UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

LIVEPERSON, INC.,

Plaintiff,

- against -

14 Civ. 1559 (RWS)

AMENDED OPINION

24/7 CUSTOMER, INC.,

Defendant.

----------X

A P P E A R A N C E S:

Attorneys for Plaintiff

HONIGMAN MILLER SCHWARTZ AND COHN LLP
130 S. First Street, 4th Floor
Ann Arbor, MI 48104
By: J. Michael Huget, Esq.

HONIGMAN MILLER SCHWARTZ AND COHN LLP
660 Woodward Ave, 2290 First National Bldg.
Detroit, MI 48226
By: Roger P. Meyers, Esq.

DUANE MORRIS, LLP
190 South LaSalle Street, Suite 3700
Chicago, IL 60603
By: Jeffrey K. Lamb, Esq.

COHEN & GRESSER LLP
800 Third Avenue, 21st Floor
New York, New York 10022
By: Mark S. Cohen, Esq.
Sandra C. McCallion, Esq.

Attorneys for Defendant

O'MELVENY & MYERS, LLP
7 Times Square
New York, NY 10036
By: Carolyn S. Wall, Esq.

O'MELVENY & MYERS, LLP
Two Embarcadero Center, 28th Floor
San Francisco, California 94111-3823
By: George A. Riley, Esq.
Mark E. Miller, Esq.
David Eberhart, Esq.
Elysa Q. Wan, Esq.

O'MELVENY & MYERS, LLP
2765 Sand Hill Road
Menlo Park, CA 94025
By: Susan Roeder, Esq.

Sweet, D.J.

Defendant 24/7 Customer, Inc. ("[24]7" or "24/7" or "Defendant), moves to dismiss plaintiff Liveperson, Inc.'s ("LivePerson" or "Plaintiff") First Amended Complaint ("FAC" or "Complaint") filed May 15, 2014. As to any claims not dismissed, Defendant moves for an order requiring Plaintiff to provide a more definite statement. Based upon the conclusions set for below, the motion to dismiss the complaint is granted in part and denied in part, and the motion for a more definite statement is granted in part and denied in part.

Prior Proceedings

LivePerson initiated this action on March 6, 2014 by filing a summons and complaint. On May 15, 2014, Plaintiff filed the FAC alleging: (i) copyright infringement in violation of 17 U.S.C. § 101 et seq.; (ii) violation of the Digital Millennium Act, 17 U.S.C. § 1201(a) ("DMCA"); (iii) violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"); (iv) misappropriation of trade secrets; (v) breach of contract; (vi) intentional interference with advantageous existing economic relationships; (vii) intentional interference with prospective advantageous economic relationships; (viii) unfair

competition in violation of the Lanham Act, 28 U.S.C. § 1125(a); (ix) common law unfair competition; and (x) unjust enrichment. On July 18, 2014, Defendant filed the instant motion, seeking to dismiss each of Plaintiff's ten causes of action, and further seeking an order for a more definitive statement for any of Plaintiff's claims that are not dismissed. The instant motion was heard and marked fully submitted on September 24, 2014.

Facts

For the purposes of this motion, the FAC's allegations are assumed true and summarized as follows.

LivePerson, a Delaware corporation with its principal place of business in New York City, provides customers with live-interaction and customer engagement technology for e-commerce websites, enabling businesses to interact in real-time with their website customers. FAC ¶¶ 1, 10. [24]7, a California corporation with its principal place in New York City, is a customer service technology that historically provided human call-center operators to answer phones in customers' call centers. FAC ¶¶ 3, 11. More recently, [24]7 also developed its own live-interaction technology. FAC ¶ 7.

In 2006 and 2007, [24]7 and LP entered into two contracts to cooperatively market to and serve certain customers: a Co-Marketing and Referral Agreement ("CMA") and a Master Service Agreement ("MSA"). FAC Ex. A and Ex. B. The contracts were executed in support of the "joint solutions" the parties intended to offer their clients, namely, use of LivePerson's technology coupled with [24]7's call center personnel. FAC ¶ 3.

Under the CMA, which took effect on July 10, 2006, [24]7 obtained a license to "access, operate, and use" LivePerson's intellectual property as specified in the CMA until expiration or termination of the agreement. CMA ¶ 2.1. The parties acknowledged the CMA did not grant a party the rights to the other party's intellectual property beyond the limited license granted in the agreement. CMA ¶ 2.4. The CMA permitted each party to co-market the other party's products and services to certain third parties, but each party reserved the right to "sell, license, support and install its own products and services either directly to customers or indirectly" through various distribution channels. CMA ¶¶ 4.1, 4.3. The CMA included schedules listing LivePerson's customers and [24]7's customers. FAC Ex. A Schedules 1, 2.

On January 26, 2007, [24]7 and LivePerson entered into the MSA. Among other things, LivePerson agreed to provide [24]7 with "access to and license to use" LivePerson's service for the purpose of delivering services to these clients. MSA ¶¶ 5(b), 7(a). The MSA set forth the terms and conditions under which LivePerson was able to offer the combined solution to its clients. FAC ¶ 27.

[24]7 began to develop its own competing live-interaction technology, allegedly by misappropriating LivePerson's software and selling it as its own. FAC ¶ 35. [24]7 also allegedly engaged in additional improper conduct in order to gain a competitive edge over LivePerson. See generally FAC ¶ 35-51. The alleged conduct includes accessing LivePerson's back-end systems to download and manipulate LivePerson's data for the purpose of copying LivePerson's technology, and interfering with LivePerson's client relationships. FAC ¶ 37. [24]7 also allegedly designed its competing software to both interfere with LivePerson's software, such that a customer using both technologies on its website would experience poor performance from LivePerson's technology, and to collect performance data from LivePerson's data, which would then be sent to [24]7. FAC ¶¶ 39, 40, 44. [24]7 used its access to LivePerson's code to "mimic" LivePerson, thereby

gaining access to LivePerson's servers and mining LivePerson's confidential and proprietary system data. FAC ¶ 41. [24]7's alleged conduct also included poaching LivePerson employees to work for [24]7, falsely claiming that [24]7's software is the "first predictive or smart chat platform," and disseminating fabricated and disparaging LivePerson performance metrics to clients. FAC ¶¶ 38, 45-46.

The Applicable Standard

Under Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 663 (quoting Twombly, 550 U.S. at 556). In other words, the factual allegations must "possess enough heft to show that the pleader is entitled to relief." Twombly, 550 U.S. at 557 (internal quotation marks omitted).

Though the court must accept the factual allegations

of a complaint as true, it is "not bound to accept as true a legal conclusion couched as a factual allegation." Iqbal, 556 U.S. at 678 (quoting Twombly, 550 U.S. at 555).

In considering a motion to dismiss, "a district court may consider the facts alleged in the complaint, documents attached to the complaint as exhibits, and documents incorporated by reference in the complaint." DiFolco v. MSNBC Cable L.L.C., 622 F.3d 104, 111 (2d Cir. 2010).

The Copyright Infringement Claim Is Not Adequately Pled

The parties agree that a copyright infringement claim must allege: (1) which specific original works are the subject of the claim; (2) plaintiff's ownership of the copyrights in those works; (3) proper registration of the copyrights; and (4) "by what acts during what time the defendant infringed the copyright." Kelly v. L.L. Cool J., 145 F.R.D. 32, 36 (S.D.N.Y. 1992), aff'd, 23 F.3d 398 (2d Cir. 1994), cert. denied, 513 U.S. 950 (1994), cited in Def.'s Mem. in Supp. 4 and Pl.'s Mem. in Opp'n 5.

With respect to the first three elements, Plaintiff has adequately identified the LivePerson Visitor Monitoring

Module (the "Module") as its original work, alleged that it is copyrighted, and that the copyright was registered with the United States Copyright Office. See FAC ¶ 53 and FAC Ex. C. Defendant contends, however, that Plaintiff has failed to adequately plead the fourth infringement element.

Plaintiff alleges that "24/7, without LivePerson's authorization or consent" copied "LivePerson's own copyrighted software code." FAC ¶ 53. Plaintiff further alleges that "[24]7's conduct constitutes direct and intentional infringement of LivePerson's exclusive rights under the Copyright Act to control the reproduction, publication, use and display of LivePerson's live-interaction technology, including the LivePerson Visitor Monitoring Module." FAC ¶ 54.

Defendant contends that Plaintiff fails to adequately allege the time of infringement, that the FAC does not identify [24]7's infringing product, and that the Plaintiff has not pled which aspects of its Module were copyrightable. Def.'s Mem. in Supp. 5-6. For the purposes of a motion to dismiss, courts evaluating the time of infringement element under Kelly consider whether the complaint, read in the light most favorable to the non-moving party, contains enough factual allegations to provide notice of the period of time during which infringement occurred.

See Tangorre v. Mako's, Inc., 01-cv-4430, 2002 WL 313156, at *3 (S.D.N.Y. Jan. 30, 2002) (collecting cases to outline the distinction: "Compare Carell v. Shubert Org., Inc., 104 F. Supp. 2d 236, 251 (S.D.N.Y. 2000) (complaint sufficient under Rule 8 [. . .] where plaintiff alleged the publication of certain designs in national and international stage productions and videos in 1997 and 1998 and their use in certain commercial products) and Kelly, 145 F.R.D. at 36 n.3 (infringement claim adequately supported when plaintiff narrowed the infringing act to the publishing and distribution of two specific songs during 1991) with Mahnke v. Munchkin Prod., Inc., 99-cv-4684, 2001 WL 637378, at *5 (S.D.N.Y. Jun. 07, 2001) (no proper allegation of the nature of the infringing act with only generic references to an infringing 'baby soda bottle,' beginning some time in 1993) and Plunket v. Doyle, 99-cv-11006, 2001 WL 175252, at *5 (S.D.N.Y. Feb. 22, 2001) (claim insufficiently detailed where plaintiff merely alleged that defendants had entered into or had offered licenses "granting the rights to exploit [the books at issue] in various media" during an unspecified period of time)").

A complaint containing no reference to time of infringement will not survive a motion to dismiss, but one in which the plaintiff alleges continued infringement from a

specific time to the present may survive. Compare Jacobs v. Carnival Corp., 06-cv-0606, 2009 WL 856637, at *5 (S.D.N.Y. Mar. 25, 2009) (granting motion to dismiss where "Plaintiffs make no reference whatsoever to time in the Complaint") with Home & Nature Inc. v. Sherman Specialty Co., 322 F. Supp. 2d 260, 266-267 (E.D.N.Y. 2004) (denying motion to dismiss where complaint alleges ongoing infringement since December 2000); but see Mahnke, 2001 WL 637378, at *5 (described above).

Plaintiff contends that the FAC's allegations, taken together, are fairly read as alleging that the period of infringement was "between 2006 when the parties began their contractual relationship and May 2014 when LivePerson filed the FAC." Pl.'s Mem. in Opp'n 6. However, the FAC does not specify time of infringement, nor can a period of infringement fairly be implied from the various allegations in the FAC and its exhibits. While the FAC clearly alleges that the parties' contractual relationship began in 2006, this allegation does not place Defendant on notice that the alleged copyright infringement started then as well. Nor does the FAC contain any allegation either stating the end of the infringement period or that the infringement continued from 2006 to the present. This assertion was made for the first time in Plaintiff's brief in opposition, rather than in the FAC. See Pl.'s Mem. in Opp'n 6.

The case law Plaintiff cites in support of its contention that time of infringement is adequately pled does not contradict the outcome here. In Richard Feiner & Co. v. Larry Harmon Pictures Corp., the complaint alleged that the purportedly infringed "copyrights remain in full force as and of the date of this complaint and were in effect at all times during the complained of acts." 38 F. Supp. 2d 276, 279 (S.D.N.Y. 1999). A similar assertion cannot be made by Plaintiff, since the Module was registered in 2014, not in 2006 when the FAC's time frame began. See FAC Ex. C. In Home & Nature, the complaint, unlike here, explicitly alleged ongoing infringement. 322 F. Supp. 2d 260, 266-267. Finally, in Tangorre, the complaint explicitly alleged a defined period, December 21, 2000, through April 5, 2001, during which the copyright was infringed. 2002 WL 313156, at *3 (S.D.N.Y. Jan. 30, 2002).

In addition to its time-of-infringement argument, Defendant further contends that the FAC does not identify [24]7's infringing product, and that the Plaintiff has not pled which aspects of its Module were copyrightable. Def.'s Mem. in Supp. 5-6. The accusation that Defendant copied the entire module necessarily implies that Defendant copied protectible elements of the module. Nevertheless, failure to plead a time period of infringement renders the claim inadequate.

The DMCA Claim Is Not Adequately Pled

Defendant contends that Plaintiff failed to allege both the existence of a technological measure and actions constituting circumvention within the meaning of the Digital Millennium Act. Def.'s Mem. in Supp. 7-8.

The DMCA states, in relevant part, that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a). "[T]o 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201 (a)(3)(A). The act of circumvention under the DMCA can be characterized as "breaking and entering (or hacking) into computer systems. I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004). Moreover, "a person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material." Dish Network L.L.C. v. World Cable Inc., 893 F. Supp. 2d 452, 466 (E.D.N.Y. 2012) (internal quotations and citations omitted).

A "technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201 (a)(3)(B).

Courts in this Circuit have held that password protection, DVD encryption measures, and activation and validation keys are technological measures within the meaning of the DMCA. I.M.S. Inquiry, 307 F. Supp. 2d at 531 (S.D.N.Y. 2004) (password protection); Paramount Pictures Corp. v. 321 Studios, 03-cv-8970, 2004 WL 402756, at *1 (S.D.N.Y. Mar. 3, 2004) (encryption system for DVDs); Macrovision v. Sima Prods. Corp., 05-cv-5587, 2006 WL 1063284, at *1 (S.D.N.Y. Apr. 20, 2006) (same); Adobe Sys. Inc. v. Feather, 895 F. Supp. 2d 297, 301-02 (D. Conn. 2012) (activation and validation key codes for software). Outside this Circuit, a "secret handshake" protocol, a software security measure ensuring that only authorized users would be able to access to a particular website, was found to qualify as a technological measure. Davidson & Associates v. Jung, 422 F.3d 630, 640 (8th Cir. 2005).

The Complaint's allegations here are somewhat contradictory. In one portion, Plaintiff alleges that Defendant

already had access to its backend system pursuant to Defendant's business relationship with Plaintiff, and that Defendant misused its access to "observe, penetrate, and manipulate the operation of LivePerson's technology and download extensive data . . . in order . . . to reverse engineer and copy LivePerson's technology." FAC ¶ 37. Plaintiff further alleges that [24]7 improperly used its knowledge of LivePerson's customer-facing software architecture to mimic LivePerson, thereby gaining unauthorized access to LivePerson's secure internal computer system. FAC ¶ 37. In another part of the Complaint, Plaintiff alleges that [24]7 improperly used its knowledge of LivePerson's customer-facing software architecture to mimic LivePerson, thereby gaining unauthorized access to LivePerson's secure internal computer system. See FAC ¶¶ 41, 61. Once inside LivePerson's secure system, [24]7 allegedly installed spyware to obtain competitive information on LivePerson's software product and also introduced code that would degrade the functionality of LivePerson's software product. FAC ¶¶ 41, 61. The FAC also alleges that, having accessed Plaintiff's internal computer system, Defendant reverse-engineered Plaintiff's software products. FAC ¶ 42.

Plaintiff contends that its allegations are akin to those in Davidson, where the plaintiff established circumvention

by claiming that the defendant reverse-engineered the plaintiff's software in order to bypass the plaintiff's security measures. Pl.'s Mem. in Opp'n 8; see Davidson, 422 F.3d at 641. Even setting aside Paragraph 37's contradicting allegation, the reverse-engineering here is alleged to have occurred after [24]7 allegedly breached LivePerson's system. See FAC ¶ 42. The Complaint does not allege that Defendant used reverse engineering to circumvent its security measures, but rather that "LivePerson believes that [24]7 [breached its security measures] in an effort to reverse engineer and misappropriate the proprietary technology and methodologies that LivePerson pioneered." FAC ¶ 42. In short, the reverse engineering allegations do not constitute circumvention within the meaning of the DMCA.

The remaining allegation that may be construed as "an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material," Dish Network, 893 F. Supp. 2d at 466, is Defendant's purported mimicking Plaintiff in order to gain access to Plaintiff's secure system. However, even if that were to constitute circumvention, Plaintiff does not adequately allege what technological measure the mimicry circumvented. In all of the cases discussed above, including Davidson, upon which Plaintiff

relies, Pl.'s Mem. in Opp'n 8, the complaints explicitly referenced a password, encryption system, software protocol, validation key, or some other measure designed to thwart unauthorized access to a protected work. The FAC states that Defendant, by impersonating Plaintiff, "circumvented LivePerson's security measures" without specifying what those measures were. FAC ¶ 42. Without specifying the technological measure, the FAC does not provide Defendant with adequate notice of the claim, i.e., information upon which to determine whether the measure "effectively controls access to a work" within the meaning of the DMCA. 17 U.S.C. § 1201 (a)(3)(B).

Plaintiff has not adequately alleged circumvention of a technological measure within the meaning of the DMCA.

The CFAA Claim Is Not Adequately Pled

Defendant contends that Plaintiff fails to state a claim under the Computer Fraud and Abuse Act, both because Plaintiff has not pled facts showing that [24]7 exceeded its authorization to access LivePerson's computers and because Plaintiff has not adequately alleged damages cognizable under the CFAA. See Def.'s Mem. in Supp. 9-10.

The CFAA is principally a criminal statute prohibiting "fraud and related activity in connection with computers." 18 U.S.C. § 1030. The Act also establishes a private cause of action against a person who "knowingly accessed a computer without authorization or exceeding authorization," and whose prohibited access result in: (a) "loss" in excess of $5,000; (b) interference with a person's medical treatment; (c) physical injury; (d) a threat to public health or safety; or (e) damage to a specific category computers used by the United States Government and its affiliates. See 18 U.S.C. § 1030(g), referencing 18 U.S.C. § 1030(c)(4)(A)(i)(I)-(V), see generally 18 U.S.C. § 1030(a).

Plaintiff's CFAA claim is presumably based upon economic damages in excess of $5,000, as FAC's allegations foreclose the other bases for liability under the CFAA. See e.g., 18 U.S.C. § 1030(a)(1) (relating to certain classes of computers protected the United States Government); § 1030(a)(3) (relating to certain classes of computers used by the United States Government); § 1030(a)(4) (accessing computers with intent to defraud); § 1030(a)(6) (trafficking in computer passwords); § 1030(a)(7) (engaging in extortion).

To state a claim for loss in excess of $5,000,

Plaintiff must plead that Defendant: (1) accessed a "protected computer"; (2) "without any authorization or exceeding its authorized access"; and (3) caused "loss" in excess of $5,000. See, 18 U.S.C. § 1030(g) referencing 18 U.S.C. § 1030(a)(2) (obtaining information from a "protected computer" through unauthorized access) and § 1030(a)(5) (damaging a protected computer directly through unauthorized access or by knowingly, and without authorization, introducing a program, information, code or command into the protected computer resulting in damage). Under the Complaint's set of allegations, Section 1030 limits damages to "economic damages." 18 U.S.C. § 1030(g).

Under the Act, a "protected computer" is defined, in relevant part, as a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). While authorization is not defined, "exceeds authorized access" is defined as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). "Loss" is defined 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." 18 U.S.C. § 1030(e)(11). Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

Plaintiff's allegation that its servers are engaged in internet commerce sufficiently establishes that they are "protected computers" within the meaning of the Act. FAC ¶ 65.

With respect to unauthorized access, Plaintiff alleges that Defendant "abused its access to LivePerson's back-end systems to observe, penetrate, and manipulate the operations of LivePerson's servers." FAC ¶ 37. As Defendant correctly notes, there is some uncertainty on the question of whether a user who is authorized to access a computer and abuses that privilege to the detriment of the computer-owner is "exceeding [the user's] authorized access" within the meaning of the Act. See Def.'s Mem. in Supp. 9-10 citing, JBC Holdings NY, LLC v. Pakter, 931 F. Supp. 2d 514, 522 (S.D.N.Y. 2013).

As the Honorable Paul A. Engelmayer explained in JBC, the Second Circuit has not ruled on this issue and other Circuits are split. 931 F. Supp. 2d at 521-22. The First,

Fifth, Seventh and Eleventh Circuits held that a defendant that misuses information to which he was given access constitutes exceeding authorized access within the meaning of the Act, what Judge Engelmayer termed the "broad" approach. Id. By contrast, the Fourth and Ninth Circuits held that that misuse of information alone is insufficient to establish that a defendant exceeded his authorized access, what Judge Engelmayer termed the "narrow" approach. Id.

Different district courts within this Circuit have likewise come to divergent conclusions on the question of how broadly to interpret the term "exceeds authorized access." Id. ("Compare United States v. Aleynikov, 737 F.Supp.2d 173, 190-94 (S.D.N.Y.2010) (Cote, J.) (taking the narrow approach, and stating that "[t]he phrases 'accesses a computer without authorization' and 'exceeds authorized access' cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access. What use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place."), Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ. 9505 (ALC) (DCF), 2013 WL 410873, at *7 (S.D.N.Y. Jan. 30, 2013) (Carter, J.) (narrow approach), Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F.Supp.2d 378, 383-84 (S.D.N.Y.2010)

(Holwell, J.) (narrow approach), and Orbit One Commc'ns., Inc. v. Numerex Corp., 692 F.Supp.2d 373, 384-86 (S.D.N.Y.2010) (Kaplan, J.) (narrow approach), with Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LLM), 2010 WL 2034404, at *7 (S.D.N.Y. May 18, 2010) (McKenna, J.) (broad approach), Calyon v. Mizuho Secs. USA, Inc., No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007) (Owen, J.) (broad approach), and Register.com, Inc. v. Verio, Inc., 126 F.Supp.2d 238, 253 (S.D.N.Y.2000) (Jones, J.) (broad approach)").

This Court joins the majority in this district in adopting the "narrow" approach, for the reasons more extensively articulated in JBC. See generally, 931 F. Supp. 2d at 522-25. Briefly, the narrow approach grounds the definition in access rather than use, and avoids adding "a subjective intent requirement that Congress did not impose" to the Act. Id. The narrow approach is also in harmony with the type of "loss" against which the Act protects, since the Second Circuit made clear that the Act does not recognize losses related to misappropriation of information. Id. citing Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 563 (2d Cir. 2006) (affirmed the district court's reading of this provision to exclude losses incurred as a result of plaintiff's misappropriation of proprietary information). Finally, "lenity

requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them," and the narrow approach conforms to this rule. JBC, 931 F. Supp. 2d at 524 quoting Jones v. United States, 529 U.S. 848, 858 (2000).

In sum, a defendant "exceeds authorized access" as defined by Section 1030(e)(6) "when he has permission to access certain information on a computer, but accesses other information as to which he lacks permission." JBC, 931 F. Supp. 2d at 523.

Applied to this case, the Complaint does not adequately allege that Defendant exceeded its authorized access with respect to Plaintiff's computer system. Plaintiff's allegations focus primarily on Defendant's misuse of data obtained through authorized access. See, e.g., FAC ¶ 37 (alleging that "[24]7 enjoys the client's access to LivePerson's back end systems . . . and . . . abused its access"); FAC ¶ 39 (same); FAC ¶ 41 (alleging that Defendant mimicked Plaintiff in order to "hijack[] LivePerson's programming . . . secretly . . . inject[ing] millions of tracking and indexing numbers into LivePerson's systems"); FAC ¶ 47 (alleging that "the MSA and Co-Marketing Agreement put strict protections in place to prevent 24/7 from using its access to LivePerson's intellectual property

for any purpose other than the mutually beneficial activities of the parties . . . [and] access to LivePerson's technology was never provided for the purpose of allowing or assisting 24/7 to create competing technology"); FAC ¶ 48 (same). Other allegations of Defendant's purported abuses of the Plaintiff's systems do not discuss the means by which Defendants allegedly gained access to those systems and so cannot be construed as establishing that Defendant either lacked or exceeded its authorization within the meaning of the CFAA. See, e.g., FAC ¶ 40 (alleging that Plaintiff discovered "[24]/7 programming code embedded on client websites that is clearly designed to siphon data regarding the operation and activity of LivePerson's proprietary behavioral analytics and predictive targeting functionalities - and then stream this information back to [24]7's servers"); FAC ¶ 43 (alleging that "LivePerson also has discovered evidence that 24/7 has abused its access to client websites and to LivePerson systems" in order to disrupt Plaintiff's systems and harm its relations with its customers).

In addition to inadequately pleading the authorization element of the CFAA claim, Plaintiff also fails to adequately allege economic damage as required under the Act. To state a private claim under the CFAA, a plaintiff must plead damage or loss in excess of $5,000. See 18 U.S.C. § 1030(g); Nexans Wires

S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004) aff'd, 166 F. App'x 559 (2d Cir. 2006). Loss is defined 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." 18 U.S.C. § 1030(e)(11). Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Both loss and damage must relate to the victim's computer systems. Nexans, 319 F. Supp. 2d at 477; Civic Center Motors, Ltd. v. Mason Street Imported Cars, Ltd., 387 F.Supp.2d 378, 381 (S.D.N.Y. 2005).

Plaintiff alleges that Defendant's "wrongful conduct . . . endangered LivePerson's relationships with several major clients . . . and harmed LivePerson financially in an amount well in excess of the diversity jurisdictional threshold of $75,000." FAC ¶ 51. Specifically in support of its CFAA claim, Plaintiff further alleges that it suffered "disruption of its business relationships and the loss of clients and potential clients, dilution of good will, injury to its reputation, misappropriation of its intellectual property, and devaluation

of its live-interaction and analytic technology and its trade secrets." FAC ¶ 67. Neither of these allegations are sufficient. The former does not specify what portion of the over $75,000 in damages constitute either loss or damage under the Act, i.e., whether $5,000 or more of the damages alleged are attributable to the CFAA claim. The latter CFAA-specific allegation does not quantify the loss it alleges and therefore also does not satisfy the $5,000 threshold requirement. Plaintiff's CFAA claim is therefore inadequately pled.

The Misappropriation of Trade Secrets Claim Is Adequately Pled

Defendant contends that Plaintiff fails to state a claim for misappropriation of trade secrets, both because the FAC does not establish the elements of a trade secret and because Plaintiff's allegations do not establish misappropriation. See Def.'s Mem. in Supp. 11.

The parties agree on the applicable standard. Def.'s Mem. in Supp. 11; Pl.'s Mem in Opp'n 11. To state a claim for trade secret misappropriation under New York law, Plaintiff must plead that (1) it possessed a trade secret, and (2) defendant is using that trade secret in breach of an agreement, confidence, or duty, or as a result of discovery by improper means.

Geritrex Corp. v. Dermarite Indus., LLC, 910 F. Supp. 955, 961 (S.D.N.Y. 1996).

To determine whether information qualifies as a trade secret, New York courts generally consider six factors: "(1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the information; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. N. Atl. Instruments, Inc. v. Haber, 188 F.3d 38, 44 (2d Cir. 1999). These factors are guideposts, not elements, and it is not necessary to plead every single factor to state a claim, and "the most important consideration is whether the information is actually a secret." See Jinno Int'l Co. v. Premier Fabrics, Inc., 12-cv-07820, 2013 WL 4780049, at *4 (S.D.N.Y. May 24, 2013) (citing Lehman v. Dow Jones & Co., 783 F.2d 285, 298 (2d Cir. 1986)).

Plaintiff alleges that its "predictive algorithms" and "proprietary behavioral analysis methods" based on "many years'

of research undertaken at great expense" constituted a trade secret. FAC ¶¶ 1-2. These algorithms and methods "allow LivePerson to understand when a website visitor needs help, and what type of help or content will benefit that visitor at any given moment" based on "sophisticated analysis of website visitors' actions and behaviors online, both individually and in the aggregate." FAC ¶¶ 17-18. The methods are based on "identifying key actions or 'events' that take place during one or more web browsing sessions, and applying artificial intelligence to determine whether, when, and how to initiate a personalized interactive experience to assist that web visitor." FAC ¶ 19. And Plaintiff claims that "[these technologies] are secured by patents, copyrights, trademarks, trade dress and other trade secret protections," and that Plaintiff included confidentiality provisions and prohibitions against reverse engineering, infringing, or disrupting LivePerson's technology in its direct contracts with [24]7, as well as confidentiality and limited-use license restrictions in its client agreements, to which [24]7 is subject as one of the clients' vendors. FAC ¶¶ 2, 26, 28-29, 32-33. Finally, Plaintiff alleges that Defendant could not have replicated Plaintiff's technology without incurring "millions of dollars in research and development costs and many years' worth of effort and investment." FAC ¶ 8.

Plaintiff has adequately alleged that its technology was contractually protected from dissemination, was the result of Plaintiff's significant investment of both time and money, and could not have been developed independently by Defendant without a similarly substantial investment. Plaintiff's use of contractual provisions in contracts with Defendant and with clients indicate the confidential nature of its technology. See Jinno, 2013 WL 4780049, at *5. Plaintiff has also alleged that Defendant misappropriated the trade secret by accessing Plaintiff's backend system in order to "reverse engineer and copy" the technology. FAC ¶ 37. These allegations are sufficient to plead possession and misappropriation of a trade secret.

The Breach of Contract Claim Is Adequately Pled

To state a claim for a breach of contract under New York law, Plaintiff must plead plausible facts regarding: (1) the existence of a contract; (2) performance of the plaintiff's obligations; (3) breach by the defendant; and (4) damages to the plaintiff caused by the breach. Diesel Props S.r.l. v. Greystone Bus. Credit II LLC, 631 F.3d 42, 52 (2d Cir. 2011). Defendant contends Plaintiff has not satisfied the first, third or fourth elements. Def.'s Mem. in Supp't 14-16.

With respect to existence of a contract, Defendant contends that Plaintiff must identify the dates of any wrongful act by Defendants to satisfy by this element, but do not provide case law to substantiate this assertion. See Def.'s Mem. in Supp't 15. Plaintiff has adequately pled existence of two contracts: the MSA and the Co-Marketing Agreement. FAC ¶¶ 25, 27. Plaintiff has also attached copies of those agreements as Exhibits A & B to FAC. Defendants have admitted to the existence of the agreements. See Def.s' Mem. in Supp't 14, fn. 2. The existence of the contracts is therefore established.

With respect to Defendant's breach, Plaintiff adequately identifies the relevant contractual provisions and by what alleged actions Defendant violated those provisions. FAC ¶¶ 35-49, 76-77. Plaintiff alleges that Defendant misused its technology in violation of several contractual provisions limiting its usage of Plaintiff's programs, and further breached its contracts with Plaintiff by introducing malicious software code into its programs. FAC ¶ 77. Thus, and in contrast to Defendant's contention, the FAC's allegations distinguish between behavior permissible under the contracts and behavior that constitutes breach. See Def.'s Mem. in Supp't 15. Moreover, Defendant is mistaken in its contention that that the contracts required Plaintiff to provide Defendant with an

opportunity to cure a breach prior to suit. See Def.'s Mem. in Supp't 15-16. In fact, the provisions which Defendant cites govern a non-breaching party's right to terminate upon breach, but do not limit a non-breaching party's right to sue for breach. See MSA ¶ 11(a)(5); CMA ¶ 2.5.

With respect to damages, Plaintiff alleged that it has "lost or been notified of cancellation by major clients expressly due to 24/7's improper conduct" and that it "also has been informed by several clients that 24/7 actively is disparaging LivePerson's technology and services based on misrepresentation and misuse of LivePerson's confidential data, which 24/7 is not authorized to use for competitive purposes." FAC ¶ 50. Plaintiff further alleges that the damages resulting from Defendant's conduct exceed $75,000. FAC ¶ 67. While Plaintiff does not itemize the client relationships harmed and does not estimate damages beyond the assertion that they are substantially greater than the federal amount-in-controversy requirement, the FAC provides adequate notice to Defendant on the issue of damages. See Xpedior Creditor Trust v. Credit Suisse First Boston (USA) Inc., 341 F. Supp. 2d 258, 272 (S.D.N.Y. 2004) (Under Rule 8(a), [the plaintiff] need only allege that it was damaged; it is not required to specify the measure of damages nor to plead proof of causation."); U.S.

Network Servs., Inc. v. Frontier Commc'ns of W., Inc., 115 F. Supp. 2d 353, 358 (W.D.N.Y. 2000). Defendant's reference to Jinno does not alter this conclusion, as the dismissed claim in that case only stated that the counterclaimant "suffered damages in a sum to be determined at trial." 2013 WL 4780049, at *3. By contrast, Plaintiff here stated that damage exceeded $75,000 and impacted numerous client relationships, allegations that provide Defendant with adequate notice of the breach of contract claim. The elements of this claim are adequately pled.

The Claims for Intentional Interference with Prospective and Existing Economic Relationships Are In Part Adequately Pled

A claim for intentional interference with an existing or prospective economic relationship requires the pleading of facts giving rise to a plausible inference that: (1) the plaintiff had an existing or prospective business relationship with a third party; (2) the defendant knew of that relationship and intentionally interfered with it; (3) the defendant acted solely out of malice, or used dishonest, unfair, or improper means; and (4) the defendant's interference caused injury to the relationship. Kirch v. Liberty Media Corp., 449 F.3d 388, 400 (2d Cir. 2006)); Camp Summit of Summitville, Inc. v. Visinsk, 06-cv-4994, 2007 WL 1152894, at *14 (S.D.N.Y. Apr. 16, 2007).

Plaintiff has adequately alleged the existence of business relationships and Defendant's knowledge regarding those relationships. Contrary to Defendant's contention that Plaintiff failed to mention affected clients, the Complaint specifically references Plaintiff's client list attached to the Complaint in Exhibit A, alleging that Defendant "interfered with and continues to interfere with . . . these clients," and that Defendant was aware of those relationships as they were part of the CMA which Defendant signed. Compare Def.'s Mem in Supp't 18-19 with FAC ¶¶ 81-82, 91.

Plaintiff also adequately alleged improper interference. See FAC ¶ 34; see also FAC ¶¶ 36, 37, 81. Plaintiff alleged that Defendant "provided inaccurate business performance data regarding LivePerson to LivePerson's clients, which (a) could not be produced without accessing LivePerson's confidential system data; and (b) differs significantly from LivePerson's business performance data shown when LivePerson technology is used by any of a dozen or so other outsourced call-center labor providers and/or client call-center employees." FAC ¶¶ 38, 83. Plaintiff also allegedly found "24/7 programming code expressly designed to suppress the proper operation of LivePerson's technology, such as preventing livechat sessions from being initiated, and/or eliminating

LivePerson's "chat" button from appearing altogether" on its clients' websites. FAC ¶¶ 44, 83. This conduct, assumed true for the purposes of this motion, is sufficient to constitute improper interference. Carvel Corp. v. Noonan, 3 N.Y.3d 182, 190-91 (N.Y. 2004) (explaining that competitors are barred from engaging in "wrongful" means of interference, defined to include "physical violence, fraud or misrepresentation, civil suits and criminal prosecutions," or where the defendant is accused of engaging in "conduct [that] was criminal or independently tortious"); see also N. State Autobahn, Inc. v. Progressive Ins. Grp., 928 N.Y.S.2d 199, 206-07 (N.Y. Sup. Ct. 2011) (denying summary judgment where defendant allegedly used "deceptive, misleading and untrue statements which disparaged plaintiff" to divert business), aff'd as modified 953 N.Y.S.2d 96 (App. Div. 2012); DiCosomo v. Getzoff, 11 Misc. 3d 1063(A), 816 N.Y.S.2d 695, at *5-6 (N.Y. Sup. Ct. Apr. 8, 2004) (denying motion to dismiss where plaintiff pled "the making of false and misleading statements and [the conduct of] an anonymous and malicious smear campaign").

With respect to injury, Plaintiff adequately alleged that "several of LivePerson's major clients have cancelled or notified LivePerson that they intend to cancel their relationship with LivePerson" as a result of the interference.

FAC ¶ 87.

By contrast, the portion of the FAC referencing interference with Plaintiff's employees is not adequately pled. Plaintiff did not allege that its employees were subject to covenants not to compete, and failed to meet the "high burden of asserting that defendant employed wrongful means, such as fraud, misrepresentation or threats to effect the termination of employment." Lockheed Martin Corp. v. Aatlas Commerce Inc., 283 A.D.2d 801, 803, 725 N.Y.S.2d 722 (App. Div. 2001) (internal quotations and citations omitted). The allegations with respect to employees are limited to one paragraph alleging that Defendant engaged in a "pattern of deliberate corporate raiding of employees, up to and including entire business teams to leave LivePerson for employment with 24/7." FAC ¶ 84. This does not establish the "wrongful means" required to make this claim.

The Lanham Act Claim is Adequately Pled

False advertising claims under the Lanham Act require allegations that the defendant: (1) made material misrepresentations about the nature, characteristics, or geographic origin of either the plaintiff's or defendant's goods and services; (2) used the false or misleading representations

in commerce; (3) made the representations in the context of commercial advertising or promotion; and (4) made the plaintiff believe he is likely to be damaged by the misrepresentation. Randa Corp. v. Mulberry Thai Silks, Inc., 00-cv-4061, 2000 WL 1741680, at *2 (S.D.N.Y. Nov. 22, 2000); see also 28 U.S.C. § 1125(a); FAC ¶ 99.

Plaintiff contends that Defendant "falsely claim[ed] to have developed the 'first' predictive or smart chat platform," when in fact Plaintiff did, which resulted in damage in the form of "loss of clients and potential clients, dilution of good will, injury to its reputation, misappropriation of its intellectual property, and devaluation of its live-interaction and predictive analytics technology and its trade secrets." FAC ¶ 98.

Plaintiff has not provided the context for the allegedly false advertisement, making it difficult to evaluate the "entire mosaic" of the advertisement rather than "each tile separately," as the Second Circuit instructs. See Vidal Sassoon v. Bristol-Myers Co., 661 F.2d 272, 276 (2d Cir. 1981) quoting FTC v. Sterling Drug, Inc., 317 F.2d 669, 674 (2d Cir. 1963). As Defendant correctly notes, "context may establish that the statement was true, such as if [24]7 was promoting innovative

features unique to [24]7's technology." Def.'s Mem. in Supp't 20-21 (citing Data Cash Sys., Inc. v. JS&A Grp., Inc., No. 79 C 0591, 1984 U.S. Dist. LEXIS 18446, at *7-8 (N.D. Ill. Mar. 20, 1984) (in case brought under Lanham Act, defendant's claim that its computerized chess program was "a new product" "is technically true, i.e., [the product] was a new product for [the defendant]. It marked [the defendant's] entry into the computer chess field.")).

The 'first' claim may prove to be immaterial puffery, considering the sophistication of the clients in this industry and the unlikelihood that claims of developing the 'first' such software would influence their purchasing decisions. See Allen Organ Co. v. Galanti Organ Builders, Inc., 798 F. Supp. 1162, 1169-70 (E.D. Pa. 1992) (any false advertisement of church organs did not tend to deceive intended audience and were not material; organ market was "unlike that of a mass market for a consumer item purchased off the shelf, such as dog food or orange juice, where the advertisement alone may sell the product"); Data Cash Sys., Inc. v. Js&a Grp., Inc., No. 79 C 0591, 1984 WL 63623, at *3 (N.D. Ill. Mar. 20, 1984) (rejecting Lanham Act claim because advertisement stating that a computer chess game was a "new product" and "new technology" was "puffing" and there was only de minimis likelihood of deception

of readers of advertisements in trade journals, who were somewhat sophisticated about the technology); but see Basile Baumann Prost Cole & Assocs., Inc. v. BBP & Assocs. LLC et al., 875 F. Supp. 2d 511, 522, 530 (D. Md. 2012).

Since "materiality is generally a question of fact" poorly suited to a determination at the pleadings stage, this claim is not dismissed. See id. at 530. Plaintiff is instead directed to provide, pursuant to Rule 12(e) of the Federal Rules of Civil Procedure, a more definite statement regarding the context and materiality of Defendant's alleged false advertisement and how the advertisement damaged Plaintiff.

The Common Law Unfair Competition Claim is Adequately Pled

A claim for unfair competition requires the pleading of facts giving rise to a plausible inference that the defendant, acting in bad faith, misappropriated the plaintiff's labor and expenditures to gain a commercial advantage or maliciously interfered with the plaintiff's good will. See Kwan v Schlein, 441 F. Supp. 2d 491, 502-03 (S.D.N.Y. 2006). "As numerous courts have noted, the scope of the unfair competition action is generally limited to three categories: passing off one's goods as those of another, engaging in activities solely

to destroy a rival, and using methods themselves independently illegal." Coca-Cola N. Am. v. Crawley Juice, Inc., 09-cv-3259, 2011 WL 1882845, at *7 (E.D.N.Y. May 17, 2011) (internal quotations and citations omitted).

Plaintiff has adequately alleged that Defendant embedding spyware code on LivePerson's clients' websites to reverse engineer LivePerson's proprietary behavioral analytics and predictive targeting functionalities, injecting tracking markers into LivePerson's systems to facilitate unauthorized data mining, manipulating LivePerson's software on client deployments to reduce its performance, and deploying software code designed to suppress the proper operation of LivePerson's technology. See FAC ¶¶ 37-44. This conduct, if true, would either be independently illegal or would constitute Defendant passing off Plaintiff's product as its own. Common law unfair competition is therefore adequately pled.

The Unjust Enrichment Claim is Adequately Pled

To plead unjust enrichment, New York law requires that (1) the defendant benefitted; (2) at the plaintiff's expense; and (3) equity and good conscience require restitution. Beth Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of N.J.,

Inc., 448 F.3d 573, 586 (2d Cir. 2006). Such a claim may be pled as an alternative to a breach of contract claim. Singer v. Xipto Inc., 852 F. Supp. 2d 416, 426 (S.D.N.Y. Mar. 20, 2012) ("While a party generally may not simultaneously recover upon a breach of contract and unjust enrichment claim arising from the same facts, it is still permissible to plead such claims as alternative theories.").

FAC alleges that Defendant improperly obtained Plaintiff's intellectual property and confidential information and used them to develop a competing product. FAC ¶¶ 35-44. The FAC further alleges that Defendant's conduct caused Plaintiff's clients to terminate their dealings with Plaintiff in favor of Defendant. A claim for unjust enrichment is established.

Conclusion

For the reasons set out above, Defendant's motion is granted in part and denied in part. With respect the claims and portions of claims held to be inadequately pled, Plaintiff may replead within twenty days of the date of this opinion. With respect to the Lanham Act claim, Plaintiff shall provide a more definite statement as outlined above within twenty days of the date of this opinion.

It is so ordered.

New York, NY
January 15, 2015

ROBERT W. SWEET
U.S.D.J.