IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

FINANCIALAPPS, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 19-1337-CFC-CJB
	)	
ENVESTNET, INC. and YODLEE, INC.,	)	
	)	
Defendants.	)	

MEMORANDUM ORDER

Presently pending in this action is Plaintiff FinancialApps, LLC's ("Plaintiff" or "FinApps") motion seeking a Court order directing Defendants Envestnet, Inc. ("Envestnet") and Yodlee, Inc. ("Yodlee, and collectively with Envestnet, "Defendants") to comply with the Court's October 8, 2020 Order regarding FinApps' request for access to Defendants' Development and Operational Systems associated with the Competing Products (the "Motion"). (D.I. 258)[1]

I. BACKGROUND

The Court[2] here writes primarily for the parties, who are well familiar with the issues relating to the Motion.

In this action, FinApps asserts claims against Defendants for misappropriation of trade secrets, fraud, tortious interference with prospective business opportunities, unfair competition,

[1] While FinApps' letters with respect to the Motion reference "Defendants," (D.I. 260; D.I. 273), Defendants' letters reference Yodlee with respect to this issue, (D.I. 259; D.I. 269). Defendants explain that the issues relevant to the Motion "only" relate to Yodlee—"[n]one of [it] relates to Envestnet[.]" (D.I. 286 at 50; *see also, e.g.*, D.I. 262 at ¶ 1) In light of Defendants' representation, the Court will assume that this Motion relates to Yodlee only.

[2] On October 7, 2019, United States District Judge Colm F. Conolly referred this case to the Court to conduct all proceedings and to hear and determine all motions, pursuant to 28 U.S.C. § 636(b). (D.I. 18)

violation of state deceptive trade practices statutes, breach of contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment. (D.I. 2; D.I. 126) FinApps' claims arise out of an alleged "systematic scheme to copy, misappropriate, and 'reverse engineer' FinApps' proprietary technology in order to assist [Defendants'] secret development of several Competing Products [the 'Competing Products']" that compete with FinApps' products. (D.I. 134 at 1) According to FinApps, Defendants developed the Competing Products through the use of certain internal development and testing environments, third-party operational systems, and related tools (the "Development and Operational Systems"). (*Id.*)

In the Fall of 2020, the Court resolved a discovery dispute between the parties in which FinApps sought an order compelling "Defendants [to] provide access to, or otherwise make available for FinApps' review, the Development and Operational Systems associated with [the] Competing Products[.]" (*Id.*) On October 8, 2020, the Court issued an order agreeing with FinApps "that some form of access to Defendants' systems is warranted" but directing the parties to meet and confer regarding the "particulars with regard to such access" (the "Oct. 8 Order"). (D.I. 165) FinApps' instant Motion requests further relief with respect to the Oct. 8 Order, as will be described in more detail below.

The parties have submitted letter briefs and various declarations in connection with the Motion. (D.I. 259; D.I. 260; D.I. 261; D.I. 262; D.I. 269; D.I. 270; D.I. 271; D.I. 273; D.I. 274) On March 1, 2021, the Court heard argument from the parties during a teleconference. (D.I. 286 (hereinafter, "Tr."))

II. STANDARD OF REVIEW

Federal Rule of Civil Procedure 34 outlines the procedures through which a party must produce electronically stored information. Fed. R. Civ. P. 34. The Rule requires that such information be produced “in a form [] in which it is ordinarily maintained or in a reasonably usable form[.]” Fed. R. Civ. P. 34(b)(2)(E)(ii). Rule 34’s 2006 advisory committee notes explain that the production should be made in such a form as to “protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party.” Fed. R. Civ. P. 34(b) advisory committee’s note to 2006 amendment. At the same time, the 2006 advisory committee notes also point out that Rule 34(a)’s addition of testing and sampling with regard to documents and electronically stored information “is not meant to create a routine right of direct access to a party’s electronic information system, although such access might be justified in some circumstances[,]” because “[i]nspection or testing ... of a responding party’s electronic information system may raise issues of confidentiality or privacy.” Fed. R. Civ. P. 34(a) advisory committee’s note to 2006 amendment.

With respect to electronically stored information, Federal Rule of Civil Procedure 26(b)(2)(B) also provides:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery . . . the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Fed. R. Civ. P. 26(b)(2)(B); *see also, e.g.*, *Knightly v. CentiMark Corp.*, 2:19-cv-00304-RJC, 2020 WL 1532330, at *1 (W.D. Pa. Mar. 31, 2020).

III. DISCUSSION

FinApps now requests an order compelling Yodlee to either provide adequate “remote access” to two key Development and Operations Systems, or to provide a clear explanation as to why such access cannot be provided or no longer exists. (D.I. 260 at 1, 3) The two systems at issue are Yodlee's JIRA system used to develop its Competing Products,[3] and its QA/Testing environments and related DAG and IQBank data used to test the functionality of the Competing Products.[4] (*Id.* at 1) FinApps seeks access to the JIRA system in a "complete format equivalent to the manner in which it was maintained and used . . . to develop [the] Competing Products[.]" (*Id.* at 2; *see also* D.I. 261 at ¶ 9) Similarly, it seeks access to the QA/Testing environments and related DAG and IQBank data "in a manner that reflects how such environments and data were maintained and used in the normal course by Defendants' developers[.]" (D.I. 260 at 3; *see also* D.I. 261 at ¶ 24)

What has Yodlee produced to date with respect to these two systems, and why does FinApps assert that this production is inadequate?

First, with regard to the JIRA system, Yodlee has produced spreadsheet "exports" of JIRA data, as well as JIRA "tickets" and e-mails that reference and describe JIRA projects. (D.I. 260 at 2; *id.*, ex. B at 8; D.I. 259 at 3; D.I. 261 at ¶ 15; D.I. 262 at ¶ 10; D.I. 269 at 1) FinApps contends that: (1) this production contains "significant gaps in data" due to the omission of many screenshots, attachments and entire JIRA projects relating to the Competing Products; and (2) "exporting" this information will necessarily always result in just such gaps in data; such that (3) only remote access will allow FinApps to search the JIRA system in a full and complete way.

[3] FinApps asserts that the JIRA system "is one of the most important and critically relevant repositories of information in this case concerning the development of the Competing Products[.]" (D.I. 260, ex. C at 4; *see also* Tr. at 51) FinApps asserts that the DAG and IQBank test data "is of central relevance to this case" in light of FinApps' belief that Defendants relied on this data "to conduct comparative testing to ensure that Snapshot 2.0 and the Equifax VOA/MVP generated output identical to Risk Insight 2.0[.]" (D.I. 260, ex. C at 3)

[4] These systems were utilized in the development of at least two Competing Products: Snapshot 2.0 and the Equifax VOA/VMP product. (D.I. 260 at 1; *id.*, ex. A at 11-12)

(D.I. 261 at ¶¶ 16-17; *see also* D.I. 260, ex. B at 2, 9; *id.*, ex. C at 4, 7-8; D.I. 273 at 4; Tr. at 19-20, 27)

Second, with regard to QA/Testing environments and related DAG/IQBank testing data, Yodlee provided "customer level" access to certain Snapshot environments. (D.I. 260 at 2; D.I. 261 at ¶¶ 26, 30) For its part, Yodlee asserts that with respect to these environments: "[a]ny data that was retained or stored by the developer for Snapshot 2.0 and the Equifax VOA/MVP project has been produced to the extent it exists in shared databases, as well as recorded in various emails, tickets, spreadsheets and reports." (D.I. 262, ex. G at 3) But FinApps counters that Yodlee's production is deficient because Yodlee did not provide access to the same environments that Defendants' developers used. (D.I. 260 at 2; D.I. 261 at ¶¶ 26, 30; Tr. at 30) FinApps contends that the environments to which Yodlee provided access post-dated the period during which development and testing of the Competing Products occurred. (D.I. 261 at ¶¶ 27-28; Tr. at 30-31) Finally, FinApps notes that Defendants have suggested that certain relevant DAG data has not been preserved. (D.I. 260 at 2; *id.*, ex. E at 3)

In light of the purported deficiencies set out above, FinApps is now asserting that it should be given "remote access" to Yodlee's JIRA and its QA/Testing environments and to related DAG and IQBank data. In FinApps' view, only if it is provided with such access will it be able to access all of the critical information that it needs to help prove its case.

Yodlee counters by arguing that providing FinApps with "unfettered remote access" to its systems is "simply not reasonable[,]" because Yodlee's systems are subject to "bank-level security[.]" (D.I. 269 at 2; *see also* D.I. 259 at 3; D.I. 260, ex. B at 8 ("In the abstract, it's difficult and burdensome for our client to allow unfettered access into these databases due to the bank-level security of most of this."); Tr. at 42) Yodlee's Vice President of Data Strategy &

Strategic Solutions, Brian Costello, also submitted a declaration that attempts to provide support for Yodlee's assertion. Mr. Costello's declaration states that many of Yodlee's customers are financial institutions, and that a requirement of Yodlee's contracts with those clients is the ability to represent "that it has a security level that meets various standards and audits ('bank level security')." (D.I. 270 at ¶ 2) Mr. Costello further asserts that providing remote access to certain Yodlee databases:

> would violate Yodlee's prescribed security posture, breaching the confidentiality and integrity of our systems and triggering noncompliance with our regulatory and contractual requirements. This non-compliance could rise to a reportable event, further impacting Yodlee's legally mandated security posture and the commercial considerations that depend upon it. If there is a breach in security during or as a result of a remote access review as requested (even if through no fault of Financial Apps' experts), the damage to Yodlee would be incalculable.

(*Id*. at ¶ 11)

For both systems at issue, Yodlee has informed FinApps that it "will consider further searches based upon specific identification by [FinApps] of information, an explanation of its relevancy and why that information is not available in previously produced documents." (D.I. 260, ex. E at 2-3; *see also* D.I. 269 at 1-2) Moreover, "[a]s a compromise," Yodlee stated that it is "investigating the feasibility of permitting [FinApps] to examine the environments at a secure location and subject to the Source Code Protocol." (D.I. 269 at 3; D.I. 262 at ¶ 14; D.I. 271 at ¶ 16)

This is not an easy issue. The amendments to Rule 34 encourage caution before a Court permits direct access to a party's electronic systems. *See Scotts Co. LLC v. Liberty Mut. Ins. Co*., Civil Action No. 2:06-CV-899, 2007 WL 1723509, at *2 (S.D. Ohio June 12, 2007). Moreover, no Court ever wants to issue a discovery order that would harm a party's business, and here

Yodlee has at least asserted that providing remote access to its systems would (or, at least *could*) do just that. And Yodlee has also claimed that were FinApps provided with access to "developer level" environments with respect to QA/Testing environments and related DAG/IQBank testing data, this would require allowing FinApps access to the actual laptop computers that are used by Yodlee's software engineers[,] (D.I. 269 at 2; D.I. 271 at ¶¶ 11-13); Yodlee argues that FinApps has not directly addressed why it should be permitted access to the laptops of these engineers.

But on the other hand, FinApps' expert, Isaac J. Pflaum, has submitted declarations that clearly explain why Yodlee's productions with respect to the two systems at issue in this Motion are deficient. (D.I. 261 at ¶¶ 15-20, 25-31) Mr. Pflaum has further asserted that meaningful reviews (1) of JIRA would require "direct read-only access to both a JIRA database and its related attachments folder;" and (2) of QA/Testing environments and related DAG/IQBank testing data would require "access to the same systems, test data, and supporting databases that were actually used to test and develop the software at issue." (D.I. 274 at ¶ 5; *see also* D.I. 261 at ¶¶ 9-12, 24; Tr. at 27) Moreover, to the extent that Yodlee is arguing that the requested access would amount to an "undue burden" on it, *see* Fed. R. Civ. P. 26(b)(2)(B), its showing in that regard could have been more robust. That is, Yodlee (via Mr. Costello's declaration) did not really explain in great detail exactly *how and why*: (1) "bank-level security" applies to the specific systems at issue in this Motion, or (2) providing remote access would amount to a "reportable event[,]" would result in a security breach, or would contravene any federal or state law, or (3) any resulting damage would be "incalculable" to Yodlee. (D.I. 270 at ¶ 11); *see also* D.I. 273 at 3; Tr. at 21, 51-52 (Plaintiff's counsel noting that in Mr. Costello's declaration, "[t]here's nothing in there that says how our remote access to the testing environments would in any way implicate bank-level security, whatever that means"))

In light of this, for now the Court believes that the most reasonable course is for the parties to proceed with Yodlee's proposal for an off-site JIRA and QA/Testing environment review. (D.I. 259 at 1; D.I. 273 at 4) FinApps has *agreed* to this proposal, at Defendants' expense and subject to the satisfaction of certain technical requirements, including confirmation that the review would not be subject to the restrictions set forth in the parties' source code protocol. (*Id.*; D.I. 262, ex. M)[5] In response, Yodlee first requested that "the Court require any off-site inspection to be subject to the agreed-upon source code inspection protocol and that FA should be required to share the cost." (D.I. 269 at 3 n.4) But at oral argument, Yodlee seemed to soften its stance with respect to the source code protocol, arguing only that Yodlee "just want[s] some control over what's being copied. In other words, [FinApps' expert] can't just make copies and take them on his own. [Yodlee is] entitled to get copies of what [FinApps' expert] copies and stamp them confidential[.]" (Tr. at 48) This specific ask with respect to copying seems reasonable. But in the absence of any further argument as to why the entire source code protocol should apply to this review (and given FinApps' expert's explanation of how application of the source code protocol to these non-source-code systems would be inefficient), the Court will not require this review to be subject to any further source code restrictions. (D.I. 274 at ¶¶ 5-9)[6]

For the reasons set forth above, Yodlee shall permit FinApps to examine the environments at issue in this Motion at a secure location and subject to the "certain specific

[5] These restrictions are set forth in the parties' First Supplemental Protective Order to Govern Access to Source Code. (D.I. 129)

[6] With respect to the parties' dispute over how the cost of Yodlee's proposal should be allocated, the Court will not make a ruling at this time. The parties did not provide any detail or argument with respect to the cost issue. To the extent that the parties continue to dispute how cost of the review should be allocated, they can raise the issue through the Court's discovery dispute procedures.

caveats" set out by FinApps. (D.I. 262, ex. M) To the extent that such access to Yodlee's JIRA system and QA/Testing environments and related DAG and IQBank data cannot be provided, Yodlee shall provide the Court and FinApps with a substantive explanation "as to why such access or information cannot be provided, or no longer exists" by **April 27, 2021**. (D.I. 260 at 3)[7] The Court expects that the parties will work cooperatively to facilitate this review as expeditiously as possible. If the above-referenced access to the system cannot be provided, the Court will consider then whether FinApps is due further relief.

IV. CONCLUSION

For the reasons set out above, the Court hereby ORDERS that FinApp's Motion is GRANTED-IN-PART in the manner set out above.

Because this Memorandum Order may contain confidential information, it has been released under seal, pending review by the parties to allow them to submit a single, jointly proposed, redacted version (if necessary) of the document. Any such redacted version shall be submitted by no later than **April 16, 2021** for review by the Court, along with a motion for redaction that includes a clear, factually detailed explanation as to why disclosure of any proposed redacted material would "work a clearly defined and serious injury to the party seeking closure." *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 786 (3d Cir. 1994) (internal quotation

[7] Yodlee's counsel asserted that the "fundamental question" and "problem" with respect to Yodlee's compromise proposal is that FinApps will want this for the "eight or nine" other Yodlee systems that have been identified as relevant to this litigation. (Tr. at 48; *see also* D.I. 259 at 3 n.3; D.I. 269 at 1 n.1) The issue of access to those other systems, however, is not presently before the Court, and the Court issues no ruling with respect to such systems. It is not clear to the Court: (1) what has been provided with respect to those systems; (2) whether or not FinApps asserts that such production has been insufficient; (3) how important these other systems are with respect to the Competing Products; or (4) what the combined burden would be on Yodlee to permit such access to all of those systems.

marks and citation omitted). The Court will subsequently issue a publicly-available version of its Memorandum Order.

Dated: April 13, 2021

Christopher J. Burke

Christopher J. Burke
UNITED STATES MAGISTRATE JUDGE