for his part, argues that Plaintiffs' unexplained delay in seeking injunctive relief undermines a finding of irreparable harm as they delayed approximately six months after filing the Complaint to file the Motion. *See* ECF No. [72] at 8-9. Next, Defendant takes the position that Plaintiffs' claims of irreparable harm are speculative and unsupported by the record. *Id.* at 9-10. Specifically, Defendant argues that his motivation to sell Plaintiffs' trade secrets to their U.S.-based competitors has no basis in fact when Defendant worked exclusively for PBM and focused on business relationships solely in the Middle East, North Africa, and Asia Pacific regions, but he never conducted any business in the United States while employed for PBM. *Id.* at 10. Defendant further argues there is no indication that Defendant ever disclosed any of Plaintiffs' trade secrets, and more importantly, Defendant never threatened to disclose the trade secrets to anyone, including anyone in the United States, and he deleted the remaining files in his possession. *Id.* at 11. Finally, Defendant cites to case law to support his position that the language in the Confidentiality Agreement does not entitle Plaintiffs to a finding of irreparable harm. *Id.* at 12.

In their Reply, Plaintiffs argue that they proceeded diligently in seeking injunctive relief in this matter, so this factor should not weigh against a finding of irreparable harm. *See* ECF No.

[82] at 2-3. As to the imminence of the harm, Plaintiffs argued that the "mere risk of disclosure from a defendant's inability to conclusively establish that he returned all confidential information in its possession is sufficient to show irreparable harm," citing to two decisions from the Southern District of Florida. *Id.* at 4. In the Reply, however, Plaintiffs did not respond to Defendant's argument that, under the case law, a confidentiality agreement, standing alone, does not entitle them to a finding of irreparable harm. The Court will address each of these arguments in turn.

i. Whether a Presumption of Irreparable Harm Applies Under the DTSA

As a threshold matter, the parties dispute whether a presumption of irreparable harm exists for injuries stemming from misappropriated trade secrets. *Compare* ECF No. [50] at 18 ("Because injuries stemming from misappropriated trade secrets are 'properly characterized as irreparable because an inadequate remedy at law is presumed,' the first two factors are satisfied.") *with* ECF No. [72] at 8 ("For claims brought pursuant to the Defendant Trade Secrets Act ('DTSA"), there is no presumption of irreparable harm in favor of the movant."). The Court first considers whether a presumption of irreparable harm exists under the DTSA and finds there is none. Although Florida law contains "a statutory presumption of irreparable injury stemming from the violation of a valid restrictive covenant," the DTSA does not contain a similar statutory presumption and the Court declines to read a non-existent presumption into a statute. *See Castellano Cosm. Surgery Ctr., P.A. v. Rashae Doyle, P.A.*, No. 21-CV-1088-KKM-CPT, 2021 WL 3188432, at *8 (M.D. Fla. July 28, 2021) (explaining that the DTSA does not contain a statutory presumption of irreparable harm). The cases on which Plaintiffs rely for the presumption do not analyze whether that presumption exists under the DTSA's statutory scheme and instead simply rely on Florida law for that presumption. *See Corp. Ins. Advisors, LLC v. Addeo*, No. 21-CV-61769, 2021 WL 6622154, at *12 (S.D. Fla. Dec. 8, 2021), *report and recommendation adopted*, No. 21-CV-61769,

2022 WL 204689 (S.D. Fla. Jan. 24, 2022) ("Additionally, *Florida* presumes irreparable injury in cases such as these involving restrictive covenants and misappropriated trade secrets."); *JetSmarter Inc. v. Benson*, No. 17-62541-CIV, 2018 WL 2709864, at *4 (S.D. Fla. Apr. 6, 2018), *report and recommendation adopted*, No. 17-62541-CIV, 2018 WL 2688774, at *4 n.8 (S.D. Fla. Apr. 26, 2018) (explaining that the injunctive relief was sought only under Florida's Uniform Trade Secrets Act and a Stock Restriction Agreement but was not based on the DTSA). Thus, the Court below will analyze whether irreparable harm applies to the DTSA claim without any presumption of irreparable harm.

ii. Whether a Presumption of Irreparable Harm for Breach of a Restrictive Covenant Applies in a Diversity Case

As for Plaintiffs' claims for a violation of a restrictive covenant in Counts IV and V, as explained above, it is unclear what law would apply to this claim as the contracts have choice-of-law provisions. But even if the choice-of-law provisions were unenforceable or enforcement thereof were waived and Florida law governed (and there was a substantial likelihood of success on the merits as to these claims), Florida's presumption does not apply in preliminary injunction proceedings under diversity jurisdiction. In a lengthy conflict-of-law analysis, Chief Judge William Pryor explained that "the Florida standard for obtaining a preliminary injunction is a matter of procedure, not of substance. Federal courts must apply the federal standard in cases involving Florida law. And under the federal standard, a plaintiff must prove irreparable harm without the presumptions afforded by Florida law." *Vital Pharmaceuticals, Inc. v. Alfieri*, 23 F.4th 1282, 1299 (11th Cir. 2022) (Pryor, C.J., concurring). And since then, district courts in this Circuit have declined to find the presumption applies to preliminary injunction proceedings in federal court governed by Florida substantive law. *See Pro Servs., Inc. v. BHS Corrugated - N. Am., Inc.*, No. 24-CV-60318-DAMIAN, 2024 WL 4290765, at *6 (S.D. Fla. July 5, 2024) (declining to apply

irreparable harm presumption in diversity case in which Florida law applied); *Eichelberg*, 2024 WL 670440 at *10 n.11 (finding that presumption of irreparable harm under Fla. Stat. § 542.335(1)(j) did not apply and explaining that "courts in the Eleventh Circuit have recently adopted Chief Judge Pryor's reasoning that a federal court should not apply state law presumptions when deciding whether to grant a preliminary injunction"); *Head Kandy, LLC v. McNeill*, No. 23-CV-60345, 2023 WL 6309985, at *16 (S.D. Fla. Sept. 12, 2023), *report and recommendation adopted*, No. 23-CV-60345-RAR, 2023 WL 7318907 (S.D. Fla. Nov. 7, 2023) ("I decline to utilize this presumption in light of Chief Judge Pryor's reasoning that a federal court should not apply state law presumptions when deciding whether to grant a preliminary injunction — a procedural issue."). Even if the Court determined that the application of Florida law to Counts IV and V were appropriate and that there was a substantial likelihood of success on the merits on these claims, the presumption of irreparable harm would still not apply to Plaintiffs' claims, and as a result, Plaintiffs must prove irreparable harm that is imminent, *Wreal*, 840 F.3d at 1248, and likely, and not merely possible, without the requested injunctive relief, *Hoop Culture*, 648 F. App'x at 985.

iii. Whether the Delay in Seeking Injunctive Relief Weighs Against a Finding of Irreparable Harm

Addressing Defendant's first argument — the delay in seeking injunctive relief, the Eleventh Circuit has explained that, "the very idea of a *preliminary* injunction is premised on the need for speedy and urgent action to protect a plaintiff's rights before a case can be resolved on its merits." *Wreal*, 840 F.3d at 1248. Thus, "[a] delay in seeking a preliminary injunction of even only a few months — though not necessarily fatal — militates against a finding of irreparable harm." *Id.* This is because a preliminary injunction requires showing "imminent" irreparable harm. *Id.* (citations omitted). Other circuit courts and district courts within this Circuit have repeatedly found that "a party's failure to act with speed or urgency in moving for a preliminary

injunction necessarily undermines a finding of irreparable harm." *Id.* Logically, "a plaintiff concerned about a harm truly believed to be irreparable would and should act swiftly to protect itself." *See Pals Grp., Inc.*, 2017 WL 532299 at *5–6 (finding no irreparable harm and denying injunctive relief when the plaintiff "sat on its rights for three months" after waiting to seek a preliminary injunction three months after filing the Complaint); *see also Sprint Commc'ns, Inc. v. Calabrese*, No. 18-60788-CIV, 2018 WL 6653079, at *4–5 (S.D. Fla. July 5, 2018), *report and recommendation adopted*, No. 18-60788-CIV, 2018 WL 6653070 (S.D. Fla. Nov. 7, 2018) ("[T]he Court observes that a finding of unexplained delay in seeking injunctive relief strongly suggests a lack of *irreparable* and *imminent* harm that would compel the denial of a request for a preliminary injunction." (emphasis in original)).

If a plaintiff delays seeking injunctive relief, courts will then consider whether the party had a reasonable justification for the delay. S*ee Sprint Commc'ns*, 2018 WL 6653079 at *5. As part of this analysis, there are two relevant time periods: (1) the delay in filing a complaint after discovering the allegedly harmful conduct and (2) the delay in filing a motion for preliminary injunction once a complaint has been filed. *See Menudo Int'l, LLC v. In Miami Prod., LLC*, No. 17-21559-CIV, 2017 WL 4919222, at *5 (S.D. Fla. Oct. 31, 2017). "If *either* is unreasonably delayed, a finding of irreparable harm is significantly weakened." *Id.* (emphasis in original). Even if a party filed a complaint seeking injunctive relief, that party cannot unreasonably delay in seeking a preliminary injunction. *See Anago Franchising, Inc. v. CHMI, Inc.*, No. 09-60713-CIV-ALTONAGA, 2009 WL 5176548, at *13–14 (S.D. Fla. Dec. 21, 2009) (finding that, although the plaintiff requested injunctive relief in the complaint, its two-month delay in filing a motion for preliminary injunction followed by another two-month delay in filing a renewed motion for preliminary injunction, in combination, "indicate the absence of actual and imminent harm").

In this case, the Court will consider each of the two relevant time periods: (1) the delay from the discovery of the data download until the filing of the Complaint and (2) the delay between the filing of the Complaint and the Motion for Preliminary Injunction. As to the former, there was an almost two-month delay from the time Plaintiffs learned of the data download until the time they filed this lawsuit. The download occurred on October 28, 2023. A mere three days later, on October 31, 2023, Mr. Downey sent Defendant an email that said: "As you are aware, on October 31, 2023, we issued a formal notification regarding an ongoing investigation into a potential breach of contract related to unauthorized downloading of data." *See* ECF No. [82-3] at 3. In response, on November 2, 2023, Defendant admitted that he downloaded the data and explained that "[t]he backup functionality I employed is part of our company's IT infrastructure, intended for use by all employees, which suggests endorsement of its use. I acted in good faith, aware that such an action would be logged and under the scrutiny of our IT department – thereby transparent to you." *Id.* at 2. And, according to Mr. Downey's affidavit, Defendant also admitted to downloading Plaintiffs' information during an in-person conversation on October 31, 2023. *See* ECF No. [82-1] at ¶10. Thus, there was an almost two-month delay from the time Plaintiffs confirmed Defendant had downloaded their data until the time they filed suit on December 22, 2023.

The Court must next look to whether there is a reasonable justification for the delay. Here, Plaintiffs explain in their Reply that they attempted unsuccessfully to negotiate the return of the information by contacting Defendant directly and then his counsel. *See* ECF No. [82] at 3. The record indeed supports that Plaintiffs first approached Defendant and requested the return of the information directly from him, *see* ECF No. [82-3] at 3, and then demanded the return of the information days later through their attorney on November 3, 2023, *see* ECF No [72] at 29-30. Plaintiffs again demanded the return of the data on November 6, 2023 through their counsel. *See*

ECF No. [96-18]. Thereafter, on December 6, 2023, Defendant responded, through his counsel, admitting that he "would occasionally conduct backups of the Company data" and that such back up "could only be conducted through the Company platform called Google Takeout." *See* ECF No. [82-4] at 4. Confusingly though, Defendant, through his attorney, denied that he "actually downloaded Pliteq's information, which might have been against the Company's internal rules." *Id.* at 10. Regardless of this internal inconsistency in the December 6, 2023 letter, in light of Defendant's admission, both verbally and in writing, that he had downloaded the information as early as October 31, 2023, Plaintiffs were on notice of the download. Although it was incumbent on Plaintiffs to act swiftly to protect their rights, the Court does not find that this delay of about two months in filing suit was unreasonable given their informal efforts to obtain the return of the information directly from Defendant and through communications with his counsel.

The Court next looks at the time between filing suit and the filing of the Motion for Preliminary Injunction. This delay is significantly longer. Plaintiffs filed suit on December 22, 2023. *See* ECF No. [1]. They did not file the instant Motion until June 4, 2024, almost six months after filing suit (despite knowing as early as October 31, 2023 that he downloaded the data). This delay is significant, and the Court must consider whether the delay here was reasonable. Plaintiffs first point out that they sought injunctive relief in the Complaint. *See* ECF No. [82] at 4. Although the Complaint includes a count for injunctive relief, a delay in filing a motion for preliminary injunction can still indicate "the absence of actual and imminent harm." *See Anago Franchising,* 2009 WL 5176548 at *13–14 (finding no irreparable harm, even though the plaintiff requested injunctive relief in the complaint, when there was a combined four-month delay in pursuing a renewed request for injunctive relief). Plaintiffs also cite to difficulties in serving Defendant in Dubai to justify their delay, but the Court notes that, at no point in time until the instant Motion,

did Plaintiffs seek a temporary restraining order on an *ex-parte* basis to preserve the status quo while they served Defendant.[9]

Plaintiffs rely on several cases that do not support the protracted delay at issue here. Starting with *Larweth v. Magellan Health, Inc.*, 841 F. App'x 146, 158–59 (11th Cir. 2021), the district court concluded the delay was reasonable given "the parties' months-long discussions regarding the enforceability of the restrictive covenants and the possibility of a settlement." *Id.* at 158. Once those discussions broke down, the defendant filed its counterclaim and its motion for preliminary injunction. *Id.* at 158-59. The same cannot be said here where the Parties' settlement discussions broke down in early December 2023. Plaintiffs filed their lawsuit by December 22, 2023 and still waited nearly six months from filing suit to seek a preliminary injunction. As explained above, Plaintiffs did not make any efforts to obtain an *ex-parte* temporary restraining order, which would have showed some level of urgency on the part of Plaintiffs.

Likewise, Plaintiffs rely on *Wood v. Fla. Dep't of Educ.*, 729 F. Supp. 3d 1255, 1287 (N.D. Fla. 2024) to support a seven-month delay in seeking a preliminary injunction, but this case is distinguishable and lends no support for Plaintiffs position. In *Wood*, a First Amendment case, the district court pointed out that "binding precedent holds that ongoing 'direct penalization of protected speech . . . constitutes a *per se* irreparable injury.'" *Id.* at 1286. There is no analogous precedent holding that a misappropriation of trade secrets constitutes a *per se* irreparable injury. In fact, as explained above, there is not even a presumption of irreparable injury in trade secret

[9] Plaintiffs could have requested a temporary restraining order issued without notice under Federal Rule of Civil Procedure 65(b)(1). Such a temporary restraining order, if successful, could have been served on Defendant and would have been in effect for 14 days, subject to an additional extension for good cause.

misappropriation cases under the DTSA, much less a *per se* rule. And, the plaintiff in *Wood* engaged in a months-long dialogue with her school and the district to find a solution to the First Amendment issue, thereby acting with "'reasonable diligence' in seeking preliminary injunctive relief." *Id.* No such months-long dialogue occurred here as the discussions between Plaintiffs and Defendant ended in December 2023, more than six months before the Motion was filed. The remaining cases on which Plaintiffs rely are likewise distinguishable, *see Sexual MD Sols., LLC v. Wolff*, No. 20-20824-CIV, 2020 WL 2197868, at *24 (S.D. Fla. May 6, 2020) (excusing the delay in seeking a preliminary injunction because part of the delay was "attributable to the parties' discussions of a 'possible joint venture'"), or provide no analysis, and therefore have little persuasive value, as to why the delay was reasonable, *see BellSouth Advert. & Publ'g Corp. v. Real Color Pages, Inc.*, 792 F. Supp. 775, 785 (M.D. Fla. 1991) (providing no explanation as to why a seven-to-eight-month delay was reasonable).

The Court recognizes that Plaintiffs sought a default judgment, which included injunctive relief, on April 19, 2024. This was four months after filing suit and nearly six months after Defendant downloaded Plaintiffs' information. Although this at least shows earlier efforts to obtain injunctive relief, it still comes with a significant delay. Ultimately, the Court finds that this factor, while not dispositive of whether Plaintiffs sustained irreparable harm, weighs against such a finding.

iv. Whether the Confidentiality Agreement Creates a Presumption of Irreparable Harm

In their Motion, Plaintiffs argued that the mere existence of the Confidentiality Agreement and its provision allowing for injunctive relief supported its position of irreparable harm. Although Plaintiffs appear to have abandoned that argument in their Reply after Defendant challenged it, the Court nonetheless addresses the issue in an abundance of caution.

In support of this argument, Plaintiffs cite to paragraph 13 of the Confidentiality Agreement, which provides:

> any breach or threatened breach by [Defendant] could result in irreparable harm to the Company which may not reasonably or adequately be compensated in damages and that, in the event of any such breach or threatened breach, the Company shall be entitled to equitable relief, including but not limited to temporary, preliminary and permanent injunctive relief enforcing the specific performance by the [Defendant] or enjoined [sic] or restraining the [Defendant] from any violation or threatened violation of the terms of this Agreement.

See ECF No. [50] at 18 (alterations in original) (citing ECF No. [1-3] at ¶13).

The Court finds that this provision in the Confidentiality Agreement, standing alone, is not "dispositive of the issue of irreparable harm, and does not insulate a plaintiff seeking a preliminary injunction from the need to prove that it will suffer imminent irreparable injury as a result of the [defendant's] conduct." *See Anago Franchising, Inc.*, 2009 WL 5176548, at *11 (alteration in original) (quoting *Boston Laser, Inc. v. Qinxin Zu,* No. 07–CV–0791, 2007 WL 2973663, at * 12 (N.D.N.Y. Sept. 21, 2007)). "In discussing the weight accorded to contractual provisions creating entitlement to injunctive relief, district courts have generally accorded them little to no weight," finding that "such a contract provision 'is not dispositive of the issue of irreparable harm, does not in and of itself create a presumption of irreparable harm, nor is it binding upon the Court.'" *B&G Equip. Co., Inc. v. Airofog USA, LLC*, No. 19-CV-403-T-36AEP, 2019 WL 2537792, at *3–4 (M.D. Fla. June 20, 2019) (internal citation omitted). This means that, regardless of the existence of this provision, courts must still engage in the case-by-case analysis of whether the party seeking the injunction will suffer imminent irreparable harm. *Anago Franchising, Inc.*, 2009 WL 5176548 at *11.

Here, the Court acknowledges that Plaintiffs and Defendant entered into the Confidentiality Agreement whereby irreparable harm and injunctive relief were presumed. But this private

agreement does not bind the Court's analysis as to whether Plaintiffs have satisfied their burden of showing irreparable harm, and the Court finds that this agreement, standing alone, is insufficient. For that reason, the Court now turns its analysis to the evidence presented in the record to determine whether Plaintiffs have indeed made the required showing of irreparable harm to warrant a preliminary injunction.

v. Whether Plaintiffs' Claims of Irreparable Harm Are Speculative and Remote

Having determined whether a presumption applies and the impact of the Confidentiality Agreement on the Court's analysis, it now looks to the evidence the Parties presented and their arguments on the question of irreparable harm. In support of their argument, Plaintiffs state that Defendant's access to their trade secret information creates "a risk of irreparable harm." *See* ECF No. [100] at 211. When coupled with Defendant's refusal to return the information, refusal to certify its destruction, and Plaintiffs' inability to verify whether the records were indeed deleted, Plaintiffs argue that they have proven they will be irreparably harmed if the preliminary injunction is not granted. *Id.* Defendant, in turn, argues that the harm here is not actual or imminent but instead highly speculative. He directs the Court to Defendant's counsel's December 6, 2023 letter in which Defendant represents that he will abide by his obligations under the Confidentiality Agreement, his deposition testimony in which he states under oath that he has not disclosed any trade secrets and will not disclose them in the future, Plaintiffs' failure to identify any disclosures of confidential or trade secret information, and the highly speculative "risk" of irreparable harm about which Mr. Ayala testified. *Id.* at 218-219. Upon close review of the evidence and the pertinent case law, the Court finds that Plaintiffs have fallen short of showing that, absent the entry of a preliminary injunction, they will suffer irreparable harm.

As Defendant correctly notes, harm can only be irreparable if it is "actual" and "imminent" and not "remote" or "speculative," relying on *TransUnion Risk & Alternative Data Sols., Inc. v. Challa*, 676 F. App'x 822, 825 (11th Cir. 2017). In *Challa*, the district court credited the defendant's testimony that he would not use or disclose the proprietary information while working for his new employer, finding the testimony credible because the defendant's new employment position was substantially different from the employment position he held with the plaintiff.

Here, the Court credits Defendant's statement that he will not share the trade secret information he downloaded for multiple reasons. First, Defendant did not download the information in a clandestine fashion, but rather used Google Takeout, which would be visible to Plaintiffs' IT department. He made no efforts to delete the email in his inbox revealing that he received the Google Takeout files and the files were ready for download. Next, he immediately admitted to downloading the files during his conversation with Mr. Downey on October 31, 2023 and again in his October 31, 2023 email to Mr. Downey. Following his termination and receipt of several letters from Plaintiffs' counsel, Defendant agreed, through his counsel, to abide by the terms of the Confidentiality Agreement and not disclose any of the downloaded information. And, at his deposition, Defendant testified that he has not shared any confidential or trade secret information, has deleted all Pliteq information from his Dropbox account, and did not transfer it to any other location before he deleted it.

While Plaintiffs remain skeptical about Defendant's statements in his December 2023 letter and at his deposition, Plaintiffs were unable to provide the Court with any evidence that Defendant has shared any of its confidential or trade secret information. During his testimony, Mr. Pulcine agreed that Pliteq had presented no evidence that Defendant had disclosed any trade secrets or confidential information to any third party. *See* ECF No. [100] at 172. From the date of the Google

Takeout download until the date of the Hearing, nearly nine months had elapsed and there was no evidence that Defendant had used or disclosed a single piece of confidential information. And, much like the defendant in *Challa*, there is no indication here that Defendant is currently working for a competing business anywhere in the world, much less one operating in the United States, where there would be a real risk for the disclosure of trade secret information.[10] Surely, if Defendant were currently working for a competitor, Plaintiffs would have argued as much.

Plaintiffs also argue irreparable harm based on the "risk" that the laptop may be turned on at some point in the future and will sync with Defendant's Dropbox again, once again giving Defendant access to the information. The foregoing theory is based on Mr. Ayala's testimony. However, the Court finds that theory to be speculative and remote, not actual and imminent. This is because multiple "ifs" must be satisfied before this "risk" ever materializes. On cross-examination, Mr. Ayala explained that, for this to occur, the laptop must first be turned on, next the laptop must be connected to WiFi, and next the Dropbox account must sync with the laptop device, which means that the passwords or access credentials must still be the same as before. *See* ECF No. [100] at 68-70. When asked, Mr. Ayala could not testify to any degree of forensic probability whether the laptop could still sync with the applications and could, at most, testify that the concept of auto sync is a "possibility" and there is a "risk" this could occur. *Id.* at 68, 70. The undisputed testimony presented at the Hearing was that Defendant changed the password to his Dropbox account on October 31, 2023, *see* ECF No. [77-2] at 91, which means the Dropbox account will not sync if the laptop, which is in the custody of the Dubai police, is ever turned on at some future point in time.

[10] Defendant was working for a company that does artificial intelligence marketing. *See* ECF No. [100] at 224.

Although Plaintiffs heavily rely on *Meachum* and *Eichelberg* to support their request for a preliminary injunction, the Court finds these cases distinguishable as they relate to the irreparable harm factor. In *Meachum*, the defendant testified that he had no intent to use the confidential information, but his actions said otherwise as he denied taking any confidential information during his exit interview and he attempted to hide his tracks by deleting evidence of his misappropriation from the company servers. 2019 WL 2637053 at *4. Further, there was evidence in *Meachum* that the defendant was starting his own competing business and that he still possessed the information. *Id.* at. *5. In light of this, the district court concluded there was evidence of irreparable harm. *Id.* Similarly, in *Eichelberg*, the district court focused on the defendant's continued possession of the trade secret information as the basis to find irreparable harm. As explained above, here, Defendant admitted to downloading the information immediately, did not download the information in a surreptitious fashion, did not attempt to conceal the download, agreed not to share the confidential information under the terms of the Confidentiality Agreement, deleted the Pliteq trade secret files from his Dropbox account, no longer has access to the laptop, and is not engaging or employed in a competing business.

For the foregoing reasons, the Court finds that Plaintiffs failed to demonstrate that the harm here is more than remote or speculative and, therefore, failed to prove that they will suffer irreparable harm without the entry of a preliminary injunction. Failing to satisfy their burden on this prong of the four-part inquiry, the Motion is due to be denied and the Court need not address the third and fourth prongs of the preliminary injunction analysis or whether a bond or civil seizure order are appropriate.

V. CONCLUSION

For the reasons explained above, Plaintiffs' Oral Motion for Sanctions for Spoliation of Evidence is **DENIED,** and Plaintiffs' Motion for Temporary Restraining Order and Preliminary Injunction, **ECF No. [50]**, is **DENIED**.

DONE and ORDERED in Chambers in Miami, Florida on March 28, 2025.

MARTY FULGUEIRA ELFENBEIN
UNITED STATES MAGISTRATE JUDGE

cc: All Counsel of Record