

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

SATMODO, LLC, a California limited liability company,  
  
Plaintiff,  
  
v.  
  
WHENEVER COMMUNICATIONS, LLC, d.b.a. StatellitePhoneStore.com, a Nevada limited liability company, HENAA BLANCO, an individual, and DOES 1 through 50, inclusive,  
  
Defendants.

Case No.: 17-cv-0192-AJB NLS

**ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS’ MOTION TO DISMISS**

Presently before the Court is Defendants’ Whenever Communications, LLC, d.b.a. StatellitePhoneStore.com and Henea Blanco, (collectively “Defendants”), motion to dismiss Plaintiff’s Satmodo, LLC, (“Plaintiff”) complaint. (Doc. No. 9.) Having reviewed the parties’ arguments and controlling legal authority, the Court finds this motion suitable for determination on the papers and without oral argument. Accordingly, the motion hearing presently set for April 20, 2017 at 2:00 p.m. is **VACATED** pursuant to Local Rule 7.1.d.1. For the reasons set forth below, the Court **GRANTS IN PART AND DENIES IN PART** Defendants’ motion to dismiss.

//

1 **BACKGROUND**

2 The following facts are taken from Plaintiff’s complaint and accepted as true for the  
3 limited purpose of resolving the pending motion before the Court. *See Vasquez v. L.A.*  
4 *Cnty.*, 487 F.3d 1246, 1249 (9th Cir. 2007) (noting a court must “accept all material  
5 allegations of fact as true” when ruling on a motion to dismiss).

6 The present action arises out of an intentional and systematic “click fraud” scheme,  
7 wherein Defendants clicked on Plaintiff’s paid online advertisements with the intent to  
8 harm Plaintiff. (Doc. No. 1 ¶ 9.) Plaintiff and Defendant Whenever Communications are  
9 two of the largest competitors in the business of online sale and rental of satellite phones.  
10 (*Id.* ¶ 12.) These companies buy satellite phones at wholesale and then sell or rent the  
11 phones to online customers. (*Id.*) Within this industry, sales and rentals are heavily reliant  
12 on a company’s online presence. (*Id.* ¶ 14.) To promote their online presence, competing  
13 companies, including Plaintiff and Defendant Whenever Communications, take part in  
14 advertisements via search engines. (*Id.*) Each time a customer clicks on a company’s  
15 advertisement through a search engine, the company pays for the click through a set daily  
16 advertising budget. (*Id.* ¶ 9.) Once a company’s set daily advertising budget has been met,  
17 the search engine will stop publishing the company’s advertisement for that day. (*Id.*)

18 From 2016 to 2017, Defendant Whenever Communications, in part through its agent  
19 Defendant Henna Blanco, intentionally sought out Plaintiff’s advertisements on search  
20 engines including Google, Yahoo!, and Bing, to carry out their “click fraud” scheme. (*Id.*  
21 ¶¶ 9-11, 20.) “Click fraud” is the practice of fraudulently or maliciously clicking the online  
22 search advertisements of an advertiser to force the advertiser to pay for the click while  
23 having no intention of buying the advertised services or products. (*Id.* ¶ 10.) Defendants  
24 intentionally clicked on Plaintiff’s advertisements to push Plaintiff out of the market and  
25 to receive a better advertising rank over Plaintiff. (*Id.* ¶¶ 18-19.) Plaintiff observed the use  
26 of multiple IP addresses used to commit this click fraud scheme and believes the addresses  
27 were tied to Defendants. (*Id.* ¶¶ 25, 28, 31.) Plaintiff believes that Defendants are utilizing  
28 automated means and rotating through proxy servers in order to avoid detection. (*Id.* ¶ 27.)

1 Specifically, on August 22, 2016, Plaintiff observed Defendants use automated means to  
2 click on Plaintiff's homepage approximately 96 times within a few minutes. (*Id.* ¶¶ 25-27.)  
3 At times where the IP addresses were unmasked by proxy servers, Plaintiff observed  
4 fraudulent clicks and chat requests originating from Lakeland, Florida, Las Vegas, Nevada,  
5 and San Diego, California, which are all locations where Whenever Communications  
6 maintains offices. (*Id.* ¶ 31.) In response to these observations, Plaintiff blocked several IP  
7 addresses associated with Defendants. (*Id.* ¶ 29.) In September 2016, Plaintiff's counsel  
8 sent a cease and desist letter to Defendants and asked Defendants to stop their click fraud  
9 scheme. (*Id.* ¶ 32.) However, instead of ceasing, Defendants used proxy servers to  
10 circumvent Plaintiff's online blockade and continued to engage in their click fraud scheme.  
11 (*Id.* ¶¶ 29, 32.) Plaintiff alleges it has been damaged in that it paid for clicks that Defendants  
12 fraudulently created and lost sales from being forced out of the market prematurely. (*Id.* ¶  
13 34.)

14 On February 1, 2017, Plaintiff filed a complaint seeking compensatory damages and  
15 injunctive relief for Defendants' alleged click fraud scheme. (Doc. No. 1.) Plaintiff alleged  
16 four causes of actions in its complaint: (1) violation of the Computer Fraud and Abuse Act  
17 ("CFAA"); (2) violation of California's Comprehensive Computer Data Access and Fraud  
18 Act ("CDAFA"); (3) intentional interference with prospective economic relations; and (4)  
19 violation of California's Unfair Competition Law, Business and Professions Code Section  
20 17200 ("UCL"). Presently before the Court is Defendants' amended motion to dismiss,  
21 which was filed on February 27, 2017. (Doc. No. 9.) Plaintiff filed an opposition on March  
22 10, 2017, (Doc. No. 10), and Defendants replied on March 16, 2017, (Doc. No. 12).

### 23 **LEGAL STANDARD**

24 A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) tests the legal  
25 sufficiency of a plaintiff's complaint and allows a court to dismiss a complaint upon a  
26 finding that the plaintiff has failed to state a claim upon which relief may be granted. *See*  
27 *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). "[A] court may dismiss a complaint  
28 as a matter of law for (1) lack of a cognizable legal theory or (2) insufficient facts under a

1 cognizable legal claim.” *SmileCare Dental Grp. v. Delta Dental Plan of Cal., Inc.*, 88 F.3d  
2 780, 783 (9th Cir. 1996) (internal quotations and citation omitted). However, a complaint  
3 will survive a motion to dismiss if it contains “enough facts to state a claim to relief that is  
4 plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In making this  
5 determination, a court reviews the contents of the complaint, accepting all factual  
6 allegations as true, and drawing all reasonable inferences in favor of the nonmoving party.  
7 *Cedars-Sinai Med. Ctr. v. Nat’l League of Postmasters of U.S.*, 497 F.3d 972, 975 (9th Cir.  
8 2007).

9 Notwithstanding this deference, the reviewing court need not accept “legal  
10 conclusions” as true. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). It is also improper for a  
11 court to assume “the [plaintiff] can prove facts that [he or she] has not alleged.” *Associated*  
12 *Gen. Contractors of Cal., Inc. v. Cal. State Council of Carpenters*, 459 U.S. 519, 526  
13 (1983). However, “[w]hen there are well-pleaded factual allegations, a court should assume  
14 their veracity and then determine whether they plausibly give rise to an entitlement to  
15 relief.” *Iqbal*, 556 U.S. at 679.

16 Further, factual allegations must meet the requisite level of specificity. *See Kearns*  
17 *v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009). Federal Rule of Civil Procedure  
18 8(a)(2) requires a party's pleading to contain “a short and plain statement of the claim  
19 showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). However, Rule 9(b)  
20 requires that, when fraud is alleged, “a party must state with particularity the circumstances  
21 constituting fraud . . . .” Fed. R. Civ. P. 9(b). When fraud is not a necessary element of a  
22 claim, a plaintiff may choose to allege a unified course of fraudulent conduct and rely  
23 entirely on that course of conduct as the basis of a claim. *Vess v. Ciba-Geigy Corp. USA*,  
24 317 F.3d 1097, 1103 (9th Cir. 2003). In such event, “the claim is said to be ‘grounded in  
25 fraud’ or to ‘sound in fraud,’ and the pleading of that claim as a whole must satisfy the  
26 particularity requirement of Rule 9(b).” *Id.* at 1103–04. Rule 9(b) demands that the  
27 circumstances constituting the alleged fraud “be ‘specific enough to give defendants notice  
28 of the particular misconduct . . . so that they can defend against the charge and not just

1 deny that they have done anything wrong.’’ *Bly–Magee v. California*, 236 F.3d 1014, 1019  
2 (9th Cir. 2001) (quoting *Neubronner v. Milken*, 6 F.3d 666, 672 (9th Cir. 1993)).

### 3 DISCUSSION

#### 4 **A. Rule 9(b) Heightened Pleading Standard**

5 As a preliminary matter, the Court will address to what extent Plaintiff’s claims are  
6 subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b).  
7 Defendants contend that all of Plaintiff’s claims are subject to Rule 9(b) because each claim  
8 is based upon a fraudulent course of conduct. (Doc. No. 9 at 11-12, 14, 16, 18.) Plaintiff  
9 counters that only specific averments of fraud must be pled with particularity and that, even  
10 if the Court disagrees, the complaint meets the heightened pleading standard. (Doc. No. 10  
11 at 15-18, 19-20, 21, 23.) The Court finds that each of Plaintiff’s claims are subject to the  
12 Rule 9(b) pleading standard.

13 Each of Plaintiff’s claims against Defendants arise from the alleged click fraud  
14 scheme. (*See generally* Doc. No. 1.) Plaintiff defines click fraud as “generating clicks with  
15 a fraudulent or malicious intent . . . despite the fact that the person or entity making the  
16 click has no intention of buying the advertised services or products.” (Doc. No. 1 ¶ 10.)  
17 Moreover, when Plaintiff alleges how Defendants implemented the scheme, it explains that  
18 “Defendants intentionally sought out Plaintiff’s ads, clicking on them to present the false  
19 impression that they were intended customers.” (Doc. No. 1 ¶ 19.) Plaintiff makes these  
20 allegations in support of its CFAA, CDAFA, UCL, and intentional interference with  
21 prospective economic relations claims; thus, it follows that all claims rely on a unified  
22 fraudulent course of conduct. *See Kearns*, 567 F.3d at 1125–26.

23 Therefore, the Court finds that Plaintiff’s complaint alleges a unified course of  
24 fraudulent conduct.

#### 25 **B. Computer Fraud and Abuse Act**

26 Plaintiff alleges Defendants violated four subsections of the CFAA, sections  
27 1030(a)(4) and (5)(A)-(C), when they accessed Plaintiff’s computers without authorization  
28 by logging onto the search engine website and making fraudulent clicks, or alternatively,

1 when they exceeded their authorized access after being put on notice of their wrongful  
2 conduct in September 2016. (Doc. No. 1 ¶¶ 37, 39.) Plaintiff alleges damages and economic  
3 loss exceeding \$75,000 based on the costs incurred in paying for invalid clicks and the loss  
4 of sales and profits from those clicks after Plaintiff was prematurely kicked out of the  
5 market. (*Id.* ¶ 39(d).) Defendants argue for dismissal because the alleged conduct does not  
6 conform to the criminal “anti-hacking” conduct that the CFAA was designed to prevent.  
7 Specifically, Defendants contend that each of Plaintiff’s claims must fail because Plaintiff  
8 (1) has not shown how accessing Plaintiff’s website through a publicly available third-  
9 party search engine is a recognized violation under the CFAA, (2) has not alleged sufficient  
10 facts for the requirement of loss or damage, and (3) fails to comply with Rule 9(b). (Doc.  
11 No. 9 at 8-12.) As explained below, the Court agrees with Defendants and will address  
12 each contention below.

13         The CFAA was first enacted to enhance the government's ability to prosecute  
14 computer crimes and to "target hackers who accessed computers to steal information or to  
15 disrupt or destroy computer functionality, as well as criminals who possessed the capacity  
16 to access and control high technology processes vital to our everyday lives." *LVRC*  
17 *Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009) (internal quotation marks  
18 and citation omitted). “The CFAA prohibits a number of different computer crimes, the  
19 majority of which involve accessing computers without authorization or excess of  
20 authorization, and then taking specific forbidden actions, ranging from obtaining  
21 information to damaging a computer or computer data.” *Id.* at 1131. Any individual may  
22 bring a private civil cause of action under the CFAA for damages and equitable relief if he  
23 or she suffers damages or loss as a result of a violation of these provisions. 18 U.S.C. §  
24 1030(g). Within this context, the statute “targets the unauthorized procurement or alteration  
25 of information, not its misuse or misappropriation.” *United States v. Nosal*, 676 F.3d 854,  
26 863–64 (9th Cir. 2012) (interpreting the phrase “exceeds authorized access” to apply to  
27 “violations of restrictions on *access* to information, and not restrictions on its *use*.”)  
28 (emphasis in original).

1                                   **1. Section 1030(a)(4)**

2           To establish a violation under section 1030(a)(4), Plaintiff must allege Defendants  
3 (1) accessed a “protected computer,” (2) without authorization or exceeding authorization  
4 that was granted, (3) “knowingly” and with “intent to defraud,” and thereby (4) “further[ed]  
5 the intended fraud and obtain[ed] anything of value,” causing (5) a loss to one or more  
6 persons during any one-year period aggregating at least \$5,000 in value. *Brekka*, 581 F.3d  
7 at 1132. Plaintiff alleges Defendants accessed its protected computers by “logging onto the  
8 search engine website in which Plaintiff used to facilitate its business and violated the terms  
9 and conditions of the search engine advertising contracts by producing invalid clicks on  
10 Plaintiff’s advertisements.” (Doc. No. 1 ¶ 37.) As currently pled, Plaintiff has not provided  
11 sufficient facts to demonstrate the threshold element that Defendants accessed Plaintiff’s  
12 computers under section 1030(a)(4).<sup>1 2</sup> *Cf. Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d  
13 962, 968 (N.D. Cal. 2013) (holding plaintiff alleged “access of a protected computer”  
14 where it alleged “[d]efendants accessed Craigslist’s website and the ‘protected computers’  
15 hosting the website”).

16           Defendants’ main contention is whether Plaintiff has sufficiently alleged that  
17 Defendants improperly accessed Plaintiff’s computers without authorization or by  
18 exceeding authorization. The Court finds that Plaintiff has sufficiently pled this element.  
19 The CFAA “provides two ways of committing the crime of improperly accessing a  
20 protected computer: (1) obtaining access without authorization; and (2) obtaining access  
21 with authorization but then using that access improperly.” *Facebook, Inc. v. Power*  
22

---

23  
24 <sup>1</sup> The Court notes that Plaintiff’s opposition explains that clicking on the advertisements  
25 on the search engines resulted in Defendants being redirected to Plaintiff’s website, servers,  
26 and computers. (See Doc. No. 10 at 11.) However, Plaintiff fails to allege this information  
27 in its complaint. See *Associated Gen. Contractors of Cal. Inc.*, 459 U.S. at 526 (discussing  
28 that because a Rule 12(b)(6) motion tests the legal sufficiency of a complaint, a plaintiff  
cannot avoid dismissal by adding information not originally alleged in the complaint).

<sup>2</sup> Accordingly, the Court finds that Plaintiff also fails to plead this element for sections  
1030(a)(5)(B)-(C).

1 *Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (quoting *Musacchio v. United States*,  
2 136 S. Ct. 709, 713 (2016)). Access without authorization under the CFAA occurs “when  
3 the person has not received permission to use the computer for any purpose (such as when  
4 a hacker accesses someone’s computer without any permission), or when the employer has  
5 rescinded permission to access the computer and the defendant uses the computer anyway.”  
6 *Brekka*, 581 F.3d at 1135. In contrast, exceeding authorized access is defined as accessing  
7 a computer with authorization and then using that access to obtain or alter information in  
8 the computer that the person is not entitled to alter or obtain. 18 U.S.C. § 1030(e)(6). The  
9 Ninth Circuit recently distilled two general rules for analyzing “authorization” under the  
10 CFAA: (1) “a defendant can run afoul of the CFAA when he or she has no permission to  
11 access a computer or when such permission has been revoked explicitly;” and (2) “a  
12 violation of the terms of use of a website—without more—cannot establish liability under  
13 the CFAA.” *Power Ventures*, 844 F.3d at 1067 (following the Court’s analysis in *Nosal*,  
14 828 F.3d 865).

15 In *Power Ventures*, the defendant initially had permission to access the plaintiff’s  
16 website. *Id.* However, plaintiff took two actions that expressly rescinded authorization:  
17 sending a cease and desist letter to the defendant and blocking the defendant's IP addresses.  
18 *Id.* The letter informed defendant that it had violated plaintiff’s terms of use, as well as  
19 federal and state law, and demanded defendant stop soliciting information, using the  
20 website’s content, or otherwise interacting with the website through automated scripts. *Id.*  
21 at 1067 n.3. While a violation, or notification of such a violation, of the website’s terms of  
22 use was not sufficient to impose liability, the content of the cease and desist letter put  
23 defendant on notice that it no longer had authorized access to plaintiff’s computers. *Id.*  
24 (citing *Nosal*, 676 F.3d at 862–63.) Plaintiff then further demonstrated that it had rescinded  
25 defendant's authorization by instituting an IP block to prevent defendant from accessing  
26 the Facebook website, which defendant circumvented by switching IP addresses. *Id.* at  
27 1063. When defendant accessed plaintiff’s website after receiving the letter, the Ninth  
28 Circuit held the access to be without authorization under the CFAA. *Id.* at 1069.



1 Here, Plaintiff asserts two theories alleging how Defendants acquired improper  
2 access: (1) violating the terms and conditions of the search engine’s advertising contracts,  
3 and (2) accessing Plaintiff’s website after Plaintiff blocked various IP addresses and asked  
4 Defendants to cease.<sup>3</sup> (Doc. No. 1 ¶¶ 29, 32.) However, a violation of a website’s terms of  
5 use, without more, is not sufficient to impose liability as a matter of law.<sup>4</sup> *See Power*  
6 *Ventures*, 844 F.3d at 1067 n.3; *Nosal*, 676 F.3d at 862–63. Regarding the second theory,  
7 Plaintiff alleges that it first blocked various IP addresses associated with Defendants and  
8 that Defendants circumvented its efforts to continue their click fraud scheme. (Doc. No. 1  
9 ¶ 29.) This allegation on its own is not sufficient to show improper access. *See Power*  
10 *Ventures*, 844 F.3d at 1068 n.5 (“Simply bypassing an IP address, without more, would not  
11 constitute unauthorized use.”). However, Plaintiff’s counsel notified Defendants in writing  
12 about their wrongful conduct and a demand was made to stop these actions immediately.  
13 (Doc. No. 1 ¶ 32.) The combination of these factual allegations is sufficient to allege  
14 improper access at the pleading stage. *See Power Ventures*, 844 F.3d at 1068; *see also*  
15 *Craigslist Inc. v. 3Taps Inc.*, 942 F. Supp. 2d 962, 969–70 (N.D. Cal. 2012) (holding  
16 defendants’ continued use of plaintiff’s website after receiving cease and desist letters and  
17 evading technological blocking measures constitutes unauthorized access). Accordingly,  
18 Plaintiff has adequately alleged that if Defendants did access its computers, such access  
19 was improper because Defendants exceeded authorization. Ultimately, however, because  
20

---

21 <sup>3</sup> Defendants contend that Plaintiff’s second theory of improper access is a new theory first  
22 introduced in Plaintiff’s opposition papers and absent from the complaint. (Doc. No. 12 at  
23 5-6.) The Court disagrees with Defendants. While Plaintiff’s opposition papers primarily  
24 focus on this second theory, the factual allegations are also pled in the complaint. (*See* Doc.  
25 No. 1 ¶¶ 29, 32.)

26 <sup>4</sup> Interestingly, the Court notes that if Plaintiff wishes to proceed on a contract-based theory,  
27 there might be an issue establishing standing without first demonstrating privity of contract.  
28 *See NovelPoster v. Javitch Canfield Grp.*, No. 13-cv-05186-WHO, 2014 WL 5687344, at  
\*5 (N.D. Cal. Nov. 4, 2014) (noting “the general rule among federal courts applying  
California law is that one who is not a party to a contract does not have standing to sue for  
breach of that contract.”).

1 Plaintiff failed to adequately plead the threshold element that Defendants accessed  
2 Plaintiff's computers, Plaintiff's claim under section 1030(a)(4) is **DISMISSED**.

3 **2. Sections 1030(a)(5)(A)-(C)**

4 Plaintiff next alleges three violations under section 1030(a)(5)(A)-(C). (Doc. No. 1  
5 ¶ 39.) Subsection A creates a cause of action against anyone who knowingly transmits a  
6 program, information, or command, intentionally causing damage without authorization.  
7 18 U.S.C. § 1030(a)(5)(A). Subsection B imposes civil liability on whoever intentionally  
8 accesses a protected computer without authorization and recklessly causes damage. 18  
9 U.S.C. § 1030(a)(5)(B). Lastly, subsection C penalizes a defendant who intentionally  
10 accesses a protected computer without authorization and causes damage and loss. 18  
11 U.S.C. § 1030(a)(5)(C). The CFAA broadly defines “loss” as “any reasonable cost to any  
12 victim, including the cost of responding to an offense, conducting a damage assessment,  
13 and restoring the data, program, system, or information to its condition prior to the offense,  
14 and any revenue lost, cost incurred, or other consequential damages incurred because of  
15 interruption of service.” 18 U.S.C. § 1030(e)(11). In contrast, “damage” is statutorily  
16 defined separately as “any impairment to the integrity or availability of data, a program, a  
17 system, or information.” 18 U.S.C. § 1030(e)(8). “Thus, while ‘damage’ covers harm to  
18 data and information, ‘loss’ refers to monetary harms sustained by the plaintiff.”  
19 *NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 961 (N.D. Cal. 2014) (citation  
20 omitted).

21 As currently pled, Plaintiff has failed to set forth facts sufficient to state a claim for  
22 relief under sections 1030(a)(5)(A)-(C). Plaintiff contends that by orchestrating the click  
23 fraud scheme, Defendants inhibited Plaintiff’s advertisements from being displayed online,  
24 essentially causing Plaintiff’s premature exclusion from the market and causing a loss of  
25 sales and profits. (Doc. No. ¶¶ 34, 39, 40.) Drawing all reasonable inferences in Plaintiff’s  
26 favor, Plaintiff has adequately pled the more loosely-interpreted element of loss.<sup>5</sup> However,  
27

---

28 <sup>5</sup> Thus, Plaintiff’s allegation of loss is also sufficient for its section 1030(a)(4) claim.

1 Plaintiff has not pled any facts sufficient to state a claim for damages based on CFFA’s  
2 statutory definition. Instead, Plaintiff pleads facts sufficient for loss and summarily labels  
3 them as “damage.” (See Doc. No. 1 ¶ 39(b)-(d).) This is insufficient. Plaintiff must allege  
4 facts that demonstrate that their data was destroyed, their computer system was harmed, or  
5 there was an inability to access their own computer data. See, e.g., *Int’l Airport Ctrs., LLC*  
6 *v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006) (harm constituted “damage” under the statute  
7 where defendant installed a secure-erasure program to prevent recovery of important files);  
8 *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 834 (N.D. Cal. 2014) (“damage”  
9 insufficiently pled where plaintiff plainly alleged “harm to the integrity of its data,  
10 programs, and computer system” without any plausible detail); *NovelPoster*, 140 F. Supp.  
11 3d at 961 (“damage” sufficient under CFAA where plaintiff alleged defendants maintained  
12 unauthorized control of plaintiff’s online accounts, which prohibited plaintiff from  
13 accessing their own data and communications within).

14 Accordingly, for the reasons stated above, Plaintiff’s claims under the CFAA are  
15 **DISMISSED.**

### 16 **C. California’s Comprehensive Computer Data Access and Fraud Act**

17 Plaintiff next alleges Defendants violated four subsections of the CDFAFA, sections  
18 502(c)(1), (3), (5), (7). (Doc. No. 1 ¶¶ 44-47.) Plaintiff’s claim under this statute arises  
19 from the same conduct alleged under the CFAA. Defendants contend that each of  
20 Plaintiff’s CDFAFA claims must fail because Plaintiff has not alleged use of its computers  
21 “without permission” and the allegations fail to comply with Rule 9(b). (Doc. No. 9 at 13-  
22 14.)

23 California Penal Code § 502 “prohibits unauthorized access to computers, computer  
24 systems, and computer networks, and provides for a civil remedy in the form of  
25 compensatory damages, injunctive relief, and other equitable relief.” *Sunbelt Rentals, Inc.*  
26 *v. Victor*, 43 F. Supp. 3d 1026, 1032 (2014). Section 502 is also considered an “anti-  
27 hacking statute intended to prohibit the unauthorized use of any computer system for  
28 improper or illegitimate purpose.” *Id.* Section 502 “is seen as the California corollary to

1 the CFAA, and the requisite elements for pleading violations of the CFAA and CCDAFA  
2 are the same.” *Lakeland Tours, LLC v. Bauman*, No. 13cv2230-CAB-JMA, 2014 WL  
3 12570970, at \*7 (S.D. Cal. Feb. 11, 2014) (citing *Multiven v. Cisco Sys. Inc.*, 725 F. Supp.  
4 2d 887, 895 (N.D. Cal. 2010)). Plaintiff brings a private action pursuant to section 502(e)  
5 and alleges violations of Sections 502(c)(1), (c)(3), (c)(5), and (c)(7), which provides that  
6 a person is liable if he or she:

7 (1) Knowingly accesses and without permission alters, damages, deletes,  
8 destroys, or otherwise uses any data, computer, computer system, or computer  
9 network to either (A) devise or execute any scheme or artifice to defraud,  
deceive, or extort, or (B) wrongfully control or obtain money, property or data.

10 ...  
11 (3) Knowingly and without permission uses or causes to be used  
computer services.

12 ...  
13 (5) Knowingly and without permission disrupts or causes the disruption  
14 of computer services or denies or causes the denial of computer services to  
an authorized user of a computer, computer system, or computer network.

15 ...  
16 (7) Knowingly and without permission accesses or causes to be accessed  
any computer, computer system, or computer network.

17 Cal. Penal Code §§ 502(c)(1), (3), (5), (7). All of the prohibited conduct articulated in the  
18 subsections above requires that the defendant act “without permission.” *In re Carrier IQ,*  
19 *Inc.*, 78 F. Supp. 3d 1051, 1098 (N.D. Cal. 2015). “For purposes of Section 502, parties act  
20 without permission when they circumvent [ ] technical or code-based barriers in place to  
21 restrict or bar a user’s access.” *Sunbelt Rentals Inc.*, 43 F. Supp. 3d at 1032 (internal  
22 quotations omitted).

23 Defendants contend that “access” or “use of data without permission” requires a  
24 showing of “circumventing technical or code based barriers intended to restrict such  
25 access.” (Doc. No. 9 at 13.) However, the Court notes that circumventing technical barriers  
26 is not the *only* way to access or use a computer “without permission,” but that it is the  
27 relevant requirement for the Court’s consideration here because Plaintiff does not allege  
28

1 facts that Defendants misused information.<sup>6</sup> *See Christensen*, 828 F.3d at 789–90. Here,  
2 Plaintiff alleges Defendants acted “without permission” after Plaintiff “blocked various IP  
3 addresses associated with Defendants, and instead of ceasing [the click fraud scheme],  
4 Defendants began to use proxy servers that automatically rotated IP addresses to  
5 strategically avoid the Plaintiff’s blocking efforts.” (Doc. No. 1 ¶ 29.) The Court finds this  
6 allegation to be a sufficient for pleading the “without permission” requirement. *See Power*  
7 *Ventures*, 844 F.3d at 1069 (finding CDAFA analysis to be same as CFAA analysis on  
8 similar facts).

9       However, Plaintiff’s CDAFA claims ultimately fail on its allegations of “access” and  
10 “disruption of computer services.” Similar to Plaintiff’s alleged CFAA violations, the Court  
11 finds Plaintiff has not adequately pled facts with enough particularity to show that  
12 Defendants accessed Plaintiff’s computers. Further, Plaintiff’s allegation of disruption  
13 under section 502(c)(5) is conclusory and merely restates the statutory language instead of  
14 providing factual support to show Defendants’ click fraud scheme disrupted their computer  
15 service or data. (*See* Doc. No. 1 ¶ 46.) Consequently, the Court finds Plaintiff has failed to  
16 state a claim against Defendants under this subsection as well. *See Oracle Corp. v. SAP*  
17 *AG*, 734 F. Supp. 2d 956, 964 (N.D. Cal. 2010) (defendant did not violate section 502(c)(5)  
18 where there were no facts of slowdowns; disruptions in service; impairments to the  
19 availability of the data; or changes, deletions, or destruction of data).

20       Therefore, Plaintiff’s claims under the CDAFA are **DISMISSED**.

#### 21       **D. California’s Unfair Competition Law**

22       Plaintiff alleges Defendants’ click fraud scheme also violated the “unlawful” and  
23  
24

---

25 <sup>6</sup> The Ninth Circuit highlighted the alternative method of demonstrating the “without  
26 permission” element. While the CDAFA only requires *knowing access* and *not*  
27 *unauthorized access*, using valid login credentials and subsequently misusing the  
28 information obtained does in fact constitute a CDAFA violation. *United States v.*  
*Christensen*, 828 F.3d 763, 789–90 (9th Cir. 2015).

1 “unfair” prongs of the UCL.<sup>7</sup> (Doc. No. 1 ¶ 66.) Defendants contend Plaintiff does not  
2 allege a valid violation under any of the UCL’s three available theories, is not entitled to  
3 the relief it seeks, and has failed to plead with the requisite Rule 9(b) particularity.<sup>8</sup> (Doc.  
4 No. 9 at 16-18.)

5 California's Unfair Competition Law “is a broad remedial statute that permits an  
6 individual to challenge wrongful business conduct in whatever context such activity might  
7 occur.” *Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007) (internal  
8 quotation marks and citation omitted). The UCL prohibits any “unlawful, unfair, or  
9 fraudulent business act or practice.” Cal. Bus. & Prof. Code § 17200. Accordingly, there  
10 are three prongs under which a claim may be established: unlawful, unfair, and fraudulent.  
11 *Daro v. Superior Court*, 151 Cal. App. 4th 1079, 1093 (2007) (“a business act or practice  
12 need only meet one of the three criteria—unlawful, unfair, or fraudulent—to be considered  
13 unfair competition”); *Lozano*, 504 F.3d at 731 (“[e]ach prong . . . is a separate and distinct  
14 theory of liability”).

### 15 **1. Unlawful Business Practice**

16 “Unlawful” practices are “any practices forbidden by law, be it civil or criminal,  
17 federal, state, or municipal, statutory, regulatory, or court-made.” *Saunders v. Superior*  
18 *Court*, 27 Cal. App. 4th 832, 838–39 (1994). “By proscribing any unlawful business  
19 practice, [the UCL] borrows violations of other laws and treats them as unlawful practices  
20 that the unfair competition law makes independently actionable.” *Woods v. Google, Inc.*,

---

22 <sup>7</sup> Plaintiff originally asserted a claim under the “fraudulent” prong, (Doc. 1 ¶ 66), but  
23 appears to abandon this theory in its opposition, (*See* Doc No. 10 at 23) (“Satmodo brings  
24 its UCL claim under the ‘unlawful’ and ‘unfair’ prongs of the UCL.”). Therefore, the  
25 Court will not address the “fraudulent” prong.

26 <sup>8</sup> The Court finds Defendants’ “safe harbor” argument unpersuasive. “The rule does not []  
27 prohibit an action under the [UCL] merely because some other statute on the subject does  
28 not, itself, provide for the action or prohibit the challenged conduct. To forestall an action  
under the [UCL], another provision must actually ‘bar’ the action or clearly permit the  
conduct.” *Cel-Tech Commc’ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 182–  
83 (1999).

1 No. 11-cv-1263-JF, 2011 WL 3501403, at \*7 (N.D. Cal. Aug. 10, 2011) (internal quotation  
2 marks omitted) (citing *Cel-Tech Commc'ns, Inc.*, 20 Cal. 4th at 180)). The unlawful  
3 activities Plaintiff alleges in its complaint are for violations of the CFAA and CDAFA.  
4 Since Plaintiff has not pled these claims adequately, it follows that Plaintiff has failed to  
5 provide an independent violation to state a claim under the “unlawful” prong of the UCL.  
6 *See Woods*, 2011 WL 3501403, at \*7. Thus, Plaintiff's claim of an "unlawful" practice  
7 under the UCL is **DISMISSED**.

## 8 ***2. Unfair Business Practice***

9 The “unfair” prong under the UCL, targets conduct that “threatens an incipient  
10 violation of an antitrust law, or violates the policy or spirit of one of those laws because its  
11 effects are comparable to or the same as a violation of the law, or otherwise significantly  
12 threatens or harms competition.” *Cel-Tech Commc'ns, Inc.*, 20 Cal. 4th at 187 (designating  
13 the present test for actions between competitors alleging anticompetitive practices); *see*  
14 *also Lozano*, 504 F.3d at 735 (recognizing test as appropriate for actions based on  
15 unfairness between competitors). Thus, Plaintiff must allege that Defendants’ conduct ““(1)  
16 violates the policy or spirit of the antitrust laws because the effect of the conduct is  
17 comparable to or the same as a violation of the antitrust laws, or (2) it otherwise  
18 significantly threatens or harms competition.”” *Obesity Research Inst., LLC v. Fiber*  
19 *Research Int’l, LLC*, 165 F. Supp. 3d 937, 953 (S.D. Cal. 2016) (quoting *People’s Choice*  
20 *Wireless, Inc. v. Verizon Wireless*, 131 Cal. App. 4th 656, 662 (2005)). Conduct that  
21 violates the spirit of antitrust laws includes exclusive dealing, horizontal price fixing, and  
22 monopolization. *Id.*

23 Plaintiff’s independent claim under the “unfair” prong has been sufficiently pled.  
24 The crux of Plaintiff’s complaint focuses on Defendants’ alleged click fraud scheme, which  
25 takes Plaintiff, “one of its main competitors, out of the marketplace for a period of time,  
26 all to the Defendants’ benefit.” (Doc. No. 1 ¶ 66.) These allegations, taken as true, allege  
27 unfair conduct that violates the spirit of antitrust laws and significantly threatens  
28 competition. Moreover, the Court believes the alleged click fraud scheme is the type of

1 conduct the Legislature intended to protect against. “[T]he section was intentionally framed  
2 in its broad, sweeping language, precisely to enable judicial tribunals to deal with the  
3 innumerable ‘new schemes which the fertility of man’s invention would contrive.’” *Cel-*  
4 *Tech Commc’ns. Inc.*, 20 Cal. 4th at 181 (quoting *American Philatelic Soc. v. Claibourne*,  
5 3 Cal. 2d 689, 698 (1935)). However, the Court agrees with Defendants that Plaintiff is not  
6 entitled to recover damages or nonrestitutionary disgorgement under the UCL and is  
7 limited to injunctive relief. *See Korea Supply v. Lockheed Martin Corp.*, 29 Cal. 4th 1134,  
8 1152 (2003) (holding nonrestitutionary disgorgement of profits is not an available remedy  
9 in an individual action under the UCL).

10 Accordingly, Plaintiff’s claim under the “unlawful” prong of the UCL is  
11 **DISMISSED**, and the Court **DENIES** Defendants’ motion to dismiss Plaintiff’s claim  
12 under the “unfair” prong of the UCL.

### 13 **E. Intentional Interference with Prospective Economic Relations**

14 Lastly, Plaintiff alleges "Defendants intentionally interfered with Plaintiff's  
15 economic relationship with potential customers" by making fraudulent clicks and  
16 prematurely terminating Plaintiff's online ad presence each day, thus, eliminating the  
17 number of clicks that would have resulted in a sale absent Defendants' conduct. (Doc. No.  
18 1 ¶ 56.) Defendants counter that Plaintiff has not alleged interference with existing  
19 economic relationships and has not alleged the required independently wrongful conduct.  
20 (Doc. No. 9 at 14-16.) Plaintiff argues that it need only plead a “colorable economic  
21 relationship” and that this relationship is not hypothetical because “there is a known  
22 quantifiable percentage of legitimate clicks (had they not been replaced by Defendants’  
23 fraudulent clicks) that would have led to actual customers.” (Doc. No. 10 at 15-16.)

24 First, Plaintiff must plead "that the [Defendants'] interference was wrongful by some  
25 measure beyond the fact of interference itself." *Della Penna v. Toyota Motor Sales, U.S.A.,*  
26 *Inc.*, 11 Cal. 4th 376, 392-93 (1995). A claim for intentional interference with prospective  
27 economic relations requires an allegation of some independently wrongful conduct that is  
28 "proscribed by some constitutional, statutory, regulatory, common law, or other



1 determinable legal standard." *Korea Supply*, 29 Cal. 4th at 1159. "Wrongful conduct" has  
2 been interpreted to mean conduct "outside the realm of legitimate business transactions"  
3 and conduct that "may lie in the method used or by virtue of an improper motive." *Della*  
4 *Penna*, 11 Cal. 4th at 380 n.1. Plaintiff rests its claim of independently actionable wrongful  
5 conduct upon its claims under the CFAA, CDAFA, and UCL. (Doc. No. 1 ¶ 57.) Here,  
6 because Plaintiff has adequately pleaded a claim under the "unfair" prong of the UCL, it  
7 has sufficiently alleged the necessary wrongful conduct to support a claim for intentional  
8 interference with prospect economic relations.

9         However, the Court finds that Plaintiff has not sufficiently pleaded the necessary  
10 existing economic relationship. *See Westside Ctr. Assocs. v. Safeway Stores 23, Inc.*, 42  
11 Cal. App. 4th 507, 523–28 (1996). The elements of a cause of action for intentional  
12 interference with prospective economic relations under California law are: (1) an economic  
13 relationship between the plaintiff and another containing a probability of future economic  
14 benefit, (2) knowledge by the defendant of the existence of the relationship, (3) intentional  
15 acts on the part of the defendant designed to disrupt the relationship, (4) actual disruption  
16 of the relationship, and (5) damages to the plaintiff proximately caused by the acts of the  
17 defendant. *Korea Supply*, 29 Cal. 4th at 1153. "To establish the first element, plaintiff must  
18 allege the existence of a specific prospective relationship, not potential relationships with  
19 a class of unknown investors or purchasers." *Buxton v. Eagle Test Sys., Inc.*, No. C-08-  
20 04404 RMW, 2010 WL 1240749, at \* 1 (N.D. Cal. Mar. 26, 2010) (quotation marks and  
21 citation omitted); *see also Kasparian v. Cty. of Los Angeles*, 38 Cal. App. 4th 242, 261  
22 (1995) ("an interference with an existing contract or a contract which is certain to be  
23 consummated"). Plaintiff alleges to have "prospective economic relationships with a  
24 certain percentage of all individuals making valid clicks on its paid advertisement." (Doc.  
25 No. 1 ¶ 53.) However, Plaintiff does not allege any facts that show the existence of any  
26 specific economic relationship with identifiable third parties. Without any identifiable  
27 prospective customers, Plaintiff's expectation is "at most a hope for an economic  
28 relationship and a desire for future benefit." *Blank v. Kirwan*, 39 Cal. 3d 311, 331 (1985).

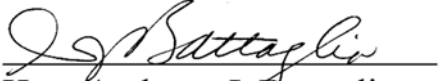
1           Consequently, Plaintiff's claim for intentional interference with prospective  
2 economic relations is **DISMISSED**.

3   **CONCLUSION**

4           In light of the above, the Court **GRANTS IN PART** and **DENIES IN PART**  
5 Defendants' motion to dismiss Plaintiff's complaint. The Court **DISMISSES WITHOUT**  
6 **PREJUDICE** Plaintiff's claims under the CFAA, CDAFA, "unlawful" prong of the UCL,  
7 and intentional interference with prospective economic relations. Plaintiff may address the  
8 deficiencies noted herein by filing an amended complaint no later than **30 days from the**  
9 **issuance of this order.**

10  
11 **IT IS SO ORDERED.**

12  
13 Dated: April 14, 2017

  
14 Hon. Anthony J. Battaglia  
15 United States District Judge  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28