UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	2:17-cv-04062-SVW-SS	Date	May 13, 2020
Title	*Calendar Research LLC v. StubHub, Inc. et al*		

Present: The Honorable	STEPHEN V. WILSON, U.S. DISTRICT JUDGE	
Paul M. Cruz		N/A
Deputy Clerk		Court Reporter / Recorder
Attorneys Present for Plaintiffs:		Attorneys Present for Defendants:
N/A		N/A

Proceedings: IN CHAMBERS ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTIONS FOR SUMMARY JUDGMENT [334] [340] [341]

I. Factual and Procedural Background

The facts of this case have been recounted extensively in the Court's previous Orders. *See* Dkt. 47; Dkt. 160; Dkt. 175. For clarity, the salient facts are briefly recounted here. Defendant Michael Hunter Gray ("Gray") was a co-founder and CEO of a start-up called Calaborate, which developed a group-scheduling mobile application (app) called Klutch. Several Calaborate employees, including Vice President of Engineering, Lisa Dusseault ("Dusseault"), and developer Lasha Efremidze ("Efremidze") also worked extensively on the Klutch app for Calaborate. Together, Gray, Dusseault, and Efremidze are the "Individual Defendants" in this case. Between 2014–15, Knight & Bishop[1] invested over $800,000 in Calaborate. Mark Kolokotrones ("Kolokotrones") served as a Managing Member of Knight & Bishop and a Director on the Board of Calaborate.

Gray tried to sell Calaborate along with its mobile app, Klutch. His most successful attempt was to StubHub, Inc. ("StubHub") which is owned by its corporate parent eBay, Inc. ("eBay"). Together StubHub and eBay are the "Corporate Defendants" in this case. The deal did not go through, however,

[1] Knight & Bishop LP ("Knight & Bishop") is an investment firm, and Knight & Bishop GP, LLC is the general partner of Knight & Bishop.

Initials of Preparer : PMC

and the Individual Defendants left Calaborate to work as independent contractors for StubHub. Because Calaborate was not purchased by StubHub, ownership of the Klutch app remained with Calaborate until the company was purchased by Calendar Research ("Plaintiff") in a foreclosure sale via a credit bid. Dkt. 370-1, Defendants' Statement of Undisputed Fact ("SUF") ¶ 48. Kolokotrones is a manager of Calendar Research and played a substantial role in Calendar Research's formation and acquisition of the Calaborate/Klutch assets.

Before the Court are Plaintiff's claims under the Defend Trade Secrets Act ("DTSA"), 18 U.S.C. §§ 1830–1839, and the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. After extensive litigation, this Court granted partial summary judgment to the Corporate Defendants on Plaintiff's DTSA claims regarding the Calaborate source code because the Court concluded there was no genuine issue of material fact that StubHub had not misappropriated any of Plaintiff's source code in StubHub's applications. Dkt. 160 at 16. The Court further concluded that "the Klutch code is not a protectable trade secret, even as a compilation." *Id.* The Court then lifted the stay on discovery regarding Plaintiff's CFAA claims.[2] *Id.* In a subsequent Order, the Court clarified that "the Court's findings in its summary judgment order applied equally to all Defendants, not just StubHub. No defendant can be held liable for their role in the 'use' of Klutch source code in StubHub applications when the Court determined as a matter of law that the Klutch code was not used in any StubHub application." Dkt. 175.

The Court further noted that the "summary judgment order does not preclude Plaintiff from asserting a DTSA claim that StubHub misappropriated the Klutch code in different ways than using the code in its own applications." Dkt. 175. In granting partial summary judgment, the Court held that "Plaintiff is permitted to allege DTSA claims regarding the acquisition, use, or disclosure of other non-code trade secrets, such as 'Calaborate's computer programs, coding methodologies computer techniques, and related concepts and know-how.'" *Id.* at 2 (quoting the Fifth Amended Complaint, Dkt. 181). But Plaintiff was strongly cautioned "that it must define these trade secrets with greater specificity when conducting discovery and when asserting the existence of a trade secret in future briefing. Plaintiff's complaint may have been sufficient to withstand a motion to dismiss, but Plaintiff's vagueness as to the nature of these non-code trade secrets would not create a triable claim under the DTSA." *Id.* at 2.

[2] As clarified in the previous Order, Plaintiff's state law claims for breach of contract and under the California Uniform Trade Secrets Act ("CUTSA"), Cal. Civ. Code § 3426 *et seq.*, have been stayed. Dkt. 175 at 3. The parties have agreed Plaintiff's Electronic Espionage Act ("EEA") claims are duplicative of Plaintiff's DTSA claims, and the Court accordingly dismissed the EEA claims. *Id.*

Initials of Preparer : PMC

What remains before this Court are Plaintiff's non-code based DTSA claims and the CFAA claims against all Defendants. Dkt. 175. Gray and Efremidze have jointly moved for summary judgment as to all remaining claims. Dusseault and the Corporate Defendants have also separately moved for summary judgment as to all remaining claims. Plaintiff has opposed all three motions.[3] Based on the discussion provided below, the Court determines that Plaintiff has failed to sufficiently identify any protectable trade secret under the DTSA. Plaintiff has also failed to produce sufficient evidence to create a triable issue of fact on all but one of its CFAA claims. As explained later, one narrow issue of fact remains—whether Efremidze archived his Calaborate email account without authorization on April 13, 2015. Accordingly, the Court GRANTS all Defendants' motions for summary judgment as to the DTSA claims, and GRANTS in part and DENIES in part Defendants' motion for summary judgment as to the CFAA claims.

II. Legal Standard

A motion for summary judgment under Federal Rule of Civil Procedure 56(a) is appropriate "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The party seeking summary judgment "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of . . . [the record that] demonstrates the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). "If a party moves for summary judgment with respect to a matter as to which the opposing party has the ultimate burden of persuasion at trial, then the moving party must show that the opposing party cannot meet its burden of proof at trial by establishing that there is no genuine issue of material fact as to an essential element of the opposing party's claim or defense . . . ." *Hill v. Skywest Airlines, Inc.*, No. 06-CV-00801-SMS, 2007 WL 2326070, at *2 (E.D. Cal. Aug. 14, 2007) (citing *Nissan Fire Ltd. v. Fritz Cos., Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000)). Once the movant meets this initial burden, the burden shifts to the nonmovant to demonstrate with admissible evidence that genuine issues of material fact remain and preclude summary judgment. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 585–86 (1986). A material fact is one that could affect the outcome of the suit, and a genuine issue is one that could permit a reasonable jury to enter a verdict in the non-moving party's favor. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). "The court must examine all the evidence in the light most favorable to the nonmoving party,

[3] Although briefed as two separate motions, Plaintiff submitted one combined opposition to the Individual Defendants' motions for summary judgment. Plaintiff also improperly incorporates by reference its arguments against the Individual Defendants into its opposition to the Corporate Defendants' motion for summary judgment. To avoid further delay in this litigation, the Court considers Plaintiff's arguments in both oppositions as to all Defendants.

and draw all justifiable inferences in its favor." *VBS Distribution, Inc. v. Nutrivita Labs., Inc.*, No. 16-CV-1601553-CJC-DFM, 2018 WL 5274172, at *2 (C.D. Cal. Sept. 10, 2018) ("*VBS*") (citing *Anderson*, 477 U.S. at 256).[4] "But conclusory and speculative testimony in affidavits and moving papers is insufficient to raise triable issues of fact and defeat summary judgment." *Id.* (citing *Thornhill Pub. Co., Inc. v. GTE Corp.*, 594 F.2d 730, 738 (9th Cir. 1979)).

Under Local Rules 56-2 and 56-3, material issues of fact must be identified in the non-moving party's "Statement of Genuine Issues" and supported by "declaration or other written evidence." *See also Sullivan v. Dollar Tree Stores, Inc.*, 623 F.3d 770, 779 (9th Cir. 2010) ("Federal Rule of Civil Procedure 56(e)(2) requires a party to 'set out specific facts showing a genuine issue for trial.'"). If the non-moving party fails to identify the triable issues of fact, the court may treat the moving party's evidence as uncontroverted, if the facts are "adequately supported" by the moving party. Local Rule 56-3; *see also Int'l Longshoremen's Ass'n, AFL-CIO v. Davis*, 476 U.S. 380, 398 n.14 (1986) ("[I]t is not [the Court's] task sua sponte to search the record for evidence to support the [parties'] claim[s].").

The importance of Plaintiff's opposition briefing and accompanying "Statement of Genuine Issues" is especially pronounced in trade secret cases, where "[a] plaintiff seeking relief for misappropriation of trade secrets 'must identify the trade secrets and carry the burden of showing that they exist.'" *Imax Corp. v. Cinema Techs., Inc.*, 152 F.3d 1161, 1164–65 (9th Cir. 1998) ("*Imax*") (quoting *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir.1993)). "The plaintiff 'should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons . . . skilled in the trade.'" *Id.* (quoting *Universal Analytics v. MacNeal–Schwendler Corp.*, 707 F. Supp. 1170, 1177 (C.D.Cal.1989)).

It is Plaintiff's burden to "clearly identify the information" that allegedly constitutes a trade secret in its briefing and supporting evidence. *Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 702 (9th Cir. 2017). "A lawyer drafting an opposition to a summary judgment motion may easily show a judge, in the opposition, the evidence that the lawyer wants the judge to read. It is absurdly difficult for a judge to perform a search, unassisted by counsel, through the entire record, to look for such evidence." *Carmen v. San Francisco United Sch. Dist.*, 237 F.3d 1026, 1029 (9th Cir. 2001); *see also Carrillo v. Cty. of Los Angeles*, No. 11-CV-10310, 2012 WL 12850128, at *5 (C.D. Cal. Nov. 14, 2012), *aff'd*, 798 F.3d 1210 (9th Cir. 2015). If Plaintiff's opposition fails to sufficiently identify a factual dispute regarding a material element of its claim, summary judgment may appropriately be granted to the Defendants. "Indeed, summary judgment should be entered, after adequate time for discovery and upon motion, against a party who fails to make a showing sufficient to establish the existence of an element essential

[4] Reversed on other grounds by *VBS Distribution, Inc. v. Nutrivita Labs.*, Inc., No. 18-56317, 2020 WL 2086557, at *3 (9th Cir. Apr. 30, 2020).

Initials of Preparer : PMC

to that party's case, and on which that party will bear the burden of proof at trial." *Hill*, 2007 WL 2326070, at *2 (citing *Celotex*, 477 U.S. at 323).

III. Analysis

a. The Defend Trade Secrets Act

Federal law defines "trade secrets" as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes." 18 U.S.C. § 1839(3). To succeed in a trade secrets claim, Plaintiff must show "(1) it possessed a trade secret; (2) [Defendants] misappropriated the trade secret; and (3) [Defendants'] misappropriation caused or threatened damage to [Plaintiff]." *Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 703 (9th Cir. 2017) (citing Cal. Civ. Code § 3426).[5]

"A plaintiff seeking relief for misappropriation of trade secrets 'must identify the trade secrets and carry the burden of showing that they exist.'" *Founder Starcoin, Inc. v. Launch Labs, Inc.*, No. 18-CV-972 JLS (MDD), 2018 WL 3343790, at *5 (S.D. Cal. July 9, 2018) ("*Founder Starcoin*") (quoting *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir. 1993)). The distinction between general industry knowledge in a complex field and a specific trade secret is inherently difficult, and "it is unlikely that the district court or any trier of fact would have expertise in discerning exactly which" technical information constitutes a "trade secret[]" without precise guidance from the plaintiff. *Imax*, 152 F.3d at 1161. As such, "[t]he plaintiff 'should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons . . . skilled in the trade.'" *Id.* at 1164–65 (quoting *Universal Analytics*, 707 F. Supp. at 1177). "Put another way, '[a] plaintiff must do more than just identify a kind of technology and then invite the court to hunt through the details in search of items meeting the statutory definition

[5] Plaintiff's CUTSA and other state law claims have been stayed by the Court, but as discussed in the previous Order, cases interpreting CUTSA can be persuasive in interpreting DTSA claims. *See* Dkt. 160 at 5. Accordingly, as the DTSA was only passed in 2016, many cases in this Order discuss interpretations of the CUTSA, the Electronic Espionage Act ("EEA") and other relevant trade secret common law. *Founder Starcoin, Inc. v. Launch Labs, Inc.*, No. 18-CV-972 JLS (MDD), 2018 WL 3343790, at *4 (S.D. Cal. July 9, 2018) ("As other district courts in this circuit have recognized, the definitions of trade secret and misappropriation are virtually the same in both the federal DTSA, 18 U.S.C. § 1839, and the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426.1."). "Accordingly, federal district courts in California have applied California's trade secret case law to causes of action brought under the federal DTSA." *Id.*

[of a trade secret].'" *X6D Ltd. v. Li-Tek Corps. Co.*, No. 10-CV-2327-GHK-PJW, 2012 WL 12952726, at *1 (C.D. Cal. Aug. 27, 2012) ("*XD6*") (quoting *Imax*, 152 F.3d at 1163–64). "[U]nless the plaintiff engages in a serious effort to pin down the secrets a court cannot do its job." *Id.* (quoting *IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581, 583 (7th Cir. 2002)).

In this case, Plaintiff faces several additional challenges. First, considering the previous Order granting partial summary judgment, Plaintiff has not directed the Court to any evidence that the Klutch source code constitutes a trade secret. *See* Dkt. 160. Although code comparison is not the only way to prove trade secret misappropriation in technology cases, it is one of the most clear-cut methodologies.[6] *See Brookhaven Typesetting Servs., Inc. v. Adobe Sys., Inc.*, 2007 WL 2429653, at *11 (N.D. Cal. Aug. 24, 2007), *aff'd*, 332 F. App'x 387 (9th Cir. 2009) (holding that where a similar source-code discovery was ordered and there was a vague comparison that was not based in code, the court could grant summary-judgment for defendants); *see also* Dkt. 160 at 14 ("The Court notes that code, being the language that creates the entire app, provides a fairly clear picture of what information and ideas moved between two parties."). The previous Order determined that the Klutch source code was not a trade secret, and Plaintiff has not presented evidence or argument of any new source code for the Court to consider as a trade secret.[7] Dkt. 160. Accordingly, the Court considers the previous ruling as undisturbed—the Klutch source code is not a trade secret. *Id.*

Second, since the Individual Defendants do not identify any trade secrets they developed while creating the Klutch app, Plaintiff must rely on post-hoc expert review to discern which trade secrets (if any) were involved in its creation. But Plaintiff is the owner of Calendar Research's assets and the master of the complaint; there can be no question that Plaintiff has had the full machinery of the justice system at its disposal to pursue this claim. *See XD6*, 2012 WL 12952726, at *8 ("this is a substantive issue on which Plaintiffs bear the burden of proof, and Plaintiffs are the only ones in possession of the evidence with which to do so."); s*ee also Loop AI Labs Inc. v. Gatti*, 195 F. Supp. 3d 1107, 1116 (N.D. Cal. 2016) ("*Loop AI Labs*") ("Plaintiff does not explain how it needs discovery from Defendants in

[6] In the previous Order, the Court noted "that the parties, particularly Plaintiff, previously focused the Court on the Klutch source code as the essence of Plaintiff's case for its DTSA claim, especially at the August 14, 2017 hearing. However, the 'essence' of Plaintiff's DTSA claim does not equate to the 'entirety' of the claim. The Court never expressly restricted Plaintiff's DTSA claims to only the source code." Dkt. 175 at 2.

[7] As discussed *infra* Part II.a.iv.2, Plaintiff claims that Dusseault retained Klutch source code on her laptop, but does not offer any explanation for how that code differs from the source code the Court already determined was not a trade secret. Dkt. 387 at 10.

order to identify with particularity its own trade secrets that it has put at issue in this case."). After over three years of litigation, two rounds of in-depth discovery spanning hundreds of thousands of documents, and supplemental briefing on privileged materials, any evidentiary failure can only be attributed to Plaintiff, who will bear the overall burden of persuasion at trial. *Hill*, 2007 WL 2326070, at *2 (citing *Matsushita*, 475 U.S. at 586).

Plaintiff now asserts that Defendants' "know-how" and "learnings" are trade secrets. Dkt. 170. These are nebulous concepts that, unless clearly defined, encounter the long-standing tension between employment law and the trade secrets doctrine. "To prevent employers from using trade secret law as a weapon against employee mobility . . . 'a party seeking to protect trade secrets [must] describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade, and to permit defendant to ascertain at least the boundaries within which the secret lies.'" *Mattel, Inc. v. MGA Entm't, Inc.*, 782 F. Supp. 2d 911, 967 (C.D. Cal. 2011) (citing *Whyte v. Schlage Lock Co.*, 125 Cal.Rptr.2d 277 (2002)). This principle echoes throughout trade secret jurisprudence. *See Hollingsworth Solderless Terminal Co. v. Turley*, 622 F.2d 1324, 1329–30 (9th Cir. 1980) (quoting *Mathews Paint Co. v. Seaside Paint and Lacquer Co.*, 306 P.2d 113, 115, 117 (Cal. 1957)) ("Some knowledge gained by an employee is of such a general character that equity will not restrict its later use . . . . A salesman who leaves one employer has a right to enter the employment of a competitor. He necessarily is possessed of information gained in the earlier employment which will enable him to better succeed in later ones."); *Cont'l Car-Na-Var Corp. v. Moseley*, 148 P.2d 9, 11 (Cal. 1944) (a former employee is "entitled to make use of his general knowledge of [the field] for the defendant corporation so long as he did not transgress upon the 'trade secrets' or secret formulae of plaintiff").

This tension is especially prominent in trade secret cases "involving technical or scientific information such as this one, [where Plaintiff has] supported [its] trade secret disclosures with declarations by expert witnesses which attempt to distinguish the alleged trade secrets from information already known in the field." *Loop AI Labs*, 195 F. Supp. 3d at 1115. "[W]here alleged trade secrets 'consist of incremental variations on, or advances in the state of the art in a highly specialized technical field, a more exacting level of particularity may be required to distinguish the alleged trade secrets from matters already known to persons skilled in that field.'" *Id.* (quoting *Advanced Modular Sputtering, Inc. v. Superior Court*, 33 Cal. Rptr. 3d 901 (Ct. App. 2005)).

These obstacles may explain, but do not excuse, Plaintiff's failure to sufficiently define its trade

Initials of Preparer : PMC

secrets. In its oppositions, Plaintiff has identified "four distinct categories" of trade secrets: "(1) Virality Capabilities; (2) UI/UX and Design; (3) Venue Focus; and (4) Integration of Third-Party Apps." Dkt. 370 at 1. Plaintiff's expert, Monty Myers ("Myers"), provided expert testimony regarding "Virality Capability" in his report and subsequent declaration, but Myers made little to no mention of the other three alleged trade secrets. Ultimately, as explained below, Plaintiff fails to define any of these categories with sufficient specificity to constitute a trade secret. Further, Plaintiff has failed to provide non-speculative evidence that these alleged trade secrets ever existed. As such, Plaintiff has not raised a genuine issue of material fact, and summary judgment is appropriate as to all Defendants on Plaintiff's DTSA claims.

i. Viral Capability/Virality API

Plaintiff claims that while working for Calaborate, the Individual Defendants developed the Klutch app with "Virality Capabilities" that constitute a trade secret. Dkt. 365 at 3. Plaintiff defines "virality" as the "ability of the application to grow its user base organically with user-to-user interactions, rather than through marketing." [8] Dkt. 370 at 2. Although Klutch was not a viral app, Plaintiff emphasizes that Klutch had the *capability* to go viral, and that capability constitutes a trade secret.

1. Definition

Without a sufficiently precise definition, the general concept of "Virality Capabilities" is too vague to constitute a trade secret—every application capable of being shared has the capacity to go viral in some sense. *See Loop AI Labs*, 195 F. Supp. 3d at 1111 ("trade secret law protects the right to maintain the confidentiality of facts, not ideas").[9] Trade secrets cannot be vague concepts, and Plaintiff fails to identify the specific set of "methods, techniques, processes, procedures, programs, or codes" that could establish Klutch's purported Virality Capability as a trade secret. 18 U.S.C. § 1839(3). Plaintiff claims that "Virality Capabilities refers to the *overall combination* of factors, datapoints, methodologies, and areas of emphasis that permitted the team to track the various virality metrics, and to determine if their efforts were

[8] There can be no dispute that Klutch never went "viral" by any reasonable definition of the word. At most, Plaintiff argues that Klutch had an "even or rising trend" of user growth. Dkt. 370-1 SUF ¶ 27; Dkt. 301-8 at 417. Even then, Myers admits that the trend was downward in late 2016. Dkt. 301-24 ¶ 45; Dkt. 370-1 SUF ¶ 28. Defendants flatly assert that "in reality Klutch had not obtained virality." Dkt. 370-1 SUF ¶ 26.

[9] Although the court in *Loop AI Labs* was interpreting Cal. Civ. Proc. Code 2019.210, part of CUTSA, Cal. Civ. Code § 3426 *et seq*., as discussed *supra* note 5, the conceptual analysis is similar.

successful." Dkt. 387 at 3 (emphasis added). As discussed more thoroughly below, Plaintiff consistently relies on broad, catchall phrases to define its trade secrets. "The Ninth Circuit has rejected the use of 'catchall' language, holding that such language is insufficiently specific 'because it does not clearly refer to tangible trade secret material.'" *Loop AI Labs,* 195 F. Supp. 3d at 1115 (quoting *Imax*, 152 F.3d at 1167).

Defendants use the shorthand of "Virality API" to encompass how this concept would be reflected in programming terms, but argue that there is no evidence to support the existence of such an API.[10] Dkt. 350 at 14. Plaintiff acknowledges that no such API exists, but contends that in defining "Virality Capabilities," "Myers explained that his focus was on a 'broader area' than the virality API and involved, among other things, know-how, techniques, and historical results data for measurement/testing/validating/reporting user engagement and virality for social oriented software applications." Dkt. 370-1 SUF ¶ 76 (quoting Myers Decl., Dkt. 387-4 ¶ 52).

Even accepting Myers' characterization, Plaintiff fails to show *which* techniques or know-how constitute the "Virality Capabilities" trade secret. In his supplemental declaration, Myers asserts "one of the key subjects/areas of the Calendar Research trade secrets is the Klutch viral and planning capabilities and knowledge (i.e. learnings), including Calendar Research's proprietary API and many other elements." Myers Decl., Dkt. 387-4 ¶ 57. Myers also provides what he claims are exemplars of the "Virality Capabilities" Defendants have failed to consider, including "various combinations of the following elements listed in [Myers'] report":

> b. Metric definition for user engagement and virality;
> c. Identification and implementation of data tracking to support all metrics;
> d. Transactional schema definition for metrics and underlying tracking data;
> e. Methods/techniques/know-how for integrating monitored apps (e.g., Klutch) with usage and virality tracking and measurement;
> f. Definition of usage/virality transforms for analytics;
> g. Realtime and/or batch tracking and monitoring processes for usage and virality;

[10] As described in the previous Summary Judgment Order, an "API" is an "Application Programming Interface . . . a set of available commands, sent over the internet that permits access to a third-party database of information." Plaintiff contests Defendants' use of this term as misleading, as Myers merely adopted Defendants' term "virality API" when discussing his larger concept. Dkt. 387-4 ¶¶ 49–50. The distinction is without significance. Even using Plaintiff's definition of "Virality Capabilities," the Court is still unable to determine the specific definition of the alleged trade secret.

h. Methods/techniques/know-how for measuring, testing, and validating usage and virality;
i. Methods/techniques/know-how for testing usage and virality due to various proposed functional/UX changes;
j. Documentation presenting measurement, testing, validation information;
k. Server-side, non-public API definition and implementation for measurement, testing, and validation information;
l. Historical results for measurement, testing, validating, reporting based upon Klutch app (including positive, negative, and inconclusive results);
m. Hardware/software/cloud specifications and configurations for usage and virality management;
n. Performance and scalability methods/techniques/know-how for usage and virality management;

Id. ¶ 52 (b)–(n). Although Plaintiff presents a voluminous list of technical terms, Plaintiff fails to articulate any of these concepts with enough specificity to distinguish them from the "special knowledge of those who are skilled in the trade." *Loops AI Labs*, 195 F. Supp. 3d at 1116. "The vast majority of Plaintiff's disclosures consist of paragraphs in which Plaintiff simply lists categories of alleged trade secrets in broad terms." *Id.* at 1113.

Plaintiff's opposition cites mostly to Myers' supplemental declaration, which in turn points back to Myers' expert report. But, upon close inspection of the expert report, Myers only offers more lists of broad technical concepts—creating a circuitous path of unexplained jargon. In his expert report, Myers identifies the following as potential trade secrets:

A. Compilation of source materials for building, maintaining, and evolving a software system for social/collaborative event management *including various combinations of the following . . .*
B. Compilation of [available] product and project related information for a social/collaborative event management software system *including without limitation various combinations of the following . . .*
C. Compilation of methods, techniques, know-how, and historical results data for measurement/testing/validating/reporting user engagement and virality for social oriented software applications i*ncluding various combinations of the following . . .*

Initials of Preparer : PMC

Myers Expert Report, Dkt. 301-22 ¶ 30 at (A)–(C) (emphasis added). Myers consistently uses vague and over-inclusive phrases to encompass as much information as possible. This is the exact type of "catchall" language rejected by the Ninth Circuit. *See Imax*, 152 F.3d at 1167. In *Imax*, the plaintiff claimed that "every dimension and tolerance that defines or reflects [the] design" of Imax's rolling-loop projector constituted a trade secret. *Id.* The Ninth Circuit rejected Imax's definition, because if failed to "achieve[] the level of specificity necessary to identify the numerical dimensions and tolerances as trade secrets." *Id.*

Similarly, in *Loop AI Labs*, a startup artificial intelligence company alleged a competitor had misappropriated its trade secrets by conspiring with plaintiff's former CEO. *Loop AI Labs*, 195 F. Supp at 1107. The court dismissed the claims, however, because plaintiff failed to provide a reasonably particular definition of its trade secrets. *Id.* (applying *Imax*). Much like the plaintiff in *Loop AI Labs*, here the "Plaintiff identifies categories of information," but fails to specifically identify which information within the categories constitutes a trade secret. *Id.* at 1116. Plaintiff's disclosures are so vague "it reads like an inventory of categories of Plaintiff's scientific or strategic business information." *Id.* at 1112. Therefore, "Plaintiff's technique of listing general concepts or categories of information is plainly insufficient; Defendants cannot fairly be expected to rebut Plaintiff's trade secrets claim without a reasonably concrete definition of the purported secrets." *Id.* at 1114–15.

Closely examining the expert report, Myers lists such information as "Product planning information," "Competitive analysis information," "Software requirements and specifications," "Performance specifications," and many others as potential trade secrets, but Myers fails define where this information existed at Calaborate. Dkt 301-22 ¶ 30. Such "broad, categorical terms" are insufficient for the Court to discern the alleged trade secret. *AlterG, Inc. v. Boost Treadmills LLC*, 388 F. Supp. 3d 1133, 1145 (N.D. Cal. 2019) (dismissing claims because plaintiff's alleged trade secrets were "not tethered to a specific technology"). "It is insufficient to claim that software merely 'contain[s] valuable trade secrets' without specifically identifying those secrets, or that a system's characteristics generally are trade secrets without clearly referring to the precise characteristics . . . ." *Modus LLC v. Encore Legal Sols., Inc.*, No. 12-CV-00699-PHX-JAT, 2013 WL 6628125, at *6 (D. Ariz. Dec. 17, 2013) (internal citations and quotation marks omitted). "Indeed, [Plaintiff] has set out its purported trade secrets in broad, categorical terms, more descriptive of the types of information that generally may qualify as protectable trade secrets than as any kind of listing of particular trade secrets [Defendants have] a basis to believe actually were misappropriated here." *Vendavo, Inc. v. Price f(x) AG*, No. 17-CV-

06930-RS, 2018 WL 1456697, at *4 (N.D. Cal. Mar. 23, 2018).

To the extent Plaintiff does identify the tools the Klutch team used to track virality, Plaintiff fails to present any evidence to rebut Defendants' direct testimony that they were "popular, publicly available (for free), services" such as "Google Analytics and Crashlytics . . ." Dkt. 350 at 14; Dkt. 301-24 at 32. These are analytical tools that are well-known in the industry, and their usage along cannot constitute a trade secret. *See VBS*, 2018 WL 5274172, at *8 (holding defendants' usage of "conventional lighting techniques used across the industry and in jewelry stores" could not constitute a trade secret because "[t]he lighting technique is not a secret, and the Plaintiffs have failed to show they took any steps to keep it confidential.").[11]

Plaintiff's fails in its burden to define Virality Capabilities as a trade secret. Without a sufficiently defined trade secret, the Court is unable to determine whether that information had "independent economic value, actual or potential, from not being generally known," or if Plaintiff "has taken reasonable measures to keep such information secret . . . ." 18 U.S.C. § 1839(3)(A)–(B). Accordingly, Plaintiff fails in its "obligation of providing a particularized description of an alleged trade secret," which "is a duty owed to the court." *DropzoneMS, LLC v. Cockayne*, No. 16-CV-02348-YY, 2019 WL 7630788, at *2 (D. Or. Sept. 12, 2019).

2. Evidence

Even if Virality Capabilities could constitute a trade secret as Plaintiff has defined them, Plaintiff has not provided any evidence beyond speculation that such a proprietary Virality Capability actually existed at Calaborate. Instead, Plaintiff asks the Court to infer its existence by its absence. It is undisputed that the alleged Virality API was never discovered. Dkt. 370-1 SUF ¶ 76. By Plaintiff's characterization, Myers "found a folder where he expected the virality API to be and that he did not know whether it had been deleted or Defendants had failed to produce it." *Id.* On summary judgment the Plaintiff bears the burden of demonstrating the essential elements of its claim, including the "existence of an element essential to [its] case . . . ." *Hill*, 2007 WL 2326070, at *2 (citing *Celotex Corp.*, 477 U.S. at 323). There is no evidence to support the inference that the Virality Capabilities/API ever existed.

[11] The *VBS* district court was affirmed on its holding regarding the lighting techniques, but reversed on its holding regarding customer lists. *VBS Distribution, Inc. v. Nutrivita Labs., Inc.*, No. 18-56317, 2020 WL 2086557 (9th Cir. Apr. 30, 2020).

As discussed *supra* Part III.a.i.1, Plaintiff contends that the term Virality API is misleading, and Plaintiff's "Virality Capabilities" trade secret is much broader than a single API. Even accepting this broader definition, Plaintiff does not carry its burden in showing such Virality Capabilities exist. Rather, Plaintiff notes "the dearth of information in the Hand-over Materials/Information related to the methods, techniques, and know-how related to the measurement/testing/validating/reporting of user engagement and virality capabilities, including Calaborate's proprietary API for this purpose." Dkt. 301-22 ¶ 37. Myers states: "In my report, one of the primary issues that I address is the dearth or lack of certain types of information handed over by the individual Defendants Gray, Dusseault and Efremidze to Calendar Research as part of the asset transfer as well as part of the production in this lawsuit." Dkt. 387-4 ¶ 67. Myers continues: "As I explain in my report, the types of information that I find lacking in this case, are precisely the types of information that I would typically expect to find as containers for a company's protected trade secret information. Those things described and explained in detail in paragraphs 30-32 of my report." *Id.* ¶ 68.

However, paragraphs 30–32 of the expert report simply produce an extensive list of programming terms and concepts that *could* constitute trade secrets *if* they did exist at Calaborate (and were kept secret)**.** Dkt. 370-22 ¶¶ 30–32. "The critical flaw in this argument is that it fails to recognize that it is Plaintiffs'—not Defendants'—burden to clearly identify their trade secrets." *X6D*, 2012 WL 12952726, at *8. Much like the plaintiff in *XD6*, here "Plaintiff[] merely list hundreds of documents that allegedly 'reflect' their trade secrets," but does not show where those trade secrets exist in the record. *Id.* at *8. "[W]hen the plaintiff effectively buries its trade secrets in documentation, we are not required to sift through those documents and speculate as to what information contained therein is claimed as a trade secret." *Id.* Although Myers identifies broadly where he would expect these categories of trade secrets to be kept, there is no evidence such information was kept in this case.

Plaintiff asks the Court to infer that, because the Individual Defendants marketed themselves as experts in "viral/social" when selling to the Corporate Defendants, the Individual Defendants must have destroyed or withheld the relevant evidence of their proprietary virality system. Dkt. 387 at 3. This is pure speculation and is not enough to create a genuine issue of material fact as to the existence of the alleged "Virality Capabilities." *Loomis v. Cornish*, 836 F.3d 991, 997 (9th Cir. 2016) ("[M]ere allegation and speculation do not create a factual dispute for purposes of summary judgment."). Neither Myers' report nor his subsequent declaration remedy Plaintiff's lack of evidence. Such "conclusory and speculative testimony in affidavits and moving papers is insufficient to raise triable issues of fact and

defeat summary judgment." *VBS*, 2018 WL 5274172, at *2 (citing *Thornhill Pub. Co., Inc. v. GTE Corp.*, 594 F.2d 730, 738 (9th Cir. 1979)). Because Plaintiff lacks any evidence beyond speculation, Individual Defendants' direct testimony that no such Virality API, or any other proprietary virality system, ever existed is undisputed. Dkt. 349-1 ¶ 25.

3. Negative Know-How

Finally, Plaintiff alleges that Defendants misappropriated trade secrets not because of what they did for StubHub, but because of what they did not do. Courts have recognized the viability of "negative know-how" as a trade secret, because it could "confer [Defendants] the benefit of steering clear of fruitless development pathways, thereby saving precious time and resources." *Genentech, Inc. v. JHL Biotech, Inc.*, No. 18- CV -06582 WHA, 2019 WL 1045911, at *19 (N.D. Cal. Mar. 5, 2019). Misappropriation of negative know-how can be especially damaging because "such information would be virtually untraceable, thereby making the task of identifying (and enjoining) . . . [the] trade secrets . . . a bone-crushing endeavor." *Id.* at *20. A clear case of negative know-how involves pharmaceutical manufacturing, where avoiding previously failed formulas avoids the expense of costly research and trials. *See id.* at *3 (defendant's alleged theft of valuable research and design techniques allowed to them to expedite the regulatory approval process for biosimilar drugs). Even in the similar field of medical device manufacturing, plaintiffs struggle to define negative know-how trade secrets when their designs are conceptual rather than technical. *See AlterG, Inc. v. Boost Treadmills LLC*, 388 F. Supp. 3d 1133, 1145 (N.D. Cal. 2019) (medical device manufacturer failed to sustain claims for misappropriation of its "positive and negative learnings of low cost mechanical unweighted systems, air pressure systems, and Differential Air Pressure systems" because they were too broadly defined).

In the software context, claims for negative know-how misappropriation require specific examples of the failed code or product that defendants misappropriated. *See Pixon Imaging, Inc. v. Empower Techs. Corp.*, No. 11-CV-1093-JM MDD, 2011 WL 3739529, at *4 (S.D. Cal. Aug. 24, 2011) (Defendants allegedly used plaintiff's "[a]lgorithms and the research underlying it as a basis for developing a different product."); *Cinebase Software, Inc. v. Media Guar. Tr., Inc.*, No. C98-1100 FMS, 1998 WL 661465, at *1 (N.D. Cal. Sept. 22, 1998) (internal quotation marks omitted) (acknowledging "[n]egative research can be protectable as a trade secret," but finding "Plaintiff's designation of the defendant software engineers' technical know-how regarding what does and does not work in the process of designing digital media management software is simply too nebulous a category of information to qualify for trade secret protection").

Initials of Preparer PMC

Here, Plaintiff is essentially seeking a determination that the Individual Defendants' knowledge of how *not* to go viral is a trade secret. The negative know-how Plaintiff seeks to protect is an inverse repetition of the broad "Virality Capabilities" the Court has already determined are too general to constitute a trade secret. As discussed above, this type of knowledge is impossible to parse from the "matters of general knowledge in the trade or of special persons who are skilled in the trade . . . ." *Founder Starcoin*, 2018 WL 3343790, at *6 (internal quotation marks omitted). Unlike the drug cases or software cases mentioned above, there is no evidence of a failed virality model in this record. At this point in the litigation, this evidentiary failure can only be imputed to Plaintiff. "In attempting to establish the existence of this factual dispute, the opposing party may not rely upon the denials of its pleadings, but is required to tender evidence of specific facts in the form of affidavits or admissible discovery material in support of its contention that the dispute exists." *Hill*, 2007 WL 2326070, at *2.

ii. UI/UX

Plaintiff also claims that Klutch's "User Interface / User Experience ("UI/UX") and Design" constitute a trade secret. Dkt. 370 at 3. In the previous Order granting partial summary judgment, this Court explained that, "as a matter of law, outward-facing features that every user of an app can see and experience are not trade secrets." Dkt. 160 at 6 (citing *Agency Solutions.Com, LLC v. TriZetto Grp., Inc.*, 819 F. Supp. 2d 1001, 1019 (E.D. Cal. 2011)). It is well established that "[p]ublicly available information, by definition, cannot be protected as a trade secret." *SocialApps, LLC v. Zynga, Inc.*, No. 11-CV-04910 YGR, 2012 WL 381216, at *2 (N.D. Cal. Feb. 6, 2012); *see also Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) ("Information that is public knowledge or that is generally known in an industry cannot be a trade secret."). To the extent Plaintiff refers to Klutch's publicly discernable features as a trade secret, that argument is entirely foreclosed. Instead, Plaintiff appears to be referring to the "patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes" that Defendants used to create the Klutch UI/UX. 18 U.S.C. § 1839(3).

1. Definition

Incorporating the analysis above, Plaintiff fails to define its UI/UX techniques with enough specificity to constitute a trade secret. Plaintiff cites to broad swaths of both Myers' expert report and his declaration but fails to define the UI/UX trade secret beyond generalities. The total substance in Myers' expert testimony regarding UI/UX consists of the following phrase: "Methods/techniques/know-how for testing usage and virality due to various proposed functional/UX changes . . . ." Myers Decl., Dkt. 387-4

¶ 52(i); Myers Report, Dkt. 301-22 ¶ 30(C)(h). Again, Myers uses broad "catch-all" language to encompass a host of design concepts, but fails to distinguish "[m]ethods/techniques/know-how" from general industry knowledge on the same topic. Myers Decl., Dkt. 387-4 ¶ 52(i); *see Imax*, 152 F.3d at 1167. Plaintiff has consequently failed to identify any non-public information that could constitute a trade secret.

2. Evidence

Again, even accepting Plaintiff's definition, Plaintiff suffers from a lack of evidence to show that a non-public UI/UX technique ever existed. Aside from Myers' spare discussion on the issue, Plaintiff presents no evidence that the Individual Defendants had a specific (and secret) system for developing Klutch's UI/UX. Plaintiff cites to massive sections of its Statement of Additional Uncontroverted Fact ("SAUF"), but the evidence contained therein only demonstrates that the Individual Defendants had skill and experience in designing accessible user interfaces, not that they had a special technique or process for achieving a viral UI/UX at Calaborate. Dkt. 387 at 9 (citing SAUF ¶¶ 283–336). Referring to Plaintiff's SAUF, Dkt. 370-1, Plaintiff characterizes the evidence as follows:

- "Gray testified that his team was trying to distinguish Klutch from other applications by its interface. The team was trying to reconcil[e] calendaring and scheduling between multiple parties…" and just tried to do it in a different way, visually." *Id.* ¶ 288.
- "Gray testified that one way his team tried to distinguish Klutch through its interface was by integrating scheduling and group chatting with a different look that was unique to Klutch." *Id.* ¶ 289.
- "In February 2015, StubHub prepared an internal presentation on Klutch which included, under Strategic Rationale, the fact that Klutch has…proven viral UX flows." *Id.* ¶ 290.
- "In February 2015, StubHub prepared an internal presentation on Klutch which included a list of Viral learnings (UX), that specified: Understanding the UX models they tried and what specific flows and UX drove the highly viral results." *Id.* ¶ 292.

Dkt. 370-1 SAUF ¶¶ 288–292 (internal quotation marks omitted). Even accepting Plaintiff's characterization, this evidence only points to public-facing information that cannot be protected as a

Initials of Preparer : PMC

trade secret. Elements like "flows and UX," or a "different look that was unique to Klutch," would be readily discernible by any user of the application, and therefore undeniably public. *See SocialApps,* 2012 WL 381216, at *3.

Plaintiff's additional evidence fares no better. Plaintiff claims that "[a]fter the Individual Defendants joined StubHub, they focused extensively on using the know-how and expertise they had developed while at Calaborate in an effort to apply those proprietary UI/UX techniques to StubHub's products." Dkt. 370-1 SAUF ¶ 299. However, this presupposes that the "UI/UX techniques" are proprietary, which Plaintiff never establishes in the first instance. Finally, Plaintiff asserts that "[i]n a September 21, 2015 email update to Kanazawa regarding TonightOut, Gray explained the 'design principle' of 'instant gratification' as 'super helpful in keeping users engaged.'" *Id.* ¶ 306. The "design principle of instant gratification" is an indefinable concept that is too vague to constitute a trade secret. *See Imax*, 152 F.3d at 1176; *IDX*, 285 F.3d at 583; *Loop AI Labs*, 195 F. Supp. 3d at 1115. Plaintiff has therefore failed to identify any non-public UI/UX information with sufficient specificity to constitute a trade secret.

iii. Venue-Focus and Third-Party App Integration

Plaintiff claims Klutch's "(3) Venue Focus; and (4) Integration of Third- Party Apps" constitute a trade secret. Although listed a separate trade secrets in Plaintiff's opposition, the concepts are so vaguely defined and there is so little evidence regarding either concept in the record that they can be disposed of together.

1. Definition

Plaintiff definitions of "(iii) venue targeting and selection, and (iv) third-party integration technology" suffer from all of the same defects explained above. Dkt. 387 at 13. Plaintiff loosely defines "venue focus" as Defendants' "expertise regarding which types of venues (e.g., restaurants, concerts, sporting events) should be featured on the app to maximize virality." *Id.* at 4. The types of venues Defendants chose to highlight in the Klutch app would have been visible to any user of the application, rendering them publicly available and unprotectable as trade secrets. *SocialApps*, 2012 WL 381216, at *3. Plaintiff provides no definition of how this general information was proprietary, or how it was kept secret. Instead, Dusseault presents unrebutted evidence that "it was widely known and publicized that restaurants, coffee shops, and bars are the most popular types of places to meet." Dusseault Sup. Decl.,

Dkt. 399-4 ¶ 2.b.[12] The broad choice to focus on "restaurants, concerts, sporting events" for a social planning application is both "generally known [and] readily ascertainable," precluding trade secret protection. 18 U.S.C. § 1839(3)(B).[13]

Plaintiff's definition of third-party app integration is equally vague. Plaintiff defines its integration strategy as follows: "After many months of investigation, experimentation, and analyzing relevant data and metrics, the Individual Defendants developed extensive expertise and know-how about how best to approach the question of integration." Dkt. 387 at 4. Referring to Plaintiff's SAUF, Plaintiff claims: "Like Klutch, TonightOut interfaced with Facebook API." Dkt. 370-1 SAUF ¶ 328. However, numerous applications integrate Facebook and other third-party apps to accelerate their growth. The previous Order granting partial summary judgment acknowledged the ubiquity of cross-application integration using publicly available APIs:

> But the APIs that TonightOut and Klutch had in common are available in a large number of mobile apps. These APIs interacted with other popular mobile apps FourSquare, Facebook, and iMessage. Dr. Goldberg confirmed the insignificance of the fact that two apps may both interact with these services because APIs are made available by the companies behind those services for the very purpose of allowing other parties to access their data.

See Dkt. 160 at 14. Plaintiff fails to define any special method or technique for integrating third-party applications, which is indisputably a common practice in the industry. *Id.*

The most concrete definition of a third-party integration technique that Plaintiff provides is the Individual Defendants' decision to use the application Parse to integrate StubHub apps with Facebook, as was done with Klutch. Dkt. 370-1 SAUF ¶ 321. Plaintiff's expert testimony does not mention this specific tool at all, nor does it explain that the Klutch team had a particular method of integrating third-party applications. *See* Dkt. 301-22; Dkt. 387-4. Further, Defendants present uncontroverted evidence

[12] It is also undisputed that the email where "restaurants, coffee shops, and bars" are discussed was sent by Dusseault to a StubHub employee preliminarily exploring the Klutch acquisition in 2014, when Dusseault was still working for Calaborate. Dkt. 399-4 ¶ 2.a.

[13] Similarly, Plaintiff fails to demonstrate how Klutch's decision to display venue hours in local time is not publicly available information.

that Parse is a well-known application integration tool in the industry. Dkt. 399-4 ¶ 6. Plaintiff fails to demonstrate that the mere use of Parse, or any other third-party application, is a protectable technique under the DTSA.

2. Evidence

Plaintiff fails to provide any evidence that a trade secret regarding "venue focus" or "third-party app integration" ever existed at Calaborate. Myers does not mention "venue focus" once in either his expert report or his subsequent declaration. *See* Dkt. 301-22; Dkt. 387-4. Myers' entire testimony regarding third-party app integration consists of the following phrase: "Methods/techniques/know-how for integrating monitored apps (e.g., Klutch) with usage and virality tracking and measurement." Dkt. 387-4 ¶ 52(e). One conclusory phrase, coupled with a complete lack of evidence regarding either "venue focus" or "third-party app integration," does not permit the Court to infer that a proprietary system ever existed for either of these categories. *See Loomis*, 836 F.3d at 997. Accordingly, Plaintiff has failed to even raise the specter of a trade secret regarding venue focus or third-party app integration.

iv. Failure to Return Intellectual Property

Finally, Plaintiff claims that the Individual Defendants failed to return the physical and intellectual property of Calaborate. Dkt. 387 at 7. Plaintiff alleges the Individual Defendants "either (i) kept or wiped computers and other devices belonging to Calaborate; (ii) deleted or delayed in returning software keys required to update the Klutch application; and (iii) withheld Calaborate documents and information located on third-party online storage platforms, including DropBox, Evernote, GitHub, and Google Documents . . . ." Dkt. 387 at 7 (internal citations omitted). It is not clear from Plaintiff's opposition if these actions are meant to constitute violations under the DTSA, the CFAA, or both.[14] Because Plaintiff has failed to define any trade secret with specificity, Defendants cannot be liable under the DTSA—Defendants cannot misappropriate trade secrets that do not exist. However, even if the Court were to accept Plaintiff's vague definitions as trade secrets, Plaintiff also fails to specify which items of allegedly withheld physical or intellectual property are correlated to which alleged trade secrets. Generally, Plaintiff argues that Individual Defendant's failure to return property constitutes the "misappropriation" element of the DTSA. Dkt. 387 at 15. However, under the DTSA, it is Plaintiff's burden to show both that the allegedly withheld information was misappropriated by Defendants *and*

[14] In the interest of efficiency, the Court considers the alleged actions as to both Plaintiff's DTSA and CFAA claims, but this confused argument further muddles Plaintiff's claims. To the extent Plaintiff argues that Defendants' access of the computers was unlawful, those claims are considered under the CFAA, *infra* Part III.b.

that it is a trade secret. *VBS*, 2018 WL 5274172, at *7 (citing Cal. Civ. Code § 3246.1(b); 18 U.S.C. § 1839(5)). As explained below, Plaintiff fails to raise any genuine issue of fact that Individual Defendants misappropriated any trade secrets.

1. Private Keys

Plaintiff alleges that Individual Defendants withheld the Android versions of Klutch's "Private Key," a unique digital code required to access the developer's tools in the Google Playstore. Dkt. 387 at 24.[15] Plaintiff presents no evidence that the Private Key constitutes a trade secret on its own. Instead, Plaintiff claims Defendants "wrongfully acquired" Plaintiff's trade secrets by delaying transfer of the Private Key, which prevented Plaintiff from exploiting the Klutch app on the Google store. Dkt. 387 at 15. Again, Plaintiff presupposes an underlying trade secret without sufficiently defining it. Because Plaintiff fails to establish that the Private Key was a trade secret, without showing that the Private Key contained or allowed access to a definable trade secret, Plaintiff's claim is without merit.[16] As such, the Court finds that there is no genuine issue of material fact as to the Private Key.

2. Source Code

Plaintiff alleges Dusseault misappropriated trade secrets by retaining some of Klutch's source code on her personal laptop. Dkt. 387 at 4. There is no dispute that Dusseault retained some of Klutch's source code on her laptop, which she took to work at StubHub. There is also no dispute that the code was first obtained during the legitimate course of Dusseault's work for Calaborate, which would not constitute "improper means" of acquisition standing alone. *See VBS*, 2018 WL 5274172, at *8 (acknowledging that "[n]o evidence was presented that [Defendant] improperly took the information home with her when she left [Plaintiff] to misappropriate it.").

Dusseault claims none of the code retained on her laptop was a trade secret because it "was either automatically generated or available verbatim in public tutorials." Dkt. 399 at 9. Dusseault argues

[15] Myers explains the "private key" as follows: "Developers of Android apps to be offered in the Google Play store create one or more 'app signing keys' that are unique to that developer. Developers must use an app signing key to 'sign' every application package they submit to the Google Play store. Once an application has been signed with a specific app signing key, all future updates to that app must also be signed using that same key. In short, the Google Play store uses a matching public key to confirm that the update package received from the develop[er] is authentic and belongs to that particular developer." Myers Expert Report, Dkt. 301-22 ¶ 39.B.a.

[16] To the extent Plaintiff argues Defendants withheld the Private Key in violation of the CFAA, that is discussed *infra* Part III.b.iii

that, considering the Court's previous Order granting summary judgment on Plaintiff's code-based claims, any code that remained on the laptop is not a trade secret. Dkt. 399 at 9. This Court's previous grant of summary judgment foreclosed Plaintiff's claim that any of the source code analyzed in the previous Order constituted a trade secret. *See* Dkt. 160. The Court left open the possibility, however, that additional code may constitute a trade secret if properly defined. *Id.* In leaving that possibility open, Court specifically "caution[ed] Plaintiff that it must satisfy its evidentiary burden to show that the Klutch code is a protectable trade secret." *Id.* The Court held:

> Plaintiff is not permitted to reassert that the lines of code identified as publicly available could constitute a trade secret on their own. If Plaintiff seeks to establish the Klutch code as a protectable trade secret based on a compilation of publicly-available information, as the Court noted in its summary judgment order, Plaintiff must put forward evidence more than "mere speculation" regarding what aspects of the compiled code are sufficiently novel to be a trade secret.

Id. Plaintiff has failed in this burden. In its opposition, Plaintiff has presented no evidence or argument that the code found on Dusseault's computer is different from the code the Court previously compared. *See* Dkt. 160 at 6. Plaintiff only contends that "Dusseault stored a copy of the Klutch code on her personal laptop and still today has that same laptop in her possession—meaning that she had access to the code during the entire time she work[ed] at StubHub." Dkt. 387 at 10. But Plaintiff does not explain with any specificity how the code on Dusseault's laptop is a trade secret. Although Plaintiff has identified *some* of the code from Dusseault's computer it believes is relevant, Plaintiff has not shown this code is a non-public, economically valuable trade secret. The Court cannot assume this code constitutes a trade secret, especially in light of the previous Order. Dkt. 160 at 6. As such, Plaintiff has failed in its burden to establish the code found on Dusseault's computer constitutes a trade secret.

3. Cloud Storage

Plaintiff also claims, "Individual Defendants wrongfully acquired Plaintiff's trade secrets by backing up their Calaborate accounts, including email and cloud-based storage repositories, before departing from Calaborate, and then accessing and downloading that proprietary information after starting work at StubHub." Dkt. 387 at 16. Plaintiff then broadly cites to Section V of its SAUF, Dkt. 370-1, as support for this assertion. Of the one-hundred-and-eleven alleged facts comprising Section V (roughly seventeen pages of text), Plaintiff provides no fact beyond mere conclusions to demonstrate the

cloud accounts contained trade secrets.[17] *See* Dkt. 370-1 SAUF ¶¶ 337–448. Again, assuming Individual Defendants did retain access to their cloud accounts, Plaintiff still had the burden to demonstrate that the information contained therein constituted a definable trade secret. Plaintiff fails to identify with any specificity which information allegedly contained in the cloud accounts constitutes a trade secret.

v. Conclusion

It is undisputed that the Individual Defendants used some of the knowledge, learnings, and know-how they developed at Calaborate while working for StubHub. It is further undisputed that Individual Defendants worked on similar projects at StubHub and Calaborate, but that does not mean that Individual Defendants necessarily misappropriated trade secrets in the process. Much like copyright law, under the DTSA, there is no "inverse ratio" rule, wherein a greater showing of access requires a lesser showing of misappropriation. *See Skidmore as Tr. for Randy Craig Wolfe Tr. v. Zeppelin*, 952 F.3d 1051, 1067 (9th Cir. 2020) (rejecting the "inverse ratio" approach between access and misappropriation in copyright law). The question for this Court was whether Defendants misappropriated a specific, definable trade secret, not whether they implemented a similar app idea for a competitor. *See Loop AI Labs*, 195 F. Supp. 3d at 1111 (N.D. Cal. 2016) (citing *Silvaco Data Sys. v. Intel Corp.*, 109 Cal. Rptr. 3d 27, 37 (2010) ("trade secret law protects the right to maintain the confidentiality of facts, not ideas").

Ultimately, Plaintiff fails to define any trade secret with enough specificity to distinguish it from "matters of general knowledge in the trade or of special persons who are skilled in the trade . . . ." *Founders Starcoin*, 2018 WL 3343790, at *6 (internal quotation marks omitted). Plaintiff also fails to show that the alleged trade secrets actually existed at Calaborate. Although Plaintiff has presented some evidence that Individual Defendants retained Calaborate's physical and intellectual property post-employment, Plaintiff has failed to show that any of the allegedly retained material contained trade secrets. Left with nothing but speculation, the Court is unable to discern a genuine issue of material fact as to Plaintiff's DTSA claims**.** "Simply put, Plaintiffs' opposition is one complete failure of proof. It is nothing more than conclusory and unsupported allegations of wrongdoing on Defendants' part. That is not enough to raise a genuine issue of material fact." *VBS*, 2018 WL 5274172, at *7. Because Plaintiff

[17] The task of sorting through these facts to see if any supported the specific claim at issue should have been undertaken by Plaintiff. *See IDX*, 285 F.3d at 583. ("[U]nless the plaintiff engages in a serious effort to pin down the secrets a court cannot do its job.").

Initials of Preparer : PMC

failed to identify any trade secret misappropriation, summary judgment on Plaintiff's DTSA claims is appropriate as to all Defendants.

b. Computer Fraud and Abuse Act Claims

Plaintiff also brings claims against all Defendants under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030 (a)(2)(C), (a)(4), (a)(5)(B)–(C), and for conspiracy to violate of all of the above under § 1030(b). Dkt. 387 at 19–20. Because an underlying wrongful act is required for both vicarious liability and civil conspiracy (which also requires agreement), the Court first determines the liability for the Individual Defendants under the CFAA. *Ajetunmobi v. Clarion Mortg. Capital, Inc.*, 595 F. App'x 680, 683 (9th Cir. 2014) (quoting *Applied Equipment Corp. v. Litton Saudi Arabia Ltd.*, 869 P.2d 454, 457 (Cal. 1994)) ("A civil conspiracy, however atrocious, does not give rise to a cause of action unless a civil wrong has been committed resulting in damage."); *see also Mintz v. Mark Bartelstein & Assocs. Inc.*, 906 F. Supp. 2d 1017, 1042 (C.D. Cal. 2012) (adopting the same language in a CFAA case).

Violations of the CFAA can lead to criminal penalties, but the CFAA also provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." *Id.* § 1030(g). Although "§ 1030 is primarily a criminal statute," the operative liability provisions under § 1030(a) have been interpreted the same in both the criminal and civil context. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) ("*Brekka*") ("§§ 1030(a)(2) and (4) create criminal liability for violators of the statute . . . our interpretation of §§ 1030(a)(2) and (4) is equally applicable in the criminal context" and in civil cases).

Plaintiff brings claims under § 1030(a)(2), § 1030(a)(4) and § 1030(a)(5)(B)–(C), and each provision has different substantive requirements. *See Brekka*, 581 F.3d at 1131 ("The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data."). For example, under § 1030(a)(4), a defendant must access a protected computer without (or exceeding) authorization with an "intent to defraud," and thereby obtain "anything of value" in the course of that fraud; whereas § 1030(a)(2)(C) only requires that a defendant obtain "information from any protected computer" via unauthorized access (or access exceeding authorization). In *Brekka*, the Ninth Circuit explained the requirements of §§ 1030(a)(2) and (a)(4) as follows :

> [T]o bring an action successfully under 18 U.S.C. § 1030(g) based on a violation of 18 U.S.C. § 1030(a)(2), [Plaintiff] must show that [Defendant]: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value. To bring an action successfully under § 1030(g) based on a violation of § 1030(a)(4), [Plaintiff] must show that [Defendant]: (1) accessed a "protected computer," (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) "further[ed] the intended fraud and obtain[ed] anything of value," causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

Id. (quoting 18 USC § 1030(a)(2), (4)). Under § 1030(a)(5)(B), Plaintiff is required to show the Defendants "intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, recklessly cause[d] damage . . . ." Under § 1030(a)(5)(C), the Plaintiff must show both "damage and loss." Although each provision has different substantive requirements, there are two threshold requirements for civil liability under any provision of § 1030(a): a defendant must 1) access a protected computer without authorization or exceeding authorization, and 2) the unlawful access must cause some form of either damage or loss. *See Brekka*, 581 F.3d at 1131 ("Thus, a private plaintiff must prove that the defendant violated one of the provisions of § 1030(a)(1)-(7), and that the violation involved one of the factors listed in § 1030(a)(5)(B)." Without a showing of unlawful access, the Court need not reach the other factors. *Id.*; *see also Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986) ("a complete failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial.").

Plaintiff alleges substantive liability under four provisions of the CFAA: §§ 1030 (a)(2)(C), (a)(4), (a)(5)(B), and (a)(5)(C). In its opposition, however, Plaintiff fails to specify which Individual Defendant committed which allegedly wrongful act, and Plaintiff does not correspond specific actions to the alleged provisions of the CFAA. *See Ewiz Express Corp. v. Ma Labs., Inc.*, No. 15-CV-01213-LHK, 2015 WL 5680904, at *7 (N.D. Cal. Sept. 28, 2015) (citing *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097 (9th Cir. 2003)) ("Plaintiff's allegations do not sufficiently describe 'the who, what, when, where, and how' of Defendants' alleged unauthorized access."). Local Rule 7.14.3 "imposes 'an affirmative

Initials of Preparer : PMC

burden to list genuine issues with appropriate record citations in order to withstand the motion for summary judgment.'" *Walker v. Boeing Corp.*, 218 F. Supp. 2d 1177, 1182–83 (C.D. Cal. 2002) (quoting *Nilsson, Robbins, Dalgarn, Berliner, Carson & Wurst v. Louisiana Hydrolec*, 854 F.2d 1538, 1545 (9th Cir.1988)). Plaintiff's method of citing broad swaths of its SAUF to support general legal propositions, without argument about how the specific evidence meets the law, is arguably insufficient to meet this burden. It forces the Court to do Plaintiff's work for them. *See Carmen*, 237 F.3d at 1031 ("The cases often refer to the unfairness to the district court, which is substantial, but hardly the full story. If a district court must examine reams or file cabinets full of paper looking for genuine issues of fact, as though the judge were the adverse party's lawyer, an enormous amount of time is taken away from other litigants."). Despite this failure, the Court analyzes each alleged wrongful act under all of the provisions applicable to the alleged action.[18]

i. Access Without or Exceeding Authorization

A threshold requirement for CFAA liability under any provision of § 1030(a) is that Defendants "accessed" a "protected computer" "without authorization" or "exceeding authorization." CFAA § 1030(a). In relevant part, CFAA defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication . . . ." *Id.* § 1030(e)(2)(B). There is no dispute that Calaborate's computers are protected under the statute.[19] The Ninth Circuit has provided four recent opinions defining and distinguishing the phrases "without authorization" and "exceeds authorized access" in the context of CFAA: *Brekka*, 581 F.3d 1127 (9th Cir. 2009), *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) ("*Nosal I*"), *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*"), and *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016) ("*Facebook*").[20]

[18] Any argument not clearly presented in Plaintiff's summary judgment opposition is considered insufficiently raised to allow this Court to provide a ruling. *See Mossimo Holdings, LLC v. Haralambus*, No. CV 14-05912, 2017 WL 1240739, at *7 (C.D. Cal. Apr. 4, 2017) ("The failure to address the remaining claims is grounds for deeming the issues conceded and granting . . . summary judgment on them.").

[19] Plaintiff also argues, in a footnote, that "third-party websites, such as Dropbox, Evernote and Google, are also considered protected computers under the CFAA." Dkt. 387 at 19 n.9. Certainly, a third-party computer may be protected in some circumstances, but whether those accounts belonged to Plaintiff is a fact-specific inquiry—discussed in context, *infra* Part III.b.i.1.

[20] The meaning of "exceeds authorization" in the criminal context was recently granted cert. by the Supreme Court in *United States v. Van Buren*, 940 F.3d 1102 (11th Cir. 2019), *cert. granted*, (U.S. Apr. 20, 2020) (No. 19-783). That case involved a criminal prosecution where a police officer allegedly violated the CFAA by improperly accessing a government computer system for a criminal purpose. It is not clear if the Supreme Court's decision in *Van Buren* will have any impact on this

In *Brekka*, the Ninth Circuit held "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it." 581 F.3d at 1131. If the defendant is authorized access the protected computers, accessing the computers for an improper purpose does violate the CFAA. *Id.* at 1137. A defendant does not lose "authorization" by breaking the company's terms of service, or even by acting against the company's interests. *See id.* (defendant's use of plaintiff's "computers to email documents to his own personal computer did not violate § 1030(a)(2) or § 1030(a)(4) because [defendant] was authorized to access the [plaintiff's] computers during his employment"). There is "[n]o language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest." *Id.*

This interpretation was affirmed in 2016 by *Nosal II*, where the Ninth Circuit held: "we conclude that 'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission." 844 F.3d at 1028–29. If a defendant was given permission to use the computer, "without authorization" does not encompass use of that computer in violation of an agreement; for a defendant's access of a protected computer to be "without authorization," the plaintiff must have first revoked the defendant's access entirely, not merely limited or conditioned it to a limited purpose. *See id.* ("Further, we have held that authorization is not pegged to website terms and conditions."). So, "when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations." *Brekka*, 581 F.3d at 1133. Contrarily, "a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question." *Id.* Once access has been revoked in its entirety, defendants are not permitted to re-access the system by other means—including password sharing or other "back doors." *See Nosal II*, 844 F.3d at 1028 ("once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party.").

Similarly, a defendant may "exceed authorized access" if they are "authorized to use a computer for certain purposes but go[] beyond those limitations . . . .'" *Brekka*, 581 F.3d at 1133 (quoting § 1030(e)(6)). The Ninth Circuit has held that "exceeds authorized access" should be read narrowly, and

---

decision. In the four recent cases mentioned above, the Ninth Circuit has provided clear, consistent, and binding precedent regarding the meaning of "without authorization or exceeds authorized access" under CFAA § 1030(a). The Court accordingly applies the binding precedent from this Circuit.

"the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." *Nosal I*, 676 F.3d at 863. In *Nosal I*, the Ninth Circuit applied the rule of lenity to determine that "exceeds authorized access" means "someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as 'hacking.'" *Id.* at 856–57. In choosing this interpretation, the court rejected the government's proposed interpretation, which would create liability for a defendant who "has unrestricted physical access to a computer, but is limited in the use to which he can put the information." *Id.* The court determined that "[t]he government's construction of the statute would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer." If a defendant has "permission to access the company database and obtain the information contained within," then the misuse of that information does not create CFAA liability, even if it violates a terms of use or employment contract. *Id.* at 864. An employee does not exceed authorized access by taking an action they are otherwise authorized to take for an improper purpose. *Id.* at 861. This interpretation places the focus on whether the employee was authorized to access the files in the first instance—not whether the employee had an improper purpose in so accessing. *See id.* at 859.

Essentially, there are "two general rules in analyzing authorization under the CFAA. First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability." *Facebook*, 844 F.3d at 1067. "Second, a violation of the terms of use of a website—without more—cannot establish liability under the CFAA." *Id*. In neither case does the purpose of the accessor determine the level of authorization, and a company's terms of service cannot be used to make an otherwise-authorized access unlawful. *Id.* Further, if an employee is authorized to access confidential information, later misappropriation does create CFAA liability. "These courts recognize that the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *Nosal I*, 676 F.3d at 863 (quoting *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D. Ariz. Feb. 20, 2008)).

There are many cases, in this Circuit and beyond, that present factually analogous scenarios to the present case—former employees allegedly accessed their employer's confidential information while employed, and later misappropriated it for their own benefit. In every case, even allegedly tortious or criminal misuses of confidential information do not imply CFAA liability if the employees accessed the information while they were still authorized. *See Nosal I,* 676 F.3d at 854 (finding no CFAA liability

Initials of Preparer PMC

when "employees used their log-in credentials to download source lists, names and contact information from a confidential database on the company's computer, and then transferred that information to [defendant]."); *1-800 Remodel, Inc. v. Bodor*, No. CV 18-472-DMG, 2018 WL 6340759, at *7 (C.D. Cal. Oct. 17, 2018) ("Plaintiff does not allege facts showing that Defendant was not authorized to access the particular information that she had forwarded to herself, thereby exceeding her authorized access."); *Shamrock Foods*, 535 F. Supp. 2d at 962 (dismissing CFAA claims when employee emailed himself confidential information while employed, then used that information while subsequently working for a competitor); *Hunn v. Dan Wilson Homes, Inc.*, 789 F.3d 573 (5th Cir. 2015) (architect did not violate the CFAA by using his employer's files, which he transferred to his home computer while employed, to compete with his former employer); *Central Bank & Trust v. Smith*, 215 F. Supp. 3d 1226 (D. Wyo. 2016) (employees did not violate the CFAA by transferring electronic information they were authorized to access from their employer's computer system to a competing bank); *Lewis-Burke Associates, LLC v. Widder*, 725 F. Supp. 2d 187 (D.D.C. 2010) (finding no CFAA liability when the employee took confidential and proprietary information with him when he left and used it to solicit clients for a competing business); *Orbit One. Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010) (Finding no CFAA liability when employees used their authorization to obtain confidential employer information, but later misappropriated the information).

Applying the analysis above, a large portion of Plaintiff's argument is without merit. Plaintiff claims that Individual Defendants stored Calaborate's intellectual property on their personal devices and cloud accounts while employed at Calaborate, but failed to delete or return the information upon termination in violation of their employment agreements. Plaintiff claims Individual Defendants continued to use those devices and accounts, and that "[a]ny attempt to access or actual accessing of [Individual Defendants'] computers in violation of those agreements would constitute unauthorized access under the CFAA." Dkt. 387 at 21. As explained above, such expansive "use restriction" liability has been roundly rejected by the Ninth Circuit. *Facebook*, 844 F.3d at 1066–67 ("Accordingly, the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions.") (internal quotation marks omitted). Plaintiff presents no evidence that any Individual Defendant was not entitled to access or backup confidential information while employed at Calaborate. To the contrary, Defendants were required to continuously access and backup their work as a regular function of their job. *See Brekka*, 581 F.3d at 1133 ("In this case, there is no dispute that [defendant] had permission to access the computer; indeed, his job required him to use the computer."). So, to the extent Plaintiff argues that Individual Defendants violated the CFAA by breaching the terms of their agreements with

:

Initials of Preparer PMC

Calaborate, those claims are foreclosed.[21]

Further, Plaintiff argues that "[a]fter their employment ended, [Individual Defendants] maintained access to Calaborate technical documents in their Dropbox and Evernote accounts, and accessed those documents long after they departed." Dkt. 387 at 21. The CFAA protects computers from unauthorized access; it does not protect information after it has already left the protected computer. *See Nosal I*, 676 F.3d at 857; *Shamrock Foods*, 535 F. Supp. 2d at 967. Even if Individual Defendants misappropriated information from Calaborate's computers to their own accounts while employed, they do not violate CFAA by later using (or misusing) that information. Such a broad "interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute," which the Ninth Circuit has been unwilling to do. *Nosal I*, 676 F.3d at 857. Further, Plaintiff does not provide any evidence that the Dropbox and Evernote accounts ever belonged to Calaborate. To the contrary, Plaintiff's own motion acknowledges these accounts belonged to the Individual Defendants. Dkt 387 at 21 ("they also maintained access to Calaborate technical documents *in their* Dropbox and Evernote accounts") (emphasis added); *see also* Dkt. 370-1 SAUF ¶ 413 ("*Gray's* Evernote account included a note titled "Things we Learned from Atlas and Klutch.'") (emphasis added).[22] Without any evidence that these accounts and devices belonged to Calaborate, Individual Defendants cannot be held liable under the CFAA for accessing their own property.[23] Even if Individual Defendants moved information into their cloud storage account while employed at Calaborate, that does not mean those cloud storage accounts belonged to Plaintiff. "[T]he CFAA is 'an anti-hacking statute,' not 'an expansive

[21] The Court makes no decision on whether Individual Defendants breached the terms of their agreements with Plaintiff. The state law breach of contract claims have been stayed pending resolution of the federal claims.

[22] Plaintiff's trade secret argument relies on the contention that Defendants moved Calaborate's trade secrets from their work computers into Individual Defendants' personal cloud storage accounts before leaving Calaborate. Contrarily, Plaintiff later contends that these cloud storage accounts belong to Plaintiff, and Individual Defendants violated the CFAA by accessing these same accounts after leaving Calaborate. These theories are in conflict—the cloud accounts cannot belong to Defendants for DTSA liability while simultaneously belonging to Plaintiff for CFAA liability.

[23] Although Plaintiff later argues that "Defendants maintained and still to this day maintain unauthorized control over *Plaintiff's* accounts, including email, Evernote, and DropBox," that is in direct contradiction to its earlier argument that Defendants acted wrongly in misappropriating data to their personal accounts. Dkt. 387 at 23 (emphasis added). Further, the evidence Plaintiff cites does not support the assertion that Plaintiff owned the accounts in question, only that Gray used his hunter@calaborate.com email address as a login to the third-party accounts he created on his last day of employment. *See* Dkt. 370-1 SAUF ¶¶ 360–368, 372, 396. The same is true of the email account calaborateinc@gmail.com, which Gray allegedly used to transfer files . Plaintiff presents no evidence it owned this account prior to Gray turning it over to Calendar Research on June 15, 2015. Dkt. 355-6 at 4.

misappropriation statute.'" *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir. 2019) (quoting *Nosal I*, 676 F.3d at 857).

Plaintiff also claims, however, that "[a]ll three Individual Defendants archived and accessed their Calaborate email accounts *after they resigned from Calaborate*." Dkt. 387 at 21. If true, this may create liability under the CFAA. *See Brekka,* 581 F.3d at 1136 ("There is no dispute that if [defendant] accessed [plaintiff's] information on the [plaintiff's] website after he left the company . . . [defendant] would have accessed a protected computer 'without authorization' for purposes of the CFAA"). The Individual Defendants allegedly took different actions in accessing their Calaborate accounts after leaving the company, and each action requires an individualized examination, provided below.

1. Hunter Gray

There is no dispute that "Michael Hunter Gray was a founder of Calaborate and served as its Chief Executive Officer" during the relevant time period. Dkt. 370-1 SAUF ¶ 9. The CFAA requires *unauthorized* access, and, as a threshold matter, Plaintiff has provided no evidence to show that (as Founder and CEO) Gray did not have plenary authority to access and grant access to Calaborate's computers and files while employed. Plaintiff has presented no evidence that Gray was restricted in the actions he could take (or authorize others to take) while acting as CEO of Calaborate.[24] Gray was not authorized, however, to access Calaborate's computers after resigning.

It is undisputed that Gray's last day of employment was April 15, 2015. *Id.* ¶ 214. Plaintiff alleges that, on his last day of work, Gray backed up his entire work email account, hunter@calaborate.com ("Calaborate Email"), to a personal account on a third-party service called Backupify. *Id.* ¶ 352; Dkt. 387 at 21.[25] Gray had to log directly into his Calaborate Email to give Backupify permission to access his Calaborate Email. However, Plaintiff's evidence shows that Gray logged into his Calaborate Email on April 15, 2020, his last day of employment, when he was still authorized to access that account. *See* Dkt. 370-1 SAUF ¶ 364; Dkt. 387, Attachments 37–40, Exh. 208-A–D. As described by Plaintiff's expert, Timothy Anderson ("Anderson"): "Google Apps keeps a token

[24] As explained *supra* Part III.b.i, to the extent Plaintiff argues Gray breached his employment contract to Calaborate by taking or authorizing actions adverse to Calaborate, that does not speak to his "authorization" under the CFAA.

[25] Plaintiff does not present any evidence that the Backupify account belonged to Calaborate rather than Gray. *See supra* note 23. As discussed further below, Plaintiff fails to establish that logging into a third-party account, even if that third-party account has some relationship to the employer's accounts, constitutes access to Calaborate's computers.

audit log. A token audit log shows all of the instances in which a user granted or revoked a programmatic connection into Google Apps." Anderson Decl., Dkt. 355-6 at 2. Plaintiff's Exhibit 208 represents this "Audit Log," which spans four exhibits (208A–D), dozens of pages, and thousands of lines of data, with each entry demonstrating an action taken by the Individual Defendants' Calaborate Email accounts.[26] *See* Dkt. 387, Attachments 37–40. However, every entry in the Audit Log related to backing up Gray's Calaborate Email occurs on April 15, 2015, while Gray was still authorized to access Calaborate's computers. *See id.* As such, Plaintiff has failed to demonstrate that Gray accessed Calaborate's computers without authorization or exceeding authorization by backing up his Calaborate Email via Backupify.

The Audit Log also shows that Gray's Backupify account was accessed on one occasion after Gray left Calaborate—April 24, 2015. Dkt. 387-37, Exh. 208-A. The Audit Log does not show that Gray directly accessed his Calaborate Email on April 24; the Audit Long only shows that Gray accessed his Backupify account, which was still linked to Gray's Calaborate Email. On that date, it is undisputed that the only action taken was a deauthorization of Backupify from further accessing Gray's Calaborate Email. As opposed to the thousands of entries on April 15, the Audit Log of April 24 only shows six total entries—all demonstrating that Backupify was revoked permission to access Gray's Calaborate Email. There is no evidence that Gray's Backupify account had any other interaction with Gray's Calaborate Email on April 24. Plaintiff argues that this still constitutes an unauthorized access of the Calaborate Email account because Gray's employment ended on April 15, 2015. Plaintiff fails to demonstrate, however, how Gray's alleged access of his own third-party Backupify account constitutes an access of Calaborate's computers, especially when Gray owned the third-party account in question and the only interaction between the Backupify account and the Calaborate Email was a deauthorization of further access.[27] Although the Audit Log shows Gray accessed Backupify on April 24, it does not show that Backupify accessed the Calaborate Email on that date. To the contrary, the evidence only shows Backupify deauthorized access to the Calaborate Email on April 24, 2015.

[26] All Individual Defendants had @calaborate.com accounts hosted in Google's suite of services which are referred to here as their Calaborate Email accounts, although they encompass more than just email.

[27] As a practical matter, Gray had to deauthorize the Backupify account at some point to fully sever himself from Calaborate. Given the Ninth Circuit's consistently narrow interpretation of the CFAA, it seems unlikely the Court should read "access" to include such a de minimis interaction, especially where the undisputed sole purpose of the action is to prevent further access. *See Nosal I*, 676 F.3d at 863 ("This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking . . .").

Plaintiff argues that third-party accounts like Evernote and Dropbox can be protected computers under the CFAA.[28] Dkt. 387 at 19 n.9. Even if the Court were to accept this as a blanket rule, it is inapplicable to Plaintiff's case for two reasons. First, Plaintiff fails to establish the third-party accounts in question were owned by Calaborate. *See supra* note 23. Plaintiff has no authority to grant or deny Defendants access to their own accounts. Second, Plaintiff fails to show that the third-party accounts had any interaction with the protected Calaborate Email accounts. Although there is evidence that Gray accessed Backupify (which was still linked to the Calaborate Email) after he left Calaborate, there is no evidence that Backupify accessed the Calaborate Email. Because the Audit Log chronicles every action taken between Backupify and Gray's Calaborate Email, if the Backupify account had any other interaction with the Calaborate Email account it would be represented in the Audit Log. Without any evidence of interaction between the Backupify account and the Calaborate Email, there is no evidence that Gray accessed his Calaborate Email without authorization.

Finally, it is undisputed that Gray turned over access to his Calaborate Email on May 4, 2015, at which time Kolokotrones reset the password. Dkt. 374 at 6. This turnover is reflected in the Audit Log by an entry on May 4, 2015 showing "Hunter Gray authorized access to iOS Account Authorize." Dkt. 387-37, Exh. 208-A. Because Gray's account was undisputedly "the master account for all of Calaborate Google accounts," this password reset gave control over all of Individual Defendants' Calaborate Emails to Kolokotrones on May 4, 2015. Dkt. 374 at 6. With the password reset, any action taken from Gray's Calaborate Email after May 4, 2015 cannot be imputed to Gray.[29] Plaintiff has therefore failed to raise a genuine issue of fact as to whether Gray accessed Calaborate's computers without authorization or exceeding authorization.

---

[28] Plaintiff presents two out of circuit district court cases for this proposition: *Stirling Int'l Realty, Inc. v. Soderstrom*, No. 6:14-CV-1109-ORL-40, 2015 WL 2354803 (M.D. Fla. May 15, 2015), and *Simmonds Equip., LLC v. GGR Int'l, Inc.*, 126 F. Supp. 3d 855 (S.D. Tex. 2015). In *Stirling International Realty*, the court determined that the defendant may have violated the CFAA by logging into a suite of Microsoft services that was undisputedly owned by the plaintiff. *Stirling*, 2015 WL 234803, at *2. In *Simmonds*, the court found CFAA liability plausible when the defendant used a third-party website to delete large portions of the plaintiff's website.

[29] This includes every access of Gray's Calaborate Email after May 4, 2015. Plaintiff's argument that Gray accessed and archived his Calaborate Email on "June 8, June 11, and June 19, 2015" is not supported by any evidence because Gray undisputedly no longer had the password to the account. Dkt. 370-1 SAUF ¶ 353. Further, the underlying evidence only shows the account was backed up, not who actually initiated the action. *See* Dkt. 387-36, Exh. 205–07.

Initials of Preparer : PMC

2. Lisa Dusseault

Both Dusseault and Efremidze stopped working at Calaborate on March 26, 2015. Dkt. 370-1 SAUF ¶ 209. Plaintiff alleges Lisa Dusseault accessed her Calaborate Email (lisa@calaborate.com) on May 5, 2015. As explained above, however, this was undisputedly *after* Kolokotrones had reset the password for the master Calaborate Email. This gave Calendar Research the absolute authority to control all of the other Calaborate Email accounts, including Dusseault's and Efremidze's. Plaintiff's evidence does not show Dusseault logged into the Calaborate Email; it only shows that *someone* logged in on May 5, 2015. Dkt. 387-35, Exh. 203. With the account under Calendar Research's complete control, the Court is unable to speculate that Dusseault actually affected this login. *See Brekka*, 581 F.3d at 1136 ("While we must draw all reasonable inferences in favor of the non-moving party, we need not draw inferences that are based solely on speculation.").

In *Brekka*, the Ninth Circuit considered a similarly dubious login to an employee's work account after the employee had been terminated. There, the defendant presented undisputed evidence that several employees had access to his login information after his employment was terminated. *Id.* at 1136. Just like in *Brekka*, the Plaintiff here undisputedly had access to Dusseault's Calaborate Email after May 4, 2015. Much like the plaintiff in *Brekka,* "[i]n its response to the motion for summary judgment, [Plaintiff] did not provide any explanation, let alone supporting evidence, to show" it was the defendant who logged in. Dusseault has provided direct testimony that she did not login at this time. Dkt. 399 at 11. It is entirely plausible that Plaintiff logged into Dusseault's Calaborate Email one day after receiving complete control of the account. It is implausible that Dusseault, having just lost access to her account, would be able to login the day after turning it over. "If the factual context makes the non-moving party's claim of a disputed fact implausible, then that party must come forward with more persuasive evidence than otherwise would be necessary to show that there is a genuine issue for trial." *Brekka*, 581 F.3d at 1137 (internal quotation marks omitted). Plaintiff has produced nothing to show Dusseault logged in; this is plainly insufficient to raise a genuine issue of fact.

Finally, as discussed *supra* Part III.a.iv.2, it is undisputed that Dusseault retained some of Calaborate's code on her personal laptop. Dkt. 399 at 9. But it is further undisputed that the code was created on her computer while employed at Calaborate and in the regular course of her duties therein. *Id.* Without unauthorized access or access exceeding authorization, this fails to create liability under the CFAA. *See New Box Sols., LLC v. Davis*, No. CV 18-5324-RSWL-KSX, 2018 WL 4562764, at *10 (C.D. Cal. Sept. 18, 2018). Thus, Plaintiff has failed to raise a genuine issue of material fact regarding Dusseault's access of Plaintiff's protected computers.

Initials of Preparer PMC

3. Lasha Efremidze

Plaintiff's forensic technology expert, Anderson, concludes that "Efremidze authorized iOS access for his Calaborate email account on June 8, 2015." Dkt. 355-6 at 2. This conclusion is not supported by the evidence, however, as the login occurred after the master password was transferred and reset. Plaintiff provides no additional evidence beyond speculation by which the Court could conclude that Efremidze, not Plaintiff, actually logged into the account on June 8, 2015. *See Brekka*, 581 F.3d at 1136–37.

There is evidence, however, that Efremidze directly accessed his Calaborate Email after leaving Calaborate but before the password handover.[30] Plaintiff has presented evidence that Efremidze's Calaborate Email (lasha@calaborate.com) was directly archived through Google on April 13, 2015. Dkt. 387-41, Exh. 209. Unlike the previously discussed logins, this event occurred in the limited window between Efremidze leaving Calaborate on March 26, 2015 but before the master password was turned over on May 4, 2015. Unlike Dusseault's login, there is no evidence on the record that anyone else may have accessed Efremidze's Calaborate Email on the date of the login. This is enough to raise a genuine issue of material fact as to whether Efremidze logged into his Calaborate Email without authorization or exceeding authorization on April 13, 2015.

Plaintiff has presented evidence to raise an issue of fact as to whether Efremidze accessed a protected computer without authorization under § 1030(a). However, to maintain a civil action under § 1030(g), Plaintiff must also show that the alleged access caused "damage or loss." *See Andrews*, 932 F.3d at 1262 (quoting § 1030(g)) (The CFAA "provides a private right of action for '[a]ny person who suffers damage or loss by reason of a violation of [the statute] . . . .").

a. Damage

Plaintiff fails to present any evidence that the alleged backup caused damage. The only action Efremidze is alleged to have taken (which is supported by the record) is archiving his Calaborate Email account on April 13, 2015. Courts have emphasized that a "mere copying of data is not enough" to

[30] This evidence was, inexplicably, not addressed by Plaintiff's expert. Plaintiff's argument regarding this login is extremely cursory, stating only "All three Individual Defendants archived and accessed their Calaborate email accounts after they resigned from Calaborate," and citing sections of Plaintiff's SAUF. Dkt. 387 at 21. Examining the underling SAUF, Plaintiff argues, "Following his departure from Calaborate, Efremidze archived his lasha@calaborate.com account," but does not specify the date which this is alleged to have happened. Dkt. 370-1 SAUF ¶ 357. However, Exhibit 209, does indicate that someone accessed and archived lasha@calaborate.com on April 13, 2015. Dkt. 387-41, Exh. 209.

satisfy the damage requirement of the CFAA. *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 961–62 (N.D. Cal. 2014); *see NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 834 (N.D. Cal. May 12, 2014) ("[Plaintiff] alleges only that [defendant] accessed its databases without permission, not that he damaged any systems or destroyed any data."); *Doyle v. Taylor*, No. CV-09-158-RHW, 2010 WL 2163521, at *2 (E.D. Wash. May 24, 2010) (copying and distributing files off of plaintiff's thumb drive was not cognizable "damage" under the CFAA); *see also Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc.*, 616 F. Supp. 2d 805, 811 (N.D. Ill. Mar. 19, 2009) ("copying electronic files from a computer database . . . is not enough to satisfy the damage requirement of the CFAA"). Without a showing of damage related to Efremidze's allegedly unauthorized access, Plaintiff has not met its burden under § 1030(a)(5)(B), which requires a defendant "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage . . . ." Plaintiff also fails to support its claim under § 1030(a)(5)(C), which requires a showing of "damage and loss."

b. Loss

Although Plaintiff has not presented evidence of damage related to Efremidze's alleged unauthorized access, CFAA liability under §§ 1030(a)(2)(C) and (a)(4) is still permissible with a finding of loss. "The CFAA defines 'loss' as 'any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.'" *Erhart v. BofI Holding, Inc.*, No. 15-CV-02287-BAS-NLS, 2020 WL 1550207, at *46 (S.D. Cal. Mar. 31, 2020) (quoting CFAA § 1030(e)(11)); *see also Del Monte Fresh Produce*, 616 F. Supp. 2d at 811("A plaintiff that has not suffered any damage may still prevail on a CFAA claim by showing that it has suffered a loss."). Of the CFAA violations alleged, "the only one relevant to [Plaintiff's] potential claim is that the offense caused 'loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value.'" *Andrews*, 932 F.3d at 1263.

Plaintiff claims the cost of its forensic investigation to determine who accessed its computers cost over $5,000, thus satisfying the requirements of the statute.[31] Dkt. 365-3 ¶ 10. The cost of

[31] Individual Defendant's object to the inclusion of this statement as a belated disclosure under Fed. R. Civ. P. 37. However, Plaintiff has alleged loss in its Fifth Amended Complaint, dkt. 181, even if was not directly tied to the forensic investigation. Defendants also do not dispute that a professional forensic investigation occurred, and Defendants have been able to respond to the results of that investigation in their reply briefs. If Plaintiff had produced this evidence of loss (one line in

Plaintiff's forensic investigation is cognizable as "loss," but not "damage." *See NovelPoster*, 140 F. Supp. 3d at 962 (distinguishing damage and loss under the CFAA). As stated above, however, Plaintiff has failed to specify which provision of § 1030(a) Efremidze's alleged access violates. Having excluded § 1030(a)(5)(B)–(C), only §§ 1030(a)(2)(C) and (a)(4) remain. Under CFAA § 1030(a)(4), Plaintiff must present evidence that Defendant:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and *obtains anything of value*, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period...

CFAA § 1030(a)(4) (emphasis added). "In other words, Plaintiff must demonstrate that a defendant: "(1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value,' causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value." *Ewiz Express Corp.*, 2015 WL 5680904, at *4 (quoting CFAA § 1030(a)(4)).

As briefly discussed earlier, § 1030(a)(4) requires an "intent to defraud," but the Court need not reach the intent requirement unless all of the other elements of the statute are satisfied. Assuming Efremidze had the requisite "intent to defraud," Plaintiff has still failed to present any evidence that Efremidze "obtained anything of value" by backing up his account. CFAA § 1030(a)(4). Because the Court determined that Defendants did not misappropriate any trade secrets, it was Plaintiff's burden to show that the information obtained by backing up the account contained some other information of value. Plaintiff has not cited to any evidence establishing the value of information in Efremidze's

---

Kolokotrones' declaration) during discovery, Defendants' dispute of that evidence would, at most, create a factual issue to be resolved at trial. This new evidence of loss is not the type of new theory of damages that would "most likely require[] the court to create a new briefing schedule and perhaps re-open discovery." *Hoffman v. Constr. Protective Servs., Inc.*, 541 F.3d 1175, 1180 (9th Cir. 2008). The cost of this forensic investigation is not entirely inconsistent with Plaintiff's earlier testimony that Kolokotrones investigated the computers himself, although it does supplement the record somewhat. This belated disclosure does not warrant the strong remedy of summary judgment. *AtPac, Inc. v. Aptitude Sols., Inc.*, 787 F. Supp. 2d 1108, 1112 (E.D. Cal. 2011) (defendants have "not shown that the supplemental responses are inconsistent with plaintiff's prior testimony, as opposed to merely expanding on it.").

account beyond the alleged trade secrets. Based on the discussion above, Plaintiff has failed to show evidence to raise a genuine issue of fact as to whether Efremidze "obtain[ed] anything of value" from his Calaborate Email. *Ewiz Express Corp.*, 2015 WL 5680904, at *4 (quoting CFAA § 1030(a)(4)).

This leaves only § 1030(a)(2)(C), which allows liability if a defendant accesses a protected computer without authorization and obtains "information from any protected computer." If Efremidze archived and downloaded his Calaborate Email account, he may have obtained information that belonged to Calaborate. Plaintiff has therefore raised a genuine issue of fact that Efremidze's allegedly unauthorized access violated the CFAA under §§ 1030(a)(2)(C).

ii. Deletion of Files

Plaintiff also argues that Individual Defendants violated the CFAA by deleting Calaborate's files off of their work computers and devices before returning them. There is no dispute that Individual Defendants were generally authorized to modify and delete files on Calaborate's computers. Dkt. 387 at 22. The only question relevant for the CFAA is whether Defendants deleted the files while still employed. Plaintiff's own expert concludes the devices were wiped before Gray left Calaborate.[32] Dkt. 355-6 ¶ 15. Plaintiff presents these alleged deletions as a CFAA violation because Plaintiff claims it was unable to recover the files allegedly deleted, which caused damage to Plaintiff's ability to use the Klutch application.[33] *Id.* at 22. However, Plaintiff fails to establish that Individual Defendants were not authorized to delete files off of their work computers while they were still employed. Unlike other cases finding plausible CFAA liability, Plaintiff here had not revoked Defendants' access to the computer at the time of the alleged erasure. *See Erhart v. BofI Holding, Inc.*, No. 15-CV-02287-BAS-NLS, 2020 WL 1550207, at *46 (S.D. Cal. Mar. 31, 2020) (denying summary judgment for the defendant when the plaintiff provided direct testimony that defendant "did not have permission . . . to delete information from the protected computer."); *1-800 Remodel, Inc.*, 2018 WL 6340759, at *7 (denying motion to dismiss CFAA claims where the employee deleted and forwarded emails after employer had explicitly revoked her access to any work computer).

[32] Anderson only provided conclusions for the dates of the data wipes for some devices, all of which occur before Gray left Calaborate. Anderson also does not specify *who* erased the devices, just that they were erased. *See* Anderson Decl., Dkt. 355-6.

[33] Although Defendants argue they backed up their devices to Calaborate's computers before wiping their devices, the Court cannot weigh evidence on summary judgment. Since Plaintiff fails to establish the alleged deletions were not authorized, this dispute does not create a genuine issue of material fact as to Plaintiff's CFAA claims.

"View[ing] all inferences drawn from the underlying facts in the light most favorable to the nonmoving party," *Apodaca v. White,* 401 F. Supp. 3d 1040, 1047 (S.D. Cal. 2019) (citing *Matsushita*, 475 U.S. at 587), the evidence only shows Individual Defendants deleted files they were authorized to access while employed at Calaborate. Plaintiff has cited no evidence to show that the Individual Defendants were restricted in their ability to copy, modify, or delete files on Calaborate's systems while employed. "As long as [defendant] was authorized to access the computers, the CFAA does not penalize what he did with the information he accessed." *New Box*, 2018 WL 4562764, at *10; *see also Clarity Servs., Inc. v. Barney*, 698 F. Supp. 2d 1309, 1316 (M.D. Fla. 2010) ("To show that [defendant] exceeded his authorized access to the laptop or accessed the laptop without authorization, [plaintiff] must evidence an attempt to restrict [defendant's] access to the laptop."). Even if the Individual Defendants intended harm by wiping their computers, the CFAA does not punish employees who take otherwise-authorization actions for improper purposes. *See Cornerstone Staffing Sols., Inc. v. James*, No. 12-CV-01527 RS, 2013 WL 12124430, at *9 (N.D. Cal. Oct. 21, 2013) ("Because the Ninth Circuit has interpreted 'access without authorization' to apply to outside hackers for purposes of subsections (a)(4) and (a)(2)(C), it stands to reason that 'intentionally causes damage without authorization' in subsection (a)(5)(A) was also intended to guard against outside hackers, not inside employees who impermissibly delete employer files."); *see also Dresser-Rand Co. v. Jones,* 957 F. Supp. 2d 610 (E.D. Pa. 2013) ("Whatever happens to the data subsequent to being taken from the computers subsequently is not encompassed in the purview of the CFAA."). The alleged deletions may be a violation of Individual Defendants' agreements with Calaborate, but even if the employees violated their agreements with the employer, there is no CFAA liability unless the employee was not authorized to access the files.[34] Here, all Individual Defendants were undisputedly authorized to access the files on their computers, and they were even *required* to delete some files on their computers upon termination**.** Dkt. 387 at 21. Accordingly, Plaintiff has failed to raise a genuine issue of fact regarding Individual Defendant's deletion of files.

iii. Private Key

Plaintiff also alleges that Defendants withheld the Android Private Key,[35] which was required to

[34] Even if the alleged deletion caused damage, since the actions were within the scope of the employee's authorization, there is no liability under CFAA. Plaintiff's arguments regarding *NovelPoster* are inapposite because Individual Defendants here were authorized to access their own Calaborate Email accounts before they resigned. 140 F. Supp. 3d at 956. As described above, there is no evidence Individual Defendants deleted their Calaborate Email accounts without authorization, which was an essential allegation in *NovelPoster*.

[35] Neither of Plaintiff's oppositions make any mention of an "Amazon Private Key" or "Amazon Web Services Account,"

update the Klutch app in the Google Playstore. Unlike the alleged trade secrets, the Private Key itself did not contain independently valuable information; it is just a digital password which allows the holder to access and update the Klutch app on the Google store. Plaintiff does not explain how this password can itself constitute a protected computer under the CFAA, but even assuming the Private Key constitutes a protected computer, Plaintiff presents no evidence beyond speculation that the Individual Defendants had possession, actual or constructive, of the Key after leaving Calaborate.

Plaintiff claims it began seeking the Private Key in 2015, Dkt. 370-1 SAUF ¶ 660, at which time Gray instructed Plaintiff to contact Steve Oren, a non-defendant in this case and a "senior mobile engineer for Android at Calaborate beginning on November 22, 2013." *Id.* ¶ 14. Plaintiff has presented no evidence to indicate it contacted Orens. Instead, Plaintiff claims to have relied on Gray's statement that neither he nor Orens knew where the Key was located. Dkt. 387 at 25. Plaintiff has not presented any evidence beyond speculation to show that Gray actually knew where the Key was at that time. *See Crawford-El v. Britton*, 523 U.S. 574, 600 (1998) ("plaintiff may not respond simply with general attacks upon the defendant's credibility, but rather must identify affirmative evidence from which a jury could find that the plaintiff has carried his or her burden of proving the pertinent motive"); *Miller v. Baxter Healthcare Corp.*, 165 F. App'x 550, 553 (9th Cir. 2006) ("Plaintiffs cannot rely on credibility attacks to defeat summary judgment.").

The record shows Plaintiff sought a writ of possession for the Private Key in May of 2017, Dkt. 370-1 SAUF ¶ 683, and in response Gray testified that he did not know where the Key was located. *Id.* ¶ 684. Both Gray and Efremidze have testified that it was not until July of 2017 that Gray learned from Efremidze that Jose Ayerdis, "the Calaborate programmer developing the Android version of Klutch from June of 2014 until Plaintiff's foreclosure in 2015," may have the Android Key.[36] Dkt. 340 at 11; Gray Decl. Dkt. 340-1; Efremidze Decl. Dkt. 340-2. Plaintiff admits that, after Gray informed Plaintiff of what Efremidze had said, Plaintiff contacted Ayerdis and the Private Key was delivered within a matter of days. *See* Dkt. 387 at 25; Dkt. 370-1 SAUF ¶ 669. Moreover, Plaintiff has presented no

see Dkt. 370, Dkt. 387, so the Court does not consider those arguments as raised here. To the extent Plaintiff argues its Amazon account was unlawfully accessed, Plaintiff has presented no evidence that Defendants ever accessed that account after leaving Calaborate. Even Plaintiff's argument regarding the Android Private Key is vague, claiming "In addition, because Individual Defendants failed to return essential Calaborate assets without authorization, including but not limited to the Android developer key . . ." Dkt. 387 at 24. The Android Private Key is explained *supra* Part III.a.iv.1 note 15.

[36] Ayerdis was an independent contractor with Calaborate who worked from Nicaragua, dkt. 370-1 SAUF ¶ 17, and was later hired to work for Gray on StubHub projects. Dkt. 387 at 25.

evidence that it ever contacted Ayerdis (a Calaborate employee known to Plaintiff) before late 2017. Dkt. 370-1 SUF ¶ 55. Plaintiff has presented no evidence that, despite deposing him, it ever asked Efremidze about the location of the Private Key. Plaintiff has not presented any evidence that it sought discovery from or deposed Orens, the employee identified by Gray as in charge of the Android Private Key. Plaintiff has failed to meet its burden to show that any individual Defendant had possession of the Key or withheld information of whereabouts from Plaintiff.

Plaintiff has also failed to present evidence to show any of the Individual Defendants actually or constructively possessed the Private Key after leaving Calaborate. To impute constructive possession of the Private Key to Gray would require impermissible speculation, as Plaintiff has presented no evidence to suggest Gray knew who possessed the Key beyond what he told Plaintiff. *See Nelson v. Pima Cmty. Coll.*, 83 F.3d 1075, 1081–82 (9th Cir. 1996) ("mere allegation and speculation do not create a factual dispute for purposes of summary judgment."). The only evidence in the record shows that the Private Key was in the possession of Ayerdis, a non-defendant in this case, and was returned promptly once Plaintiff contacted Ayerdis. Dkt. 370-1 SUF ¶ 55; SAUF ¶ 669. This cannot create liability under the CFAA, which is "aimed at 'hackers who accessed computers to steal information or to disrupt or destroy computer functionality.'" *Nosal II*, 844 F.3d at 1028 (quoting *Brekka*, 581 F.3d at 1130–31). Accordingly, Plaintiff has failed to raise a genuine issue of fact regarding the Private Key.

iv. Conspiracy and Vicarious Liability

Having dismissed all but one of Plaintiff's substantive claims, the Court now turns to vicarious and conspiracy liability. As both vicarious liability and conspiracy require an underlying substantive violation, *see Ajetunmobi,* 595 F. App'x at 683, the only wrongful act for which any Defendant could be liable is Efremidze's allegedly unlawful access of his Calaborate Email on April 15, 2015. Accordingly, the Court bifurcates the vicarious liability and conspiracy claims from the remaining alleged violation under § 1030(a)(2)(C). Although Plaintiff has presented no evidence that StubHub or eBay actually knew of this allegedly unlawful access, deliberate ignorance can sometimes result in aiding and abetting liability under the CFAA. *Nosal I*, 844 F.3d at 1024. Conspiracy liability is specifically provided for in the CFAA under § 1030(b), but Plaintiff may not rely on general or conclusory allegations of conspiracy. *NetApp*, 41 F. Supp. 3d at 836. Accordingly, as stated above, any vicarious or conspiracy liability must be tied to Efremidze's allegedly unauthorized access on April 13, 2015. Litigation will proceed as to vicarious and conspiracy liability only if Efremidze is found liable for the underlying CFAA violation, and Plaintiff is able to present evidence already in the record that shows agreement or deliberate ignorance by the remaining Defendants.

Initials of Preparer PMC

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	2:17-cv-04062-SVW-SS	Date	May 13, 2020
Title	*Calendar Research LLC v. StubHub, Inc. et al*		

IV. **Conclusion**

The sole issue remaining for trial is whether Efremidze accessed his Calaborate Account on April 13, 2015 without authorization, and, if so, what loss that incurred to Plaintiff. "The statute's 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself." *Andrews*, 932 F.3d at 1263. The only loss related to hacking for which Plaintiff has provided any evidence is the cost of Plaintiff's forensic investigation of its computer systems. Therefore, Plaintiff may only recover for this loss, and Plaintiff must show this loss is related to Efremidze's allegedly unlawful access. Plaintiff is not permitted include other litigation expenses, such as expert testimony or discovery in anticipation of this lawsuit. *See Wichansky v. Zowine*, 150 F. Supp. 3d 1055, 1071–72 (D. Ariz. 2015) ("such expenses are not a cognizable loss under the CFAA"); *Delacruz v. State Bar of California*, No. 16-CV-06858-BLF, 2018 WL 3077750, at *8 (N.D. Cal. Mar. 12, 2018), *aff'd*, 768 F. App'x 632 (9th Cir. 2019) ("legal expenses are not a cognizable loss under the CFAA"); *see also Brooks v. AM Resorts, LLC*, 954 F.Supp.2d 331, 338 (E.D. Pa. 2013) ("fees paid to an expert to assist in litigation" do not constitute a "loss" under CFAA); *First Mortg. Corp. v. Baser*, 2008 WL 4534124, at *3 (N.D. Ill. Apr. 30, 2008) ("costs unrelated to the computer itself, such as litigation expenses or speculative future damages do not qualify."). The trial will be accordingly limited.

The Court GRANTS summary judgment as to all Defendants on Plaintiff's DTSA claims. The Court GRANTS in part and DENIES in part Defendants' motion for summary judgment of the CFAA claims. A jury trial on the sole remaining issue is scheduled for July 7, 2020, at 9:00 a.m., with a pretrial conference set for June 29, 2020 at 3:00 p.m.

IT IS SO ORDERED.

:

Initials of Preparer PMC