

FINANCIALAPPS, LLC,

Plaintiff,

v.

ENVESTNET, INC. and
YODLEE, INC.,

Defendants.

FILED UNDER SEAL

1

(D.I. 625–27.) FinancialApps filed its reply and supporting declaration on March 14, 2024.

(D.I. 636, 637.)

On December 10, 2024, the Court entered an Order appointing me to provide a Report and Recommendation for the resolution of FinancialApps’s spoliation motion and the spoliation motion that Defendants had advised they would be filing. (D.I. 655.)

On December 13, 2024, Defendants Envestnet, Inc. and Yodlee, Inc. filed their Motion for Finding of Spoliation and for Sanctions, supporting brief, and declarations. (D.I. 657–659.) Defendants’ spoliation motion concerns FinancialApps’s alleged deletion of two items: (1) a non-disclosure agreement (NDA) with an independent contractor named Mr. Dye; and (2) a public “Developer” website used to promote FinancialApps’s software. (*Id.*) On January 24, 2025, FinancialApps filed its answering brief and two supporting declarations. (D.I. 663–665.) Defendants filed their reply and supporting declarations on February 18, 2025. (D.I. 669–671.)

On March 7, 2025, Plaintiff filed a Request for Oral Argument. (D.I. 674.)

On April 29, 2025, the Special Master conducted a transcribed videoconference, and the parties provided me with copies of their slides used during the hearing.

II. General Background Relevant to Both Motions

Defendants approached FinancialApps in April 2016 to license software for a platform called “Risk Insight.” Risk Insight was to generate financial profiles for credit applicants to help financial institutions decide whether to lend them money. On January 31, 2017, FinancialApps and Yodlee entered into a Master Services Agreement (“MSA”). (D.I. 665, Ex. 2.) The MSA included a fee structure and payment for services rendered. (*Id.* § 4(a)–(g).) Notwithstanding the terms of the MSA, by October 2018, Yodlee had accrued an unpaid balance in the mid-six figure range. (D.I. 665, Ex. 3.) FinancialApps engaged counsel who, on April 9, 2019, sent a

letter to Yodlee’s General Counsel regarding the alleged delinquent payments. (D.I. 665, Ex. 5.) The letter did not contain any allegations of trade secret misappropriation.

In May 2019, FinancialApps first suspected that Defendants might be misappropriating FinancialApps’s technology to create a product to compete with Risk Insight. On May 16, 2019, FinancialApps received the first of several emails it says revealed that Defendants were well into developing their own competing platform, potentially based on FinancialApps’s Risk Insight platform. (D.I. 665, Ex. 11.) FinancialApps sent a cease-and-desist letter on May 17, 2019, the next day. Then, on May 20, 2019, FinancialApps claims that Defendants sent them an email “exposing their reverse engineering of FinancialApps’s technology.” (D.I. 2 ¶ 107, Ex. 4.) In response, FinancialApps terminated the contract for cause on May 27, 2019. (*Id.* ¶ 199.) After settlement discussions failed, FinancialApps filed its Complaint on July 17, 2019. The Complaint focuses on alleged technology misuse, but also includes claims related to the fee dispute. (*Id.* ¶¶ 207–338.)

III. Background for FinancialApps’s Spoliation Motion

In the May 17, 2019 letter from FinancialApps to Defendants advising them of FinancialApps’s potential claims of misappropriation of their Risk Insight platform, FinancialApps also requested that Yodlee “ensure preservation of all relevant information, including ...electronic files and data.” (D.I. 616, Ex. 12.) After a series of discussions, on June 11, 2019, FinancialApps suspended Defendants’ access to the Risk Insight platform through a software application called HashiCorp Vault (“Vault”). On June 13, 2019, Mr. Uberoi (at the time Yodlee’s General Counsel and Senior Vice President for Legal Affairs) circulated a document-hold notice requiring retention of “[a]ll documents relating to the Risk Insight product; ... [a]ll documents relating to the development of any software, product, or service with Equifax

Inc. or any related entity; ... and [a]ll other documents you believe may be relevant to a potential dispute with Financial Apps.” (D.I. 616, Ex. 19.) The document-hold notice also specifically called out third-party sources of information:

SPECIAL INSTRUCTIONS FOR DATABASES

If you are aware of potentially relevant data stored on a network, departmental database, shared or public mailbox, or with a third-party vendor, it must be identified for me immediately so that our legal counsel are alerted and the information can be preserved. Document destruction policies must be suspended. Steps to preserve information created on an on-going basis should be discussed with counsel.

(*Id.* at 2.) Along with being sent to Yodlee employees, Mr. Uberoi’s document-hold notice was sent to Debra DeVoe (at the time, Envestnet’s Chief Compliance Officer and Senior Vice President)¹ and Timothy O’Brien (at the time, Envestnet’s Chief Information Security Office and Group Head of Enterprise Security and IT). (D.I. 616, Ex. 19.) This was “because the scope of the litigation was wider than just Yodlee. ... [T]he people [who] are in charge of [Envestnet’s] document and retention and [Envestnet’s] records, [Envestnet’s] chief compliance officer and [Envestnet’s] head of systems were told to take steps to preserve documents in connection with the litigation.” (D.I. 616, Ex. 20 at 250:12–23.) Under the hold notice, “[Envestnet] had discussions with Yodlee legal, in-house legal, and Yodlee IT about where data could reside and where they were preserving data.” (*Id.* at 274:6–9.) Envestnet’s Rule 30(b)(6) designee described “four to six separate discussions over a period of time with Yodlee by Envestnet, Inc. on this matter.” (*Id.* at 276:3–5.) These discussions included discussion of “AWS and third-party services related to Risk Insight[.]” (*Id.* at 280:11–18.) Despite being a “very broad do-not-destroy-documents type of discussion,” there were also “discussions regarding what materials

¹ I confirmed the titles and employers referenced throughout this opinion by looking at email signatures in the exhibits and referencing LinkedIn pages.

could be deleted and what electronic materials could not be deleted[.]” (*Id.* at 298:17–284:16.) Specifically, “[t]here was discussion about a certain database in I believe AWS that did not need to be utilized any longer and what Yodlee was doing to preserve any of that data.” (*Id.* at 274:11–15.)

As a result of these meetings and notwithstanding the document-hold notice issued over a month prior that directed recipients to “err on the side of preservation” (D.I. 616, Ex. 19 at 2), Jeff Schulte (Yodlee’s Senior Vice President for Cloud Operations) emailed Yodlee technical personnel on July 15, 2019, informing them that there was “[Executive Team]² clearance to proceed with decommissioning the FA/Credit Insights environment.” (D.I. 616, Ex. 22.) Schulte identified specific categories of ESI sources to be “terminated,” including “[a]ll stage environment AWS instances”³ and “[t]hird party services that are purely run-time and hold no client data[.]” (*Id.*) Schulte did not tell the technical personnel to make copies or otherwise back up the data from any of the to-be-decommissioned environments or vendor services, instead selectively instructing that only “[c]ustomer and report data need to be backed up and made readily available for future customer inquiries.” (*Id.*)

² In addition to Lisa Hingley, Arun Anur, and Jeff Schulte, members of the Yodlee Executive Team included Anil Arora (at the time, Yodlee’s CEO), Bill Parsons (at the time, Yodlee’s Group President of Data Analytics and International), Julie Solomon (at the time, Yodlee’s Senior Vice President and Head of North American Sales), Arjun Singh (at the time, Yodlee’s Managing Director for Asia), Marc Blouin (at the time, Yodlee’s CFO), and Chris Chen (at the time, Yodlee’s Senior Vice President and General Manager of the API Team). (D.I. 616, Ex. 21 at 36:2–17.)

³ For clarity, there were two types of AWS instances maintained by Defendants. The first, which are not the subject of the Motion, were called “production” instances, which were the “live” instances used to provide the Risk Insight platform to contracting clients. The second type, called “stage” instances, were used internally by Defendants for development, testing, and demonstration. (Priegues Decl. ¶ 6.) Each environment contained a full version of Risk Insight.

On July 17, 2019, the same day Plaintiff filed its Complaint, Schulte forwarded the decommissioning communication to Stuart DePina (at the time, Envestnet’s Chief Executive and President), Brandon Rembe (at the time, Envestnet’s Senior Vice President of Products and Strategy), Arun Anur (at the time, Yodlee’s Senior Vice President of Services), Lisa Hingley (at the time, Yodlee’s Senior Vice President of Strategic Account Management), and Sidharth Uberoi (at the time, Yodlee’s General Counsel), confirming that clearance for decommissioning was provided by Mr. Rembe of Envestnet and Mr. Anur of Yodlee. (*Id.*)

A. Papertrail

That same day, July 17, 2019, Katie McCarthy (at the time, Yodlee’s Senior Manager for Cloud Business Operations) identified Papertrail as “log management” in the “list of all third-party relationship [sic] that we will have to cancel,” stating that she was “[p]retty sure this can be cancelled right away, please confirm no data is needed from this account.” (D.I. 616, Ex. 23 at 6.) Within a day, Ganesh Mani (at the time, Yodlee’s Director of Site Reliability Engineering)⁴ confirmed that “[Papertrail] can be cancelled.” (*Id.*) Despite Ms. McCarthy asking whether there were certain third-party vendors “that we might want to take some extra steps beyond simple cancellation” and several references to other repositories being backed up before deletion (*e.g.*, MongoDB and S3 (*id.* at 4–5) and Cloud66 (*id.* at 3)), the Papertrail account was cancelled by July 23, 2019 without any attempt to back up its contents. (*Id.* at 1.) Contrary to representations made at deposition that “decommissioning is not the same as deletion” and “[d]ata deletion has not – has not happened” (D.I. 626, Ex. 16 at 226:19–23), under the governing Software Services Agreement, “[w]hen the Papertrail account was cancelled, all user

⁴ <https://www.yodlee.com/financial-products/api-best-practices-for-maximum-performance-and-scalability>

data and preferences were deleted immediately, and the Papertrail log data aged out [*i.e.*, were deleted] 30 days after the cancellation[.]” (D.I. 617, Ex. 48.)

Despite costing only \$395 per month to maintain (D.I. 616, Ex. 23 at 6), Papertrail provided 25 gigabytes of log storage per month, search capability for 2 weeks’ worth of logs, and—most importantly—one year’s worth of downloadable log archives. (D.I. 637, Exs. 63–64.) Doing the math, it is likely that at the time of its decommissioning, Defendants’ Papertrail account may have archived upward of 300 gigabytes of logs⁵ spanning the period from July 23, 2018, through July 23, 2019.

B. AWS

The Risk Insight platform was hosted in discrete environments on AWS, a cloud computing service. (D.I. 614, Priegues Decl. ¶ 3; D.I. 615, Pflaum Decl. ¶ 7; D.I. 616, Ex. 1 at -2668.) Defendants owned the AWS account. (D.I. 614, Priegues Decl. ¶ 9.) Each Risk Insight client received a “tenancy” within the AWS workspace, each of which contained discrete “Production Environments” and “Stage Environments.” (D.I. 614, Priegues Decl. ¶ 3; D.I. 615, Pflaum Decl. ¶ 7; D.I. 616, Ex. 1 at -2668.) Each environment contained a full version of Risk Insight. (D.I. 614, Priegues Decl. ¶ 7; D.I. 615, Pflaum Decl. ¶ 8.)

Risk Insight in the AWS environments used Vault for credential management and data encryption. (D.I. 614, Priegues Decl. ¶ 15; D.I. 616, Ex. 1 at -2667.) The Vault software could “seal” and “unseal” the Risk Insight software. In the “sealed” state, the Vault software prevented the Risk Insight application from working by blocking its API endpoints. (D.I. 614, Priegues Decl. ¶ 15; D.I. 616, Ex. 1 at -2667–77; D.I. 616, Ex. 9 at 57:6–58:9.) The Vault software did

⁵ Emails attached as Exhibits by Defendants indicate that the parties routinely met or exceeded their 25 GB per month limit of log storage. (D.I. 627, Exs. 35–37.)

not affect access to Risk Insight’s AWS environments or the data they contained. (D.I. 614, Priegues Decl. ¶ 16; D.I. 616, Ex. 10 at 564:21–565:10.)

In the same July 23, 2019 email confirming that the Papertrail subscription had been cancelled, Ms. McCarthy also confirmed that the termination of “[a]ll stage environment AWS instances” had been “done.” (D.I. 626, Ex. 24 at -449828.) Like the production instances, the staging instances stored working data in a MongoDB⁶ output report in the cloud using Amazon’s S3 services. (D.I. 616, Ex. 1 at -132663; D.I. 616, Ex. 18 at 26 (“S3 has both orders (reports) and application logs (API, portals, Embedded rails, etc)”)).) But unlike Defendants’ backup of the MongoDB and S3 data from the *production* instances, the only data backed up from the terminated *stage* instances appears to have been the stage MongoDB data (D.I. 616, Ex. 18 at 14), *not* the stage instance report data ostensibly stored in S3. It is unclear what (if any) reports may have been stored in the stage instance S3 account or whether any applied to the claims at issue.

IV. Background for Defendants’ Spoliation Motion

A. The Developer Website

In early 2016, FinancialApps used the URL <https://developer.financialapps.com> (the “Website”) to host early versions of the FinancialApps API,⁷ which were made accessible to potential customers. (D.I. 659, Ex. 13 at 7:9–10:4.) FinancialApps stopped updating the Website around June 2017 when FinancialApps began its collaboration with Defendants. (D.I.

⁶ MongoDB is a type of NoSQL database commonly used by cloud providers. See Jeffery Erickson, *What Is MongoDB? An Expert Guide*, October 30, 2024, <https://www.oracle.com/in/database/mongodb/>.

⁷ An Application Programming Interface, or API, is a form of application-based connection between computers or between computer programs. See *Data APIs Explained*, <https://www.mongodb.com/resources/basics/what-is-an-api>.

659, Ex. 13 at 9:11–10:4; D.I. 659, Ex. 14.) According to FinancialApps, the content of the Website did not include downloadable documents. (D.I. 665, Ex. 8 at 27.)

In 2018, the host of the Website (first called Gelato and then later Kong) informed FinancialApps that the Website had reached its end-of-life and was to be decommissioned on February 1, 2019. (D.I. 659, Exs. 15 and 16.) FinancialApps declined to migrate any data off the Website before it was decommissioned, and, accordingly, “[a]ll data hosted on the Website and all associated data, including any visitor logs, content logs, version and/or revision logs, if they existed, were deleted in the ordinary course of business by AWS when Kong terminated this service in 2019.” (D.I. 659, Ex. 17.) Neither Kong nor FinancialApps retained any data from the Website. (*Id.*; D.I. 663 at 5.)

While Plaintiff’s expert, Mr. Pflaum, opined that the Website contained “an early iteration of *a* data dictionary” (D.I. 659, Ex. 1 ¶ 226 (emphasis added)), he later qualified his response by stating that:

[T]he early iteration of FinancialApps’ Data Dictionary [present on the Website] describes some data structures that could be retrieved through version 1 of the FinancialApps API and shows only raw examples of account and transaction data and category codes. It does not reveal the API specification, workflows, data structures, Platform schema, data selections, data conditioning, or rules (attribute logic) documented in, for example, the FinancialApps Data Dictionary, Full API Portal Development document, Attributes Glossary, or Master Schema file.

(*Id.* ¶ 229.)

B. The Dye NDA

On March 27, 2019, FinancialApps sent a copy of the Data Dictionary to Christian Dye, who at the time worked for a third-party company. (D.I. 659, Ex. 5.) According to FinancialApps’s expert, this Data Dictionary contained key trade secret information. (*Id.*, Ex. 1 ¶ 31.) FinancialApps asserts that Mr. Dye signed an NDA prior to receiving any information

(including the Data Dictionary), but that the NDA, which allegedly existed only in hard copy, was lost during an office move. (D.I. 663 at 7.)

Defendants believe that the Dye NDA never existed. (D.I. 658 at 1 (“[T]he document record contains no evidence that FA had entered into an NDA with Mr. Dye or his employer.” ... “The likeliest explanation for FA’s failure to produce an NDA with Dye is that FA did not actually enter into an NDA with Dye.”), D.I. 658 at 3 (“There is no NDA with Dye in the record.” ... “[T]he document record contains no evidence that FA had entered into an NDA with Dye or with NTT Data.”), D.I. 658 at 5 (“...assuming FA’s claim that [the NDA] existed is true...”), D.I. 658 at 11–12 (“The Purported Dye NDA obviously should have been preserved (*if it existed*).” (emphasis added.)), D.I. 658 at 13 (“*If it ever existed*, the Purported Dye NDA now is gone.”) (emphasis added.), D.I. 658 at 18 (“...the dubious ultimate claim that the Purported Dye NDA existed. *If it did exist*, it is lost...” ... “But because it is lost (*by FA’s telling, at least*)...”, etc.); D.I. 669 at 1 (“...if the Purported Dye NDA actually did exist,...”), D.I. 669 at 3 (“And there is no electronic trace of [the NDA].”), D.I. 669 at 4 (“Defendants will happily withdraw this portion of the Motion if FA provides affidavits stating that an NDA actually did not exist after all.”), D.I. 669 at 7 (“...a contractor who supposedly signed an NDA.”).)

LEGAL STANDARDS

Fed. R. Civ. P. 37(e) provides that “[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery,” the court may cure any prejudice from the loss of the evidence. Failing to take reasonable steps to preserve ESI “equate[s] to roughly a negligence standard.” *IOENGINE LLC v. PayPal Holdings, Inc.*, No. CV 18-452-WCB, 2022 WL 1443867, at *3 (D. Del. May 3, 2022)

(quoting *Leidig v. BuzzFeed, Inc.*, No. 16-CIV-542, 2017 WL 6512353, at *10 (S.D.N.Y. Dec. 19, 2017)). Under the court’s inherent authority, “[s]poliation occurs where: the evidence was in the party’s control; the evidence is relevant to the claims or defenses in the case; there has been actual suppression or withholding of evidence; and, the duty to preserve the evidence was reasonably foreseeable to the party.” *CIGNEX Datamatics, Inc. v. Lam Rsch. Corp.*, No. 17-320-MN, 2019 WL 1118099, at *2 (D. Del. Mar. 11, 2019) (quoting *Bull v. United Parcel Serv. Inc.*, 665 F.3d 68, 73 (3d Cir. 2012)). Historically, in the Third Circuit, “a finding of bad faith [has been] pivotal to a spoliation determination.” 665 F.3d at 79.

If a court finds that spoliation occurred, it must then determine an appropriate sanction for the suppression or withholding of evidence. The sanctions analysis focuses on “(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party, and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future.” *CIGNEX Datamatics*, 2019 WL 1118099, at *2 (quoting *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994)). [U]nder Rule 37(e) an adverse inference sanction is available “only upon finding that the party [in possession of the ESI] acted with the intent to deprive another party of the information’s use.” *IOENGINE LLC*, at *7 (quoting Fed. R. Civ. P. 37(e)(2)).

Whether the movant must prove spoliation by a preponderance of the evidence or clear and convincing evidence is somewhat unclear. Courts in the Third Circuit often apply the preponderance standard as to whether the elements of spoliation have been shown. *See, e.g., Painadath v. Good Shepherd Penn Partners*, 348 F.R.D. 16, 26 (E.D. Pa. 2024) (citing *Cianci v. Phoenixville Area Sch. Dist.*, No. 20-cv-4749, 2022 WL 824026, at *5 (E.D. Pa. March 18,

2022)). And courts often apply the clear and convincing evidence standard when evaluating whether a party acted in bad faith and should be sanctioned. *See, e.g., Micron Tech., Inc. v. Rambus Inc.*, 917 F. Supp. 2d 300, 324 (D. Del. 2013). Here, none of my decisions turn on whether preponderance of the evidence or clear and convincing evidence is the standard. For the portions of the motions I deny, the movant did not meet even the lower preponderance of the evidence standard. On the one issue where I find spoliation and award a sanction, I find that the movant proved the elements of spoliation and intent by clear and convincing evidence.

DISCUSSION

I. I Recommend Granting-In-Part FinancialApps’s Spoliation Motion

A. I Recommend Granting-In-Part the Portion of FinancialApps’s Spoliation Motion Concerning the Papertrail ESI

FinancialApps moves for a spoliation finding because Defendants failed to preserve data from a third-party service called Papertrail. To log the operation of the Risk Insight software in the AWS environments where it resided, FinancialApps designed Risk Insight to track all users, system activity, and system events and automatically output a log of that data into a third-party subscription software service called Papertrail. The data logged and output into Papertrail included: (1) every step of Risk Insight’s internal workflows; (2) all API calls, responses, and payloads; (3) utilization of data inputs; (4) user identities; (5) user events; (6) what Risk Insight functionality was accessed; (7) which features were used; and (8) whether data was copied from or injected into the system, among other things. (D.I. 614, Priegues Decl. ¶ 11; D.I. 615, Pflaum Decl. ¶ 12.) Papertrail is marketed as “a flight data recorder for . . . apps” (D.I. 616, Ex. 3) and provided a unified and streamlined interface to efficiently access, search, and archive Risk Insight’s application logs. (D.I. 614, Priegues Decl. ¶ 13; *see also* www.Papertrail.com.) Risk

Insight's AWS and Papertrail accounts were created, maintained, and controlled by Defendants. (*See, e.g.*, D.I. 616, Ex. 5; D.I. 614, Priegues Decl. ¶¶ 9, 14.)

As indicated by the name "Papertrail," the logs were relevant to FinancialApps's trade secret misappropriation claims. *See* <https://www.merriam-webster.com/sentences/paper%20trail> ("They covered up the fraud and were careful not to leave a paper trail."). The Papertrail logs would have shown who from Defendants accessed the Risk Insight software and the history of what they were doing during the exact timeframe when Defendants were developing their competing product. If, as FinancialApps alleges, Defendants were misusing Risk Insight to develop their competing software product, the Papertrail logs would have likely been some of the best evidence of that misuse. Yet if, as Defendants allege, their use of the Risk Insight software was permitted by the parties' agreement and they did nothing improper, the logs likely would have been exculpatory. Defendants do not contest the relevance of the Papertrail ESI.

Because the Papertrail ESI was highly relevant, Defendants had a duty to preserve it. *See, e.g., Goldrich v. City of Jersey City*, No. 15-885 (SDA)(LDW), 2018 WL 4492931, at *9 (D.N.J. July 25, 2018), *report and recommendation adopted as modified*, 2018 WL 4489674 (D.N.J. Sept. 19, 2018) ("duty to preserve evidence require[s] that [they] take reasonable affirmative steps such as backing up the ESI"). But rather than preserving the Papertrail ESI, Defendants terminated the Papertrail subscription without taking any steps to preserve the data, and Papertrail eventually deleted the data because Defendants cancelled the subscription. (D.I. 617, Ex. 48.)

Defendants' reasons for not preserving the Papertrail ESI are flimsy. Defendants argue that FinancialApps requested that they use the Papertrail service and were more familiar with the software subscription's capabilities. This is beside the point. The relevant inquiry is whether

Defendants knew or should have known that the Papertrail ESI was relevant to FinancialApps's trade secret misappropriation claims. They did. And if Defendants had any doubt about whether data from a service called "Papertrail" used to log activity in the AWS environments was relevant to the parties' disputes, they could have reached out to FinancialApps to ask whether FinancialApps, with its allegedly superior knowledge about the software, thought the data needed to be preserved. Defendants never reached out to FinancialApps. (April 24, 2025 hearing transcript at 23:6–24:21 and 40:11–41:12.) Instead, they unilaterally and intentionally cancelled the subscription days after FinancialApps filed this lawsuit. In this circumstance, even if Defendants had not known that the data was relevant (and I find that they did know), they acted unreasonably by not conferring with the other side and acting unilaterally.⁸ See *Ogin v. Ahmed*, No. 06-cv-350, 2008 WL 4722390, at *1 (M.D. Pa. Sept. 2, 2008) (finding circumstances warranted the sanction of an adverse inference instruction where the defendants destroyed evidence after unilaterally determining that the evidence was not relevant).

Defendants also argue that "[FinancialApps] presents no evidence that Yodlee thought or should have thought Papertrail held any data at all" and that they believed Papertrail was a "low priority" tool. (D.I. 625 at 13.) Defendants knew that Papertrail held logging data for the Risk Insight software environment. They knew this because they signed up for the service and selected the level of service to enroll in—to say that they had no idea that Papertrail held any data at all is contrary to the record.

Defendants make another, less extreme argument: they believed the Papertrail service stored only two weeks of data. They base this argument on an email that talks about signing up

⁸ Fed. R. Civ. P. 26(f) required the parties to "discuss any issues about preserving discoverable information." It does not appear that such a discussion took place with sufficient detail. (April 29, 2025 hearing transcript at 23:6–26:1.)

for Papertrail service with “14 days of search.” (D.I. 616, Ex. 33.) But as FinancialApps correctly points out, this email referred to “search” and not “retention” or “archives.” In fact, Papertrail allowed access to one year of archived logs. Papertrail’s website makes this clear. (D.I. 637, Exs. 63 and 64.) Defendants should have been aware of this from a knowledge transfer session they attended. (D.I. 637, Ex. 68.) And, again, if Defendants had any questions about the data available in Papertrail, they should have reached out to FinancialApps or to Papertrail before cancelling the account, which they knew would result in deletion of the data.

Defendants next argue that even if FinancialApps could carry its burden as to Yodlee, sanctions against Envestnet are not warranted because Envestnet did not actually destroy anything. (D.I. 625 at 18–20.) But “actual destruction” is not the inquiry. Under Rule 37, the inquiry is whether evidence was “lost because a party failed to take reasonable steps to preserve it.” Here, Envestnet, like Yodlee, failed to take reasonable steps to preserve the Papertrail ESI. Envestnet admits that its in-house counsel was involved in the decision to “decommission” the Papertrail account, among other actions. Patrick Marr, Envestnet’s corporate designee and deputy general counsel, testified that Envestnet and Yodlee legal departments worked together on preservation efforts and had joint meetings about what documents would be preserved and no longer paying for certain subscriptions. (D.I. 637, Ex. 55 at 243–45.) Mr. Marr also testified on behalf of Envestnet that he and Mr. O’Brien had four to six discussions with Yodlee in-house legal personnel and Yodlee IT about preservation of data and about decommissioning. (*Id.* at 273–76.) The deposition testimony shows Envestnet was supervising, approving, and controlling Yodlee’s preservation and decommissioning efforts. (*Id.* at 277–80.) In these circumstances, Envestnet is responsible for the failure to preserve because it actively participated in the decision to discontinue the Papertrail subscription without preserving the data.

Defendants cite cases for the proposition that a parent corporation is not responsible for the spoliation of its subsidiary simply by virtue of ownership. But this is not a piercing of the corporate veil situation. Envestnet actively participated in the spoliation. This distinguishes the facts here from the cases cited by Defendants. Even if Envestnet had not actively participated in the decommissioning, it had control over Yodlee and could have and should have ensured that Yodlee preserved the Papertrail ESI. *See, e.g., United States v. Maxxam, Inc.*, No. C-06-07497CWJCS, 2009 WL 817264, at *9 (N.D. Cal. Mar. 27, 2009) (“it is entirely reasonable to hold Maxxam and Hurwitz responsible for the preservation of evidence in the hands of its agent”); *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 514 (D. Md. 2009) (in the spoliation context, parties to litigation are deemed to be in “control” of information to which they have access or the legal right to obtain, even if the evidence is in the possession of a third party). *See also N.J. Mfrs. Ins. Co. v. Hearth & Home Techs., Inc.*, No. 3:06-CV-2234, 2008 WL 2571227, at *7 (M.D. Pa. June 25, 2008) (forgoing a discussion regarding control, but nonetheless holding that “[a] plaintiff, particularly one who was represented by counsel prior to the spoliation, is not relieved of this responsibility merely because the plaintiff did not itself act in bad faith and a third party to whom Plaintiff entrusted the evidence was the one who discarded or lost it.”).

Because I find spoliation, I now turn to whether to sanction Defendants and, if so, the appropriate sanction. Under Rule 37(e), as amended in 2015, a court may impose certain severe sanctions if it finds a spoliating party “acted with the intent to deprive another party of the information’s use in the litigation.” If the intent-to-deprive standard is met, a court may:

- Presume that the lost information was unfavorable to the party;
- Instruct the jury that it may or must presume the lost information was unfavorable to the party; or
- Dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e)(2). If the intent-to-deprive standard is not met, a court may still impose lesser sanctions if the loss of ESI prejudices the other party. Fed. R. Civ. P. 37(e)(1).

I find that deletion of the Papertrail ESI prejudiced FinancialApps's ability to prove its case. The Papertrail ESI would have shown who did what within the Risk Insight environment during the period at issue. The absence of this data makes it harder for FinancialApps to prove its case, which is the *sine qua non* of prejudice. *See Magnetar Techs. Corp. v. Six Flags Theme Park Inc.*, 886 F. Supp. 2d 466, 481 (D. Del. 2012). Defendants argue that there is no prejudice because FinancialApps's expert opines that the trade secret misappropriation is clear based on other evidence. (D.I. 625 at 16.) This argument misses the mark. There is no substitute for the Papertrail log data. The availability of other evidence might be relevant if that evidence was a replacement for the spoliated evidence. But it is not. Because the Papertrail ESI was highly relevant and unique, its loss caused prejudice to FinancialApps.

I also find that Defendants acted with an intent to deprive. I base this finding on several relevant facts. First, Defendants failed to follow their own document-hold notice. On June 13, 2019, Defendants circulated a document-hold notice requiring retention of "electronically stored information . . . wherever it may be stored," and noting that "potentially relevant data stored on a network, . . . or with a third party vendor . . . must be identified . . . immediately so that . . . the information can be preserved." (D.I. 616, Ex. 19.) Defendants testified that this document-hold notice covered all data contained in Risk Insight's third-party accounts, including Papertrail. (D.I. 616, Ex. 21 at 191:1–197:24; D.I. 616, Ex. 20 at 249:9–252:14.) Despite this hold notice covering the Papertrail ESI, Defendants made the intentional decision to cancel the subscription and allow the Papertrail ESI to be deleted. For instance, on July 15, 2019, Jeff Schulte of Yodlee reported that he had "ET" (Executive Team) clearance to proceed with a plan to decommission

third-party services that included Papertrail. (D.I. 616, Ex. 22.) Two days later, Mr. Schulte reported that they were proceeding with the plan after receiving approval from the executive leadership team. (*Id.*) Then on July 23, 2019, days after FinancialApps filed its complaint, an internal email stated that the Papertrail service had been “cancelled”:

| | | | | |
|------------|----------------|----------------|----------|----------|
| Papertrail | log management | Month to month | \$395/mo | Canceled |
|------------|----------------|----------------|----------|----------|

knew that Papertrail was log management software, that it related to Risk Insight, and that it cost a mere \$395/month to maintain the subscription.⁹

Second, Defendants selectively retained documents. Courts are more likely to find that the intent requirement is satisfied where a party preserves certain data but does not preserve other data. *Ronnie Van Zant, Inc. v. Pyle*, 270 F. Supp. 3d 656, 670–71 (S.D.N.Y. 2017) (preserving pictures but not text messages “evince[s] the kind of deliberate behavior that sanctions are intended to prevent and weigh[s] in favor of an adverse inference”). Here, Defendants had several meetings and unilaterally decided to preserve some data and decommission other data, including the Papertrail ESI. This tends to show intent to deprive. Indeed, this is not a case where data was accidentally or automatically deleted—Defendants assembled a task force overseen by senior management who made a list of subscriptions to cancel that included the Papertrail subscription. *Cf. Lokai Holdings LLC v. Twin Tiger USA LLC*, No. 15CV9363 (ALC) (DF), 2018 WL 1512055, at *1–2 (S.D.N.Y. Mar. 12, 2018) (finding no intent to deprive where emails were automatically deleted).

⁹ A main driver behind Defendants’ decommissioning of certain subscriptions related to Risk Insight was to reduce ongoing spend from \$30,000 per month to \$2,000 per month. (D.I. 616, Ex. 22.) If costs were a concern, Defendants should have reached out to FinancialApps about a cost-sharing arrangement rather than making a unilateral decision that resulted in deletion of relevant data.

Third, the timing of the decommissioning supports a finding of intent to deprive. Defendants cancelled the Papertrail subscription six days after FinancialApps filed its complaint. As other courts have found, such timing suggests an intent to deprive. *DVComm, LLC v. Hotwire Communications, LLC*, No. 14-5543, 2016 WL 6246824, at *1–3, *8 (E.D. Pa. Feb. 3, 2016) (“The timing here is instructive.”); *Lexpath Techs. Holdings, Inc. v. Welch*, No. 13-cv-5379-PGS-LHG, 2016 WL 4544344, at *5 (D.N.J. Aug. 30, 2016) (finding that the timing of the defendant’s deletion of responsive documents a few days after the plaintiff sent a cease-and-desist letter was “especially telling” and supported a finding of an intent to deprive), *aff’d*, 744 F. App’x 74 (3d Cir. 2018); *GN Netcom, Inc. v. Plantronics, Inc.*, 2016 WL 3792833, at *7 (D. Del. July 12, 2016) (granting the plaintiff’s motion for sanctions and relying in part on the “strongly suggestive” fact that the company’s executive instructed others to delete emails “just one month after [the] lawsuit was filed” and again “just one week after [the defendant’s] motion to dismiss was denied — at which point the commencement of fact discovery was imminent”).

In sum, Defendants’ intent to deprive is shown by the three types of circumstantial evidence noted above. Defendants issued a document-hold notice covering the Papertrail ESI, then made the unilateral decision to contradict the hold notice and delete the Papertrail ESI, and cancelled the subscription that necessarily resulted in deletion of the Papertrail ESI a few days after FinancialApps filed its complaint. Defendants argue that intent to deprive cannot be shown by circumstantial evidence alone. (D.I. 625 at 14.) But case law is clear that “[a] finding of intent to deprive may be based on circumstantial evidence.” *Folino v. Hines*, No. 17-1584, 2018 WL 5982448, at *3 (W.D. Pa. Nov. 14, 2018). The circumstances support a finding of intent to deprive the Papertrail ESI.

FinancialApps's proposed order requests two forms of relief. First, it requests leave to permit evidence of Defendants' spoliation at trial. Second, it requests an adverse inference that the jury may infer that the Papertrail ESI would have been unfavorable to Defendants and would tend to support FinancialApps's allegations.

When determining whether to grant sanctions and what sanction to award, courts in the Third Circuit consider (1) "the degree of fault"; (2) "the degree of prejudice"; and (3) "whether" a "lesser sanction" would "serve to deter such conduct by others in the future." *GN Netcom*, 930 F.3d at 82 (quoting *Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994)).

Defendants' degree of fault was not high enough to warrant the extreme sanction of dismissal or default judgment. Indeed, FinancialApps does not even request this form of sanction. Because I find that Defendants acted with an intent to deprive FinancialApps of use of the Papertrail ESI and the loss of the Papertrail ESI greatly prejudiced FinancialApps, I find that the only lesser sanction that would cure the prejudice and deter future conduct is to allow the factfinder¹⁰ to presume that the Papertrail ESI was unfavorable to Defendants. FinancialApps also requests an inference that the evidence would tend to support FinancialApps's allegations. This portion of the requested relief goes too far in my opinion and introduces uncertainty about what allegations the data would have tended to support. So I deny this portion of the requested relief. FinancialApps also requests leave to permit evidence of spoliation at trial. The sanction of permitting the factfinder to presume that the Papertrail ESI was unfavorable to Defendants

¹⁰ I say "factfinder" instead of "judge" or "jury" because at the present time separate trials are scheduled as to each defendant. This is because of a jury waiver provision in a contract between FinancialApps and Yodlee. It exceeds the duties delegated to me as a Special Master to say how to implement the sanction I recommend. Implementation is left to the wide discretion of the trial Judge.

assumes to some extent that evidence of the spoliation will need to be presented at trial. The factfinder will need to understand what the Papertrail ESI was and why it no longer exists. So I grant that portion of the requested relief, leaving the implementation to the sound discretion of the trial Judge.¹¹

B. I Recommend Denying the Portion of FinancialApps’s Spoliation Motion Concerning the AWS ESI

At the same time Defendants canceled the Papertrail subscription, they also decommissioned certain portions of the AWS environments. FinancialApps claims that Defendants spoliated the “sandbox,” “demo,” and “UAT” “environments” on the AWS “Stage” account. Defendants’ emails indicate that they did in fact decommission the AWS Stage Environments for the Risk Insight software. (D.I. 616, Ex. 22.) But the story is not that simple.

FinancialApps “sealed” the Risk Insight software in the Stage Environments using the Vault software. The parties dispute the effect of this sealing. Defendants point to deposition testimony from FinancialApps’s Mr. Priegues where he admits that FinancialApps used the Vault software to seal access to all environments. (D.I. 625 at 2.) Defendants also point to evidence that they and their clients could not access the environments. (*Id.* at 3–4.) Defendants then point to evidence that they did in fact preserve the data in the AWS Stage environments to the extent possible and produced that data to FinancialApps. (*Id.* at 4–5.)

FinancialApps has not shown by a preponderance of the evidence that Defendants had control of the data in the AWS Stage environments after FinancialApps used the Vault software to seal the Risk Insight software. The Priegues deposition testimony supports that sealing the

¹¹ Even if I had not found intent to deprive sufficient to warrant sanctions under Rule 37(e)(2), I would recommend awarding the sanction of presenting evidence of the Papertrail ESI spoliation at trial under Rule 37(e)(1) because of the prejudice to FinancialApps from being deprived of this highly relevant evidence.

software using Vault prevented access. (D.I. 626, Ex. 1 at 57:6–59:5.) His declaration submitted with this motion paints a different story. (D.I. 614 ¶¶ 15–16.) I find his deposition testimony more believable. Further, it would be unfair to fault Defendants for failing to preserve data from systems that FinancialApps actively prevented Defendants from accessing.

I am also not convinced that the AWS Stage data is actually lost. It may be possible to recreate the AWS Stage environments as they existed before sealing if the parties worked together to unseal the software and then rebuild the AWS environments using the data Defendants preserved. But that never happened. (April 29, 2025 hearing transcript at 50:17–51:3.) I deny this portion of FinancialApps’s motion for this additional reason.

Finally, I note that the record on the AWS Stage environments is muddled and confusing. It is unclear from FinancialApps’s briefing what data from the AWS Stage environments is missing and why it matters. Some of the confusion is caused by FinancialApps’s choice to combine the facts and arguments about alleged spoliation of the AWS Stage environments with the arguments about the separate Papertrail ESI. The confusing record also supports denying the motion. *See Manning v. Safelite Fulfillment, Inc.*, No. CV 17-2824 (RMB/MJS), 2021 WL 3557582, at *7 (D.N.J. Apr. 29, 2021), *report and recommendation adopted*, No. 17-2824 (RMB/MJS), 2021 WL 3542808 (D.N.J. Aug. 11, 2021) (“the Court declines to find spoliation as to ESI which has not been identified with specificity”).

II. I Recommend Denying Defendants’ Spoliation Motion

A. I Recommend Denying the Portion of Defendants’ Spoliation Motion Relating to the Website ESI

Defendants move for a spoliation finding as to FinancialApps’s Website. To prove spoliation, the movant has the burden to show that litigation was reasonably foreseeable and that the Website was “relevant to the claims or defenses in the case.” *Monolithic Power*, 2018 WL

6075046, at *1. Defendants have not met their burden, and therefore I deny this portion of their motion. More specifically, I find that FinancialApps had no duty to preserve the Website because litigation concerning FinancialApps's trade secrets was not reasonably anticipated when the Website was deleted on February 1, 2019.

The parties' dispute has two parts. The first part is a dispute about the amount of fees owed to FinancialApps under the MSA between the parties. The Website is irrelevant to this fee dispute. Thus, FinancialApps's apprehension of litigation about the fee dispute cannot trigger a preservation obligation as to evidence irrelevant to the fee dispute. The second part of the parties' dispute is a claim by FinancialApps that Defendants misappropriated certain trade secrets in creating a competing product. FinancialApps's duty to preserve the Website only arose when FinancialApps reasonably anticipated litigation about its trade secret misappropriation claim.

The parties disagree on when FinancialApps reasonably anticipated litigation about its trade secret misappropriation claim. Defendants argue that FinancialApps's preservation duty arose by October 2018, relying on a statement in FinancialApps's Complaint, deposition testimony from Mr. Sullivan and Mr. Carroll, and certain entries on FinancialApps's privilege log.

FinancialApps's Complaint alleges that "Yodlee's misconduct first came to light in October 2018, when Equifax Inc. (a leading credit bureau directly competing with Risk Insight) publicly announced that it had entered into a deal with Yodlee to 'simplify the mortgage loan process by making it easier for lenders to derive insights from borrowers' financial data,' however, neither FinancialApps nor the Risk Insight platform was mentioned in this announcement." (D.I. 7 ¶ 15.) FinancialApps says this sentence represents its knowledge following an investigation, which uncovered previously unnoticed wrongdoing by Defendants.

(D.I. 663 at 11.) And it was not until early 2019 that FinancialApps put the pieces together and realized this is when the misappropriation began. (*Id.*)

While FinancialApps’s explanation of paragraph 15 is not completely satisfying, the Complaint uses the term “misconduct” rather than “misappropriation” and thus could be referring to either or both of the fee dispute and trade secret misappropriation. So I do not find paragraph 15 dispositive as to when FinancialApps reasonably knew about the facts underlying its trade secret misappropriation claim. I also note that allegations in a complaint are just that—allegations. Allegations are not evidence.

Focusing on the evidence, I find Defendants’ proof lacking. After reviewing the 35 privilege log entries and the underlying documents submitted for *in camera* review, I confirmed that the privileged communications concerned the fee dispute and not the trade secret misappropriation dispute, and thus do not support Defendants’ argument. As to the deposition testimony of Bob Sullivan and Neil Carroll, after reviewing the cited testimony¹² and the surrounding pages, I think the testimony at most establishes that FinancialApps began having suspicions in late 2018 that something might be amiss regarding Yodlee’s conduct. But Sullivan testified that, while Yodlee was keeping him out of the loop in late 2018, he did not know why. (D.I. 659, Defs. Ex. 20 at 321:19–20.) And Carroll’s testimony supports the idea that it was not until later that he realized the Equifax deal was part of a plan to misappropriate trade secrets. (D.I. 659, Defs. Ex. 21 at 152:20–153:14.)

FinancialApps’s actions matched its position that it discovered the trade secret misappropriation in early 2019. Upon discovery, on May 17, 2019, FinancialApps sent a cease

¹² (D.I. 659, Ex. 20 at 315:22–316:11; 322:24–323:2; D.I. 659, Ex. 21 at 152:20–153:10; 315:22–316:11.)

and desist letter to Yodlee. (D.I. 659, Defs. Ex. 20.) The date of the cease-and-desist letter is particularly persuasive evidence because FinancialApps had no reason to delay in sending that letter and aggressively prosecuted its trade secrets misappropriation case after that date.

For all these reasons, Defendants did not prove by a preponderance of the evidence that a duty to preserve the Website arose before its deletion on February 1, 2019.

Even if the duty to preserve had arisen by late 2018, I would still deny this portion of Defendants' motion because there is insufficient evidence that the information in the Website was relevant to the trade secret misappropriation claim. FinancialApps's witness with knowledge of the Website, Mr. Weatherly, testified that nothing proprietary was ever on the Website, the information on the Website only pertained to early versions of the API, and the website was merely a promotional tool. (D.I. 659, Defs. Ex. 13 at 7:9–10:4; 26:7–10 (“...this is a publicly facing website. There's nothing proprietary on that, so it's available for anyone who has access to that URL”); 45:16–46:8; 73:6–7; D.I. 665, Ex. 8 at 15:12; 26:5–15; 50:7–14.) This evidence strongly suggests that nothing of relevance to the dispute was ever on the Website.

Defendants admit that they are required to provide a “plausible, concrete suggestion” of what might have been in the deleted Website. They argue that a June 28, 2017 email from Mr. Weatherly to someone who appears to be a potential customer of FinancialApps establishes that the Website contained the then-current API version. (D.I. 659, Defs. Ex. 14 (“Please find a link to our current API documentation.”).) But the link on its face is to version 2 of the API and not to version 3 that may include some of the trade secrets at issue in this case. (D.I. 665, Ex. 10 at ¶ 181.) So this email does not provide the connection Defendants need to establish relevancy of the Website by a preponderance of the evidence. In sum, Defendants have not established that

the “data dictionary” present on the Website as of 2016 is the Data Dictionary that purportedly contains FinancialApps’s trade secrets.

B. I Recommend Denying the Portion of Defendants’ Spoliation Motion Relating to the Dye NDA

Christian Dye was an independent contractor for FinancialApps. He started working with FinancialApps in March 2019. By email, he received a copy of at least part of what FinancialApps claims in this case to be its trade secrets. FinancialApps claims that Mr. Dye signed a non-disclosure agreement (NDA) prior to receiving the email containing at least some of the trade secrets. (D.I. 506 ¶¶ 7–11; D.I. 507 ¶¶ 4–7.) At the hearing, counsel for FinancialApps made clear that this NDA was signed in hard copy with a wet signature, and then stored by FinancialApps. (April 24, 2025 hearing transcript at 115:8–11.) At this point, the story gets fuzzy. FinancialApps has been unable to find the Dye NDA. FinancialApps posits that the NDA may have been lost during office moves in 2021 or 2022. But no one knows for sure.

Defendants are skeptical—as am I. They point out that Mr. Dye was a remote worker who was onboarded to the company remotely via a video call two days after allegedly signing an NDA. (D.I. 669 at 3.) These facts make it less believable that Mr. Dye signed the NDA with a wet signature and mailed it to FinancialApps. That said, all but one of the other NDAs produced by FinancialApps in this litigation were hard copies—so keeping only hard copies of NDAs seems to have been FinancialApps’s standard practice, as odd as that sounds. It is also odd that FinancialApps found hard copy NDAs signed by over 30 other individuals but could not locate the Dye NDA.

I expected to see testimony from Mr. Dye about whether or not he signed an NDA. But the record lacks any testimony from him. This may be a function of Defendants not raising the Dye NDA issue until expert discovery, after the close of fact discovery. Defendants claim that

they did not locate the email sending the Data Dictionary to Mr. Dye until expert discovery, but FinancialApps produced the email early in the fact discovery period. Defendants could have located it earlier and could have sought discovery from Mr. Dye, either during the fact discovery period or later with leave of Court. But they did not. Or it could be that FinancialApps chose not to contact Mr. Dye because they do not want to create an adverse record. I am left to wonder.¹³

The record is incomplete and inconsistent about whether the Dye NDA ever existed and, if it did exist, when and how it was lost. This leaves me with no choice but to deny Defendants' motion as to the Dye NDA without prejudice.

Other courts have denied spoliation motions in similar situations. *See Castellani v. City of Atl. City*, No. 13-5848 (JBS/AMD), 2016 WL 7155826, at *4 (D.N.J. Sept. 15, 2016) (“The Court is unable on the present record to determine whether there has been any bad faith with respect to the Final K9 Report. There is a factual dispute as to whether the document ever existed, and consequently, the Court cannot make any determinations as to whether there was any bad faith involved in the document’s destruction or non-production.”); *Thermotek, Inc. v. Orthoflex, Inc.*, No. 11-870, 2015 WL 4138722, at *12 (N.D. Tex. July 7, 2015) (denying without prejudice the defendant’s motion for spoliation sanctions where “disputed fact issues exist[ed] with respect to whether any relevant evidence was actually destroyed or not preserved and, if it was, whether the individuals charged with its destruction acted in bad faith[,]” and concluding further that “[t]he question of intent ultimately turns on factual matters which are best decided by the District Court in the context of the trial itself where the court can consider the precise nature

¹³ Although I am not the factfinder, the available evidence suggests that the Dye NDA never existed.

of the proof offered and the credibility of various witnesses”); *Frazier v. Bed Bath & Beyond, Inc.*, No. 10-5398, 2013 WL 1845499, at *7 (D.N.J. Apr. 30, 2013) (denying without prejudice the defendants’ motion for spoliation sanctions where “the charge rest[ed] on disputed facts”).

Setting aside the fact disputes, I also deny the Dye NDA portion of Defendants’ motion because Defendants have not met their burden to show bad faith or intent to deprive by clear and convincing evidence. There is no direct or circumstantial evidence in the record that FinancialApps intentionally suppressed or destroyed the Dye NDA. To the contrary, FinancialApps presented evidence that it took steps to preserve all relevant information, and preserved and produced over 30 other NDAs. (D.I. 663 at 15.)

Defendants point to FinancialApps’s litigation conduct to prove bad faith. While a party’s litigation tactics can reflect bad faith in certain situations,¹⁴ I find no evidence of bad-faith litigation tactics here by FinancialApps. Defendants claim that FinancialApps withheld the Dye NDA for all of fact discovery. (D.I. 669 at 5.) I do not find any evidence of intentional withholding of the Dye NDA. At worst, it appears that FinancialApps failed to locate the Dye NDA during a reasonable search that located almost all the other NDAs. This is not bad faith. Defendants also focus heavily on FinancialApps’s questioning of Defendants’ expert at deposition about whether Mr. Dye was an employee, when he was in fact an independent contractor. I reviewed the portion of the Ferrara video deposition cited by Defendants. I do not find the questioning to be anything close to litigation misconduct. I also saw no “manipulation” of the spreadsheet (D.I. 670, Ex. 35) that Defendants allege on page six of their reply brief. Defendants have not presented clear and convincing evidence of bad-faith litigation conduct.

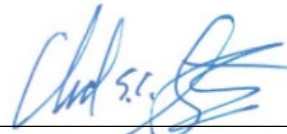
¹⁴ See *Baker Indus., Inc. v. Cerberus, Ltd.*, 764 F.2d 204, 208 (3d Cir. 1985).

CONCLUSION

As discussed above, I recommend that the Court grant-in-part the portion of FinancialApps's motion related to the Papertrail ESI and deny the remainder of both motions.

This Report and Recommendation is preliminarily submitted under seal as a precaution because various portions of the underlying briefing were marked highly confidential. Within seven business days of this Report, the parties shall jointly email the Special Master and advise of any proposed redactions.

Dated: August 7, 2025



Special Master Chad S.C. Stover