



1 Presently before the Court is Defendants' motion to dismiss pursuant to Federal  
2 Rule of Civil Procedure 12(b)(6) for failure to state a claim, filed on May 6, 2013.<sup>1</sup>  
3 (Defs.' Mot. Dismiss, May 6, 2013, ECF No. 12.) Plaintiffs filed a timely opposition on  
4 June 13, 2013. (Pls.' Opp'n to Defs.' Mot. to Dismiss, June 13, 2013, ECF No. 30.) For  
5 the reasons set forth below, Defendants' motion to dismiss is GRANTED IN PART and  
6 DENIED IN PART.<sup>2</sup>

### 8 BACKGROUND<sup>3</sup>

9  
10 Farmers sells insurance policies, including automobile, homeowner, commercial,  
11 and life insurance, to customers through independent contractor agents. Farmers' most  
12 valuable assets are its customers (policyholders) and the policyholder information that  
13 Farmers maintains about each customer. Farmers agents are exclusive agents for  
14 Farmers' insurance products. The agents may not promote or sell insurance policies  
15 issued by other insurers. Each Farmers agent must agree to use Farmers' trade secret  
16 customer information only in the course of the agent's relationship with Farmers. Each  
17 agent must further promise not to divulge Farmers' trade secret customer information to  
18 third parties or to use it in any way detrimental to Farmers. This information is not  
19 shared with Farmers' competitors.

20 Farmers maintains databases, which include the Electronic Customer Marketing  
21 System ("eCMS"). Farmers also operates a secure website for its agents, known as the  
22 "Agency Dashboard."

23 ///

24  
25 <sup>1</sup> All further references to "Rule" or "Rules" are to the Federal Rules of Civil Procedure unless  
otherwise noted.

26 <sup>2</sup> Because oral argument will not be of material assistance, the Court orders this matter submitted  
27 on the briefs. E.D. Cal. Local R. 230(g).

28 <sup>3</sup> The following factual background is taken, sometimes verbatim, from Plaintiffs' Complaint. (Pls.'  
Compl. Contained in Defs.' Notice of Removal, Apr. 5, 2013, ECF No. 1 at 9-15.)

1 The Agency Dashboard is a password-protected Internet portal to designated computer  
2 servers that allows Farmers insurance agents, District Managers and employees to track  
3 information and provide services to its policyholders. eCMS is an important tool on the  
4 Farmers' "Agency Dashboard," accessed and used by Farmers' authorized insurance  
5 agents. eCMS enables authorized users to access "Confidential Policyholder  
6 Information" about the policyholders they service, and allows agents to create  
7 policyholder reports, contact lists, mailing labels, etc. eCMS contains information about  
8 prospective, current, and former policyholders, including names, addresses, telephone  
9 numbers, social security numbers, driver's license numbers, policy expiration dates,  
10 insured properties, claims histories, discount eligibilities and other information. Farmers  
11 invests significant time, labor and capital in developing this information. The Confidential  
12 Policyholder Information is not generally available in this aggregated form in the industry  
13 or to Farmers' competitors. If this information were available to Farmers' competitors,  
14 those competitors could more easily solicit Farmers' policyholders to change insurance  
15 providers.

16 Use of eCMS is subject to certain confidentiality restrictions and security  
17 protections. Farmers maintains its Confidential Policyholder Information, including policy  
18 expirations, on a password and user-ID protected system. When an agent's Agency  
19 Appointment Agreement is terminated, Farmers turns off the agent's access, and their  
20 staffs' access, to eCMS and the Agency Dashboard, and the terminated agent's user  
21 ID/password combination is no longer valid. Farmers also issues company policies  
22 regarding access to and preservation of Confidential Policyholder Information by  
23 maintaining copies of those policies on the Agency Dashboard. Periodically, Farmers  
24 reminds its insurance agents of Farmers' confidentiality policies through bulletins, yearly  
25 compliance memoranda and other communications. Finally, each time an agent  
26 accesses Farmers' proprietary system through the Agency Dashboard, that agent must  
27 agree to be bound by the terms of a separate "Legal Disclaimer."

28 ///

1 The Legal Disclaimer provides that the information the agent is accessing is Farmers’  
2 proprietary, confidential and trade secret information.

3 Defendants Troy Steele and Steele Insurance Agency

4 Defendant Steele was appointed a District Manager with Farmers in 2001,  
5 pursuant to a District Manager Appointment Agreement.

6 Pursuant to the terms of this Agreement, Farmers terminated Defendant Steele’s  
7 Agreement in January 2010. Thereafter, Defendant Steele began his own independent  
8 insurance agency—the Steele Insurance Agency. Defendant Steele and the Steele  
9 Insurance Agency were not appointed or allowed to sell Farmers’ insurance products.  
10 Plaintiffs allege that Defendant Steele is using improper means to obtain access to  
11 Farmers’ policyholder information. Plaintiffs further contend that Defendant Steele is  
12 directing current and former Farmers agents, or their staff members, to use Plaintiffs’  
13 customer lists and other trade secret information to solicit Farmers’ customers to switch  
14 to the Steele Insurance Agency. According to Plaintiffs, Farmers has lost numerous  
15 customers (previously serviced by Defendant McCarren, Charlie Finister and Bill Henton)  
16 to the Steele Insurance Agency as a result of Defendant Steele’s trade secret  
17 misappropriation.

18 Defendant Larry McCarren

19 Defendant McCarren was appointed as a Farmers agent in January 1992,  
20 pursuant to an Agency Appointment Agreement. Defendant McCarren worked in the  
21 district of District Manager Defendant Blalock until January 2012. Defendant Blalock’s  
22 District Manager Appointment Agreement was terminated in January 2012. Defendant  
23 Blalock then went to work for the Steele Insurance Agency.

24 ///

25 ///

26 ///

27 ///

28 ///

1 According to Plaintiffs, while Defendant McCarren was still a Farmers agent, he  
2 was writing policies for other insurers, in violation of his Agency Appointment Agreement.  
3 In August 2012, Defendant McCarren exercised his option under his Agency  
4 Appointment Agreement to terminate his Agreement with Farmers, after giving three  
5 months' written notice. Thus, Defendant McCarren's termination became effective  
6 November 3, 2012. Defendant McCarren is now appointed with and working as an  
7 insurance agent for Steele Insurance Agency.

8 Following Defendant McCarren's resignation, Farmers received customer  
9 complaints that Defendant McCarren had contacted them in an attempt to switch their  
10 insurance business to other carriers.

11 Farmers also alleges that prior to leaving Farmers, Defendant McCarren accessed  
12 Farmers' computer system to download information regarding Farmers' policyholders,  
13 including his entire customer list, for the purpose of using this information after  
14 termination of his Agency Appointment Agreement. Downloading this information was in  
15 violation of Defendant McCarren's Agency Appointment Agreement. Plaintiffs allege that  
16 Defendant McCarren is working at the direction of Defendants Steele and Blalock in  
17 attempting to transfer Farmers' policyholders from Farmers to other insurers for the  
18 benefit of Defendant Steele Insurance Agency.

19 Defendant Cindy Jo Perkins

20 Defendant Perkins was Defendant McCarren's longtime employee. In the spring  
21 of 2012, Defendant Perkins went to work for another Farmers agent, Charlie Finister.  
22 Throughout the year of 2012, Mr. Finister was gravely ill with diabetes. Mr. Finister  
23 resigned and went into hospice in early November 2012. After Mr. Finister resigned,  
24 Defendant Perkins did not have permission to sell Farmers' insurance products or to  
25 access Farmers' computer systems. However, Defendant Perkins admitted that she had  
26 used Mr. Finister's user ID and password combination to gain access to information from  
27 Farmers' computer system while she worked in Mr. Finister's office, although she did not  
28 have permission to do so.

1 Defendant Perkins was appointed with Steele Insurance Agency and was so appointed  
2 when she was accessing Farmers' computer system. Defendant Perkins remains  
3 appointed with Steele Insurance Agency and, according to Plaintiffs, is working together  
4 with Defendants Steele and Blalock to transfer Farmers' policyholders to other insurers  
5 for the benefit of Defendant Steele Insurance Agency.

6 Defendant Bill Henton

7 Bill Henton ("Mr. Henton"), Defendant Henton's father, was a Farmers agent from  
8 1968 to 2012. In 2012, Mr. Henton's District Manager, Rudy Cedre, believed that  
9 Mr. Henton had developed severe memory problems. Defendant Henton worked in  
10 Mr. Henton's office, but Defendant Henton was not appointed as an agent with Farmers.

11 In November 2012, Mr. Henton resigned as a Farmers agent. Farmers has since  
12 learned that prior to Mr. Henton's resignation from Farmers, Defendant Henton allowed  
13 his wife and daughter to access the Farmers computer system for the purpose of  
14 accessing Farmers' policyholder information. Defendant Henton is also in the process of  
15 becoming a part of Steele Insurance Agency. Defendant Henton remains in control of  
16 the physical files relating to over 1,600 Farmers policies and will not allow Farmers to  
17 access these files. Defendant Henton also arranged for his father's mail, including  
18 Farmers' business mail, to be forwarded to Defendant Henton's new business address.  
19 Defendant Henton is working together with Defendants Steele and Blalock to transfer  
20 Farmers' policyholders from Farmers to other insurers for the benefit of Defendant  
21 Steele Insurance Agency.

22 Thus, the gravamen of Plaintiffs' complaint is that Defendants obtained Plaintiffs'  
23 trade secret information and used that information to switch Farmers customers to the  
24 Steele Insurance Agency.

25 ///

26 ///

27 ///

28 ///



1 If the “plaintiffs . . . have not nudged their claims across the line from conceivable to  
2 plausible, their complaint must be dismissed.” Id. However, “[a] well-pleaded complaint  
3 may proceed even if it strikes a savvy judge that actual proof of those facts is  
4 improbable, and ‘that a recovery is very remote and unlikely.’” Id. at 556 (quoting  
5 Scheuer v. Rhodes, 416 U.S. 232, 236 (1974)).

6 A court granting a motion to dismiss a complaint must then decide whether to  
7 grant leave to amend. Leave to amend should be “freely given” where there is no  
8 “undue delay, bad faith or dilatory motive on the part of the movant, . . . undue prejudice  
9 to the opposing party by virtue of allowance of the amendment, [or] futility of the  
10 amendment . . . .” Foman v. Davis, 371 U.S. 178, 182 (1962); Eminence Capital, LLC v.  
11 Aspeon, Inc., 316 F.3d 1048, 1052 (9th Cir. 2003) (listing the Foman factors as those to  
12 be considered when deciding whether to grant leave to amend). Not all of these factors  
13 merit equal weight. Rather, “the consideration of prejudice to the opposing party . . .  
14 carries the greatest weight.” Id. (citing DCD Programs, Ltd. v. Leighton, 833 F.2d 183,  
15 185 (9th Cir. 1987). Dismissal without leave to amend is proper only if it is clear that “the  
16 complaint could not be saved by any amendment.” Intri-Plex Techs. v. Crest Group,  
17 Inc., 499 F.3d 1048, 1056 (9th Cir. 2007) (citing In re Daou Sys., Inc., 411 F.3d 1006,  
18 1013 (9th Cir. 2005); Ascon Props., Inc. v. Mobil Oil Co., 866 F.2d 1149, 1160 (9th Cir.  
19 1989) (“Leave need not be granted where the amendment of the complaint . . .  
20 constitutes an exercise in futility . . . .”)).

## 21 22 ANALYSIS

23  
24 Plaintiffs assert nine causes of action under state and federal law. Specifically,  
25 Plaintiffs allege that Defendants are liable under California state law for breach of  
26 contract, misappropriation of trade secrets, intentional interference with contractual  
27 relations, intentional interference with prospective economic advantage, unfair  
28 competition, breach of fiduciary duty and civil conspiracy.



1 Plaintiffs also allege that Defendants are liable under federal law for violations of the  
2 Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. §§ 1030(a)(2)(c), (a)(4).  
3 Defendants first argue that California’s Uniform Trade Secrets Act preempts each of  
4 Plaintiffs’ causes of action, save for Plaintiffs’ claim for misappropriation of trade secrets.  
5 Defendants also argue that each of the nine causes of actions asserted in the complaint  
6 fails to state a claim upon which relief can be granted. The Court will address each  
7 issue in turn.

8  
9 **A. Civil Conspiracy**

10  
11 As a threshold matter, the Court must address Plaintiffs’ ninth cause of action for  
12 civil conspiracy against all Defendants. (ECF No. 1 at 23.) Plaintiffs allege that  
13 Defendants “formed and operated a conspiracy to illegally misappropriate and use . . .  
14 Farmers trade secret protected policyholder information for the purpose of soliciting  
15 Farmers customers away from Farmers and towards the Steele Insurance Agency.”  
16 (ECF No. 1 at 23.) Plaintiffs contend that “in furtherance of the conspiracy,” Defendants  
17 misappropriated and used Farmers’ trade secret policyholder information by accessing  
18 and using Farmers’ proprietary computer system without authorization. (Id.)

19 Civil conspiracy “is not a cause of action but a legal doctrine that imposes liability  
20 on persons who, although not actually committing a tort themselves, share with the  
21 immediate tortfeasors a common plan or design in its perpetration.” Applied Equipment  
22 Corp. v. Litton Saudi Arabia Ltd., 7 Cal.4th 503, 510 (1994) (citing Wyatt v. Union  
23 Mortgage Co., 24 Cal.3d 773, 784 (1979)); see also Entm’t Research Grp. Inc. v.  
24 Genesis Creative Grp., Inc., 122 F.3d 1211, 1228 (9th Cir. 1997). “Standing alone, a  
25 conspiracy does no harm and engenders no tort liability. It must be activated by the  
26 commission of an actual tort.” Applied Equipment Corp., 7 Cal. 4th at 511.

27 ///

28 ///

1 The elements of a civil conspiracy are: (1) the formation and operation of a  
2 conspiracy; (2) wrongful conduct in furtherance of the conspiracy; and (3) damages  
3 arising from the wrongful conduct. Applied Equip., 7 Cal. 4th at 511; see also Doctors'  
4 Co. v. Super. Ct., 49 Cal. 3d 39, 44 (1989). Each member of the alleged conspiracy  
5 must be legally capable of committing the underlying tort -- that is, each member must  
6 owe a duty to the plaintiff that is recognized by law and must be potentially subject to  
7 liability for breach of that duty -- and must intend the success of the purpose of the  
8 conspiracy. Applied Equip., 7 Cal.4th at 511. In addition, all elements of the underlying  
9 tort must be satisfied. See id. If the plaintiff fails to adequately plead the underlying  
10 claim, the corresponding conspiracy claim must also fail. Id.

11 A plaintiff generally need not plead a claim for civil conspiracy with particularity.  
12 See Intel Learning Tech., Inc. v. Beijing Kaidi Educ., No. C 06-7541 PJH, 2007 WL  
13 2288329 (N.D. Cal. Aug. 9, 2007) (citing Wasco Prods., Inc. v. Southwall Techs., Inc.,  
14 435 F.3d 989, 990-91 (9th Cir. 2006). However, when a plaintiff alleges that the object  
15 of the agreement is fraudulent, the plaintiff must plead a claim for civil conspiracy with  
16 the particularity required by Rule 9(b). Wasco Prods., Inc., 435 F.3d at 990-91; see also  
17 Kearns v. Ford Motor Co., 567 F.3d 1120, 1124 (9th Cir. 2009) ("Rule 9(b) requires that,  
18 when fraud is alleged, 'a party must state with particularity the circumstances constituting  
19 fraud . . . ."). "Where fraud is not an essential element of a claim, only those allegations  
20 of a complaint which aver fraud are subject to Rule 9(b)'s heightened pleading  
21 standard." Kearns, 567 F.3d at 1124. Rule 9(b) requires that the circumstances  
22 constituting the alleged fraud "be 'specific enough to give defendants notice of the  
23 particular misconduct . . . so that they can defend against the charge and not just deny  
24 that they have done anything wrong.'" Bly-Magee v. California, 236 F.3d 1014, 1019  
25 (9th Cir. 2001) (quoting Neubronner v. Milken, 6 F.3d 666, 671 (9th Cir. 1993)).  
26 Accordingly, "[a]llegations of fraud must be accompanied by 'the who, what, when,  
27 where, and how' of the misconduct charged."

28 ///

1 Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting Cooper v.  
2 Pickett, 137 F.3d 616, 627 (9th Cir. 1997)).

3 Here, Plaintiffs allege that “in perpetrating the above stated acts [of conspiracy],  
4 Defendants acted willfully, maliciously, and fraudulently . . . .” (ECF No. 1 at 24  
5 (emphasis added).) Thus, Plaintiffs’ allegations regarding the alleged conspiracy must  
6 meet the heightened pleading standard of Rule 9(b). Plaintiffs fail to do so, as Plaintiffs  
7 make only generalized allegations regarding Defendants’ actions in carrying out the  
8 alleged conspiracy. For example, Plaintiffs allege that Defendants “formed and operated  
9 a conspiracy” and “engaged in wrongful conduct in furtherance of the conspiracy,  
10 including but not limited to misappropriation and use of electronic and paper copies of  
11 Farmers’ trade secret protective policyholder information and through the unauthorized  
12 use and access [of] Farmers’ proprietary computer system.” (ECF No. 1 at 23.)  
13 However, these allegations do not come close to alleging “the who, what, when, where,  
14 and how” of the alleged conspiracy. See Vess, 317 F.3d at 1106.

15 In short, Plaintiffs’ allegations as to this cause of action amount to little more than  
16 vague claims that Defendants fraudulently conspired to steal Plaintiffs’ trade secrets.  
17 Such allegations do not meet the heightened pleading standard of Rule 9(b).  
18 Accordingly, Defendants’ motion to dismiss this claim is granted.

19  
20 **B. Preemption**

21  
22 “Only if the legislature enacts a statute intending to ‘cover the entire subject or . . .  
23 to occupy the field’ does a statute supersede the common law.” AcculImage Diagnostics  
24 Corp v. Terarecon, Inc., 260 F. Supp. 2d 941, 953 (N.D. Cal. 2003) (quoting I.E.  
25 Assocs.v. Safeco Title Ins. Co., 39 Cal. 3d 281, 285 (1985)). The California Uniform  
26 Trade Secrets Act (“CUTSA”) is codified in sections 3426 through 3426.11 of the Civil  
27 Code. “CUTSA has been characterized as having a ‘comprehensive structure and  
28 breadth . . . .”

1 K.C. Multimedia, Inc. v. Bank of Am. Tech. & Operations, Inc., 171 Cal. App. 4th 939,  
2 954 (2009) (quoting Acculmage Diagnostics Corp, 260 F. Supp. 2d at 953). The CUTSA  
3 clearly sets forth:

4 the definition of ‘misappropriation’ and ‘trade secret,’  
5 injunctive relief for actual or threatened misappropriation,  
6 damages, attorney fees, methods for preserving the secrecy  
7 of trade secrets, the limitations period, the effect of the title on  
8 other statutes or remedies, statutory construction,  
severability, the application of title to acts occurring prior to  
the statutory date, and the application of official proceedings  
privilege to disclosure of trade secret information.

9 Id. (quoting Acculmage Diagnostics Corp., 260 F. Supp. 2d at 953). “That breadth  
10 suggests a legislative intent to preempt the common law.” Id. Accordingly, “[a]t least as  
11 to common law trade secret misappropriation claims, [C]UTSA occupies the field in  
12 California.” Id. (quoting Acculmage Diagnostics Corp., 260 F. Supp. 2d at 954).

13 Moreover, CUTSA specifically addresses preemption. Section 3426.7 of the  
14 CUTSA reads in relevant part:

15 (a) Except as otherwise expressly provided, this title does not  
16 supersede any statute relating to misappropriation of a trade  
secret, or any statute otherwise regulating trade secrets.

17 (b) This title does not affect (1) contractual remedies, whether  
18 or not based upon misappropriation of a trade secret,  
19 (2) other civil remedies that are not based upon  
20 misappropriation of a trade secret, or (3) criminal remedies,  
whether or not based upon misappropriation of a trade  
secret.

21 Cal. Civ. Code §§ 3426.7(a)-(b). Thus, while section 3426.7 “expressly allows  
22 contractual and criminal remedies, whether or not based on trade secret  
23 misappropriation,” it also “implicitly preempts alternative civil remedies based on trade  
24 secret misappropriation.” K.C. Multimedia, Inc., 171 Cal. App. 4th at 954.

25 ///

26 ///

27 ///

28 ///

1 Courts applying California law have found that claims “based entirely on the same  
2 factual allegations that form the basis of [the] trade secrets claim” are preempted.  
3 Callaway Golf Co. v. Dunlop Slazenger Grp. Ams., Inc., 318 F. Supp. 2d 216, 220 (D.  
4 Del. 2004) (applying California law); see also Gabriel Techs. Corp. v. Qualcomm Inc.,  
5 No. 08cv1992–MMA(POR), 2009 WL 3326631, \*11 (S.D. Cal. Sept. 3, 2009) (“California  
6 courts have adopted a broad view of preemption in this area and have held that common  
7 law claims that are based on the same nucleus of facts as a misappropriation claim are  
8 preempted.”). “Preemption is not triggered where the facts in an independent claim are  
9 similar to, but distinct from, those underlying the misappropriation claim.” Gabriel Techs.  
10 Corp., 2009 WL 3326631 at \*11. Thus, “the preemption inquiry for those causes of  
11 action not specifically exempted by [section] 3426.7(b) focuses on whether other claims  
12 are no more than a restatement of the same operative facts supporting trade secret  
13 misappropriation. If there is no material distinction between the wrongdoing alleged in a  
14 [C]UTSA claim and that alleged in a different claim, the [C]UTSA preempts the other  
15 claim.” Id. (quoting Convolve, Inc. v. Compaq Computer Corp., No. 00 CV 5141(GBD),  
16 2006 WL 839022, at \*6 (S.D.N.Y. Mar. 31, 2006) (applying California law)).

17 Thus, in the present case, the Court’s inquiry must focus on whether the  
18 wrongdoing alleged in Plaintiffs’ claims for breach of contract, intentional interference  
19 with contractual relations, intentional interference with prospective economic advantage,  
20 unfair competition, breach of fiduciary duty, civil conspiracy and violations of the  
21 Computer Fraud and Abuse Act can be materially distinguished from the wrongdoing  
22 alleged in Plaintiffs’ trade secret misappropriation claim. See supra.

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///



1                                   **2. Intentional Interference with Contractual Relations**

2  
3           Plaintiffs’ third cause of action is for intentional interference with contractual  
4 relations, alleged against all Defendants. In support of this claim, Plaintiffs allege that  
5 Farmers had contractual relationships with Farmers agents and with Farmers  
6 policyholders. According to Plaintiffs, Defendants Steele and Blalock interfered with  
7 Farmers’ contractual relations with its former agent, Defendant McCarren, by  
8 intentionally inducing Defendant McCarren to breach his contract with Farmers by  
9 requesting, encouraging, or helping Defendant McCarren to misappropriate Farmers’  
10 proprietary information, use Farmers’ proprietary information in a manner detrimental to  
11 Farmers, or improperly retain Farmers’ proprietary information after McCarren’s Agency  
12 Appointment Agreement was terminated. (ECF No. 1 at 18.) Plaintiffs also allege that  
13 “all Defendants” interfered with Farmers’ contractual relations with its policyholders by  
14 “intentionally inducing policyholders to change their insurance coverage . . . to that  
15 provided through the Steele Insurance Agency.” (Id.)

16           As stated above, “[t]he preemption inquiry for those causes of action not  
17 specifically exempted by [section] 3426.7(b) focuses on whether other claims are not  
18 more than a restatement of the same operative facts supporting trade secret  
19 misappropriation. If there is no material distinction between the wrongdoing alleged in a  
20 [C]UTSA claim and that alleged in a different claim, the [C]UTSA claim preempts the  
21 other claim.” Bryant v. Mattel, Inc., CV 04-9049 DOC RNBX, 2010 WL 3705668, at \*20  
22 (C.D. Cal. Aug. 2, 2010) (quoting Convolve, Inc., 2006 WL 839022 at \*6). Here,  
23 Plaintiffs’ allegations regarding intentional interference with contractual relations do little  
24 more than restate Plaintiffs’ claim for trade secret misappropriation.

25 ///

26 ///

27 ///

28 ///

1 That is, Plaintiffs' allegations that Defendants Steele and Blalock intentionally induced  
2 Defendant McCarren to breach his contract with Farmers by stealing Plaintiffs' trade  
3 secret information merely restates Plaintiffs' allegations that Defendants McCarren,  
4 Steele and Blalock "misappropriated Farmers' trade secrets by . . . retaining or utilizing  
5 Farmers' Proprietary Information for the purpose of soliciting, directing, or advising  
6 Farmers' policyholders to switch their coverage away from Farmers and to Steele's  
7 competing business." (ECF No. 1 at 17.)

8 As such, Plaintiffs' claim for intentional interference with contractual relations is  
9 preempted by Plaintiffs' claim for misappropriation of trade secrets. Defendants' motion  
10 to dismiss this claim is therefore granted.

### 11 12 **3. Intentional Interference with Prospective Economic Advantage**

13  
14 Plaintiffs' fourth cause of action is for intentional interference with prospective  
15 economic advantage alleged against all Defendants. To support this claim, Plaintiffs  
16 allege that at all relevant times, an economic relationship existed between Farmers and  
17 its policyholders, and this economic relationship contained a probable future economic  
18 benefit for Farmers in the form of premiums that the policyholders would pay on currently  
19 held policies and policies that would be purchased by those policyholders in the future.  
20 (ECF No. 1 at 18.) Defendants knew that these economic relationships existed. (Id. at  
21 19.) Defendants interfered with Farmers' prospective economic advantages by  
22 intentionally inducing policyholders to change their coverage to that provided through  
23 Defendant Steele Insurance Agency. (Id.) Defendants' acts disrupted Farmers'  
24 relationships with Farmers' policyholders, and these acts were intentionally designed to  
25 interfere with, and disrupt, those relationships. (Id.) Specifically, Plaintiffs allege that  
26 Defendants "sought to benefit themselves . . . and Steele's insurance agency . . . by  
27 persuading [Farmers'] policyholders to purchase policies offered by" insurance  
28 companies other than Farmers. (Id.)



1 Finally, Plaintiffs allege that Defendants' acts were "improper [and] illegal . . . in that the  
2 scheme for interference involved . . . the misappropriation and use of Farmers' trade  
3 secret protective policyholder information, and . . . the unauthorized use and access [of]  
4 Farmers' computer system." (Id.)

5 Similar to Plaintiffs' claim for intentional interference with contractual relations,  
6 Plaintiffs' claim for intentional interference with prospective economic advantage simply  
7 restates the claim for trade secret misappropriation. The gravamen of this cause of  
8 action is that Defendants misappropriated Plaintiffs' trade secrets, which interfered with  
9 Plaintiffs' prospective economic advantage. Accordingly, there "is no material distinction  
10 between the wrongdoing alleged in" Plaintiffs' CUTSA claim and that alleged in Plaintiffs'  
11 claims for intentional interference with prospective economic advantage. See Bryant,  
12 2010 WL 3705668 at \*20. The CUTSA claim therefore "preempts the other claim." Id.  
13 As such, Plaintiffs' claim for intentional interference with economic advantage is  
14 preempted, and Defendants' motion to dismiss this claim is granted.

#### 15 16 **4. Unfair Competition**

17  
18 Plaintiffs' fifth cause of action is for unfair competition pursuant to California  
19 Business and Professions Code section 17200, against all Defendants. (ECF No. 1 at  
20 19.) "A claim for common law or even statutory unfair competition may be preempted  
21 under [section] 3426.7 if it relies on the same facts as the misappropriation claim."  
22 Gabriel Techs. Corp., 2009 WL 3326631 at \*13 (quoting AcculImage Diagnostics Corp.,  
23 260 F. Supp. 2d at 955). Here, Plaintiffs allege that Defendants "will commit or attempt  
24 to commit...acts of unfair and illegal competition ...with regard to the sale of insurance  
25 policies" by using Plaintiffs' proprietary information, including confidential information and  
26 trade secrets pertaining to Farmers' policyholders, to solicit Farmers' policyholders to  
27 change their business to other insurers, and by inducing Farmers' policyholders to  
28 cancel or not renew their Farmers insurance policies. (ECF No. 1 at 20.)

1 Plaintiffs' claim for unfair competition therefore alleges the same conduct that  
2 gives rise to Plaintiffs' claim for trade secret misappropriation. See Gabriel Techs. Corp.,  
3 2009 WL 3326631 at \*13 (finding unfair competition claim preempted when claim "rests  
4 squarely on the factual allegations of trade secret misappropriation"). Accordingly,  
5 Plaintiffs' claim for unfair competition is preempted, and Defendants' motion to dismiss  
6 this claim is granted.

## 7

### 8 **5. Breach of Fiduciary Duty**

## 9

10 Plaintiffs' sixth cause of action asserts that Defendant McCarren breached his  
11 fiduciary duties to Farmers. Plaintiffs allege that Defendant McCarren "owed fiduciary  
12 duties to Farmers as a result of his agent relationship with Farmers. The fiduciary duties  
13 McCarren owed to Farmers include, but are not limited to, the duty not to misappropriate  
14 trade secrets and unfairly compete with Farmers." (ECF No. 1 at 21.) Plaintiffs allege  
15 that Defendant "McCarren breached his fiduciary duties owed to Farmers by, among  
16 other things, misappropriating trade secrets and competing unfairly with Farmers." (Id.)

17 Plaintiffs' claim for breach of fiduciary duty therefore rests on the same facts as  
18 Plaintiffs' claim for trade secret misappropriation. Indeed, the claim simply asserts that  
19 in misappropriating Farmers' trade secrets, Defendant McCarren also breached his  
20 fiduciary duties to Farmers. Plaintiffs' claim for breach of fiduciary duty is therefore  
21 preempted by the CUTSA, and Defendants' motion to dismiss this claim is granted.

## 22

### 23 **6. Computer Fraud and Abuse Act**

## 24

25 Plaintiffs' seventh and eighth causes of action allege violations of the Computer  
26 Fraud and Abuse Act ("CFAA"). (ECF No. 1 at 21-23.) The CFAA is a federal statute  
27 "enacted in 1984 to enhance the government's ability to prosecute computer crimes.

28 ///

1 The act was originally designed to target hackers who accessed computers to steal  
2 information or to disrupt or destroy computer functionality, as well as criminals who  
3 possessed the capacity to access and control high technology processes vital to our  
4 everyday lives.” LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009)  
5 (internal quotation omitted). The majority of the crimes prohibited by the CFAA “involve  
6 accessing computers without authorization or in excess of authorization, and then taking  
7 specified forbidden actions, ranging from obtaining information to damaging a computer  
8 or computer data.” Id. More specifically, “[t]he CFAA . . . imposes liability on anyone  
9 who “intentionally accesses a computer without authorization or exceeds authorized  
10 access, and thereby obtains . . . information from any protected computer.” Mintz v.  
11 Mark Bartelstein & Assocs. Inc., 906 F. Supp. 2d 1017, 1029 (C.D. Cal. 2012) (citing  
12 18 U.S.C. § 1030(a)(2)). The CFAA also imposes liability on whoever “knowingly and  
13 with intent to defraud, accesses a protected computer without authorization, or exceeds  
14 authorized access, and by means of such conduct furthers the intended fraud and  
15 obtains anything of value.” Id. (quoting 18 U.S.C. § 1030(a)(4)). A person who “suffers  
16 damage or loss” as a result of a CFAA violation may bring a civil action against the  
17 violator under five enumerated circumstances. 18 U.S.C. §§ 1030(g), (c)(4)(A)(i)(I)–(V).

18 The Ninth Circuit has stated that “the plain language of the CFAA targets the  
19 unauthorized procurement or alteration of information, not its misuse or  
20 misappropriation.” United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (quoting  
21 Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008)) (citing Orbit One  
22 Commc’ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (“The plain  
23 language of the CFAA support a narrow reading. The CFAA expressly prohibits  
24 improper ‘access’ of computer information.

25 ///

26 ///

27 ///

28 ///

1 It does not prohibit misuse or misappropriation.”); Diamond Power Int’l, Inc. v. Davidson,  
2 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (“[A] violation for exceeding authorized  
3 access occurs where initial access is permitted by the access of certain information is  
4 not permitted.”); Int’l Ass’n of Machinists & Aerospace Workers v. Werver-Masuda, 390  
5 F. Supp. 2d 479, 499 (D. Md. 2005) (“[T]he CFAA, however, do[es] not prohibit the  
6 unauthorized disclosure or use of information, but rather unauthorized access.”). “In  
7 short, the CFAA is an “anti-hacking” statute and not a misappropriation statute.” Hat  
8 World, Inc. v. Kelley, 2:12-CV-001591-LKK, 2012 WL 3283486, at \*5 (E.D. Cal. Aug. 10,  
9 2012) (citing Nosal, 676 F.3d at 860). Thus, in the Ninth Circuit, claims alleging  
10 violation of the CFAA are not preempted by the CUTSA. Accordingly, Defendants’  
11 motion to dismiss Plaintiffs’ CFAA claims on preemption grounds is denied.<sup>4</sup>

### 13 C. Remaining Claims

14  
15 Only Plaintiffs’ claims for breach of contract, trade secret misappropriation, and  
16 violations of the CFAA survive the preemption analysis. See supra. Thus, the Court  
17 must examine whether Plaintiffs have successfully stated a claim for each of these  
18 causes of action. As set forth above, the Court’s inquiry focuses on whether Plaintiffs  
19 have pled facts sufficient to “state a claim to relief that is plausible on its face.” See  
20 Twombly, 550 U.S. at 570.

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

---

28 <sup>4</sup> Whether Plaintiffs successfully stated CFAA claims is a separate matter, discussed infra.

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

**1. Breach of Contract**

Plaintiffs allege that Defendant McCarren breached his Agency Appointment Agreement, and continues to breach his “continuing contractual obligations,” by engaging in the following conduct: (a) soliciting business from Farmers’ present and former policyholders; (b) switching or rewriting business from Farmers to other insurance carriers and servicing such insurance coverage after it was switched away from Farmers; (c) using Farmers’ confidential business information that he acquired while serving as a Farmers agent to the detriment of Farmers; and (d) using Farmers’ confidential business information that he acquired and/or retained. Defendants contend that while the Agency Appointment Agreement states in paragraph H that “for a period of one year . . . the Agent will neither directly or indirectly solicit, accept, or service the insurance business of any policyholder of record in the agencies of this district as of the date of payment or tender of payment,” this provision is invalid because it violates California Business and Professions Code section 16600. Thus, Defendants contend Plaintiffs have not pled facts showing that McCarren’s alleged actions of “soliciting business from Farmers’ present and former policyholders” and “switching or rewriting business from Farmers to other insurance carriers and serving such insurance coverage after it was switched away from Farmers” violates a portion of the contract is valid and enforceable.<sup>5</sup>

California Business & Professions Code section 16600 provides: “Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.” Cal. Bus. & Prof. Code § 16600.

///

---

<sup>5</sup> Defendants do not take issue with Plaintiffs allegations that Defendant McCarren is liable for breach of contract for using Farmers’ confidential business information he acquired while serving as a Farmers agent to the detriment of Farmers, or for using Farmers’ confidential business information that Defendant McCarren acquired and/or retained.

1 “In its recent decision in Edwards v. Arthur Andersen LLP, 44 Cal.4th 937 (2008), the  
2 California Supreme Court confirmed the continued viability and breadth of section  
3 16600. The Court explained that by enacting section 16600, the California legislature  
4 rejected the ‘rule of reasonableness’ applied to non-compete agreements at common  
5 law.” Richmond Techs., Inc. v. Aumtech Bus. Solutions, 11-CV-02460-LHK, 2011 WL  
6 2607158 (N.D. Cal. July 1, 2011). “As a result, ‘[t]oday in California, covenants not to  
7 compete are void, subject to several exceptions,’ and the California Supreme Court  
8 ‘generally condemns noncompetition agreements.’” Id. (quoting Edwards, 44 Cal. 4th at  
9 945-46).

10 But the applicability of section 16600 does not automatically undermine Plaintiff’s  
11 claim. As the Northern District of California explained, “[a]lthough California courts have  
12 consistently ‘condemn[ed]’ agreements that place restraints on the pursuit of a business  
13 or profession,” Richmond Techs., Inc., 2011 WL 2607158, \*18 (quoting Edwards,  
14 44 Cal.4th at 946), “[a]n equally lengthy line of cases has consistently held former  
15 employees may not misappropriate the former employer’s trade secrets to unfairly  
16 compete with the former employer,” id. (quoting Retirement Grp. v. Galante,  
17 176 Cal. App. 4th 1226, 1237 (2009)). Accordingly, “courts have repeatedly held a  
18 former employee may be barred from soliciting existing customers to redirect their  
19 business away from the former employer and to the employee’s new business if the  
20 employee is utilizing trade secret information to solicit those customers.” Id. (quoting  
21 Retirement Group, 176 Cal. App. 4th at 1237) (emphasis in original).

22 “At times, courts have applied this principle to create a ‘trade secret exception’ to  
23 section 16600, pursuant to which a non-compete or non-solicitation clause may be valid  
24 under section 16600 if it is necessary to protect a trade secret.”

25 ///

26 ///

27 ///

28 ///

1 Id. (citing Asset Marketing Sys., Inc. v. Gagnon, 542 F.3d 748, 758 (9th Cir. 2008)  
2 (“Under California law, non-competition agreements are unenforceable unless necessary  
3 to protect an employer's trade secret.”); Edwards, 44 Cal.4th at 946 n.4 (noting but  
4 declining to address the “so-called trade secret exception to section 16600”); Barney v.  
5 Burrow, 558 F. Supp. 2d 1066 (E.D. Cal. 2008)). However, “[o]ther cases suggest that  
6 case law protecting trade secrets does not actually create an exception to Section  
7 16600, but instead enables courts to enjoin the misuse of trade secrets as an  
8 independent wrong, either as a tort or a violation of the Unfair Competition Law.” Id.  
9 (citing Retirement Grp., 176 Cal. App. 4th at 1238; Dowell v. Biosense Webster, Inc.,  
10 179 Cal. App. 4th 564, 577 (2009)).

11       When the trade secret exception applies, a plaintiff may succeed on a breach of  
12 contract claim that alleges that defendants breached the non-solicitation provisions of  
13 the agreement. See Bank of Am., N.A. v. Lee, CV 08-5546 CAS(JWJX), 2008 WL  
14 4351348, at \*6 (C.D. Cal. Sept. 22, 2008) (holding plaintiffs likely to succeed on breach  
15 of contract claim when trade secret exception applied to non-solicitation provision of  
16 contract).

17       Here, Plaintiffs have pled facts adequate to establish a claim for misappropriation  
18 of trade secrets. See infra. Thus, for purposes of the instant motion to dismiss, Plaintiffs  
19 have pled facts sufficient to establish that the non-solicitation clause in the Agency  
20 Appointment Agreement can be enforced against Defendants for the purpose of  
21 protecting Plaintiffs’ alleged trade secrets. Thus, Defendants’ motion to dismiss  
22 Plaintiffs’ breach of contract claim is denied.

## 23 24                   **2. Trade Secret Misappropriation**

25  
26       Plaintiffs argue that Farmers’ customer lists, policyholder records, and proprietary  
27 information constitute protectable trade secrets,” and that Defendants’ actions constitute  
28 misappropriation of those trade secrets. (ECF No. 1 at 16).

1 California has adopted the Uniform Trade Secrets Act (“CUTSA”). MAI Sys.  
2 Corp. v. Peak Computer, Inc., 991 F.2d 511, 520 (9th Cir. 1993), cert. denied, 510 U.S.  
3 1033 (1993). To prevail on their trade secret misappropriation claim, Plaintiffs must  
4 satisfy the CUTSA’s “two primary elements”: “(1) the existence of a trade secret, and  
5 (2) misappropriation of the trade secret.” Acculmage Diagnostics Corp. v. Terarecon,  
6 Inc., 260 F. Supp. 2d 941, 950 (N.D. Cal. 2003) (citing Cal. Civ. Code § 3426.1(b)).

7 Existence of a Trade Secret

8 The CUTSA defines a “trade secret” as “information, including a formula, pattern,  
9 compilation, program, device, method, technique, or process, that . . . [d]erives  
10 independent economic value, actual or potential, from not being generally known to the  
11 public or to other persons who can obtain economic value from its disclosure or use; and  
12 . . . is the subject of efforts that are reasonable under the circumstances to maintain its  
13 secrecy.” Cal. Civ. Code § 3426.1(d).

14 “It is well-established that a customer list may constitute a protectable trade  
15 secret.” Wyndham Resort Dev. Corp. v. Bingham, No. 2:10-cv-01556-GEB-KJM, 2010  
16 WL 2720920, at \*5 (E.D. Cal. July 8, 2010) (quoting Gable-Leigh, Inc. v. N. Am. Miss,  
17 No. CV 01-01019 MMM (SHX), 2001 WL 521695, at \*15 (C.D. Cal. Apr. 13, 2001)); see  
18 also Robert Half Int’l, Inc. v. Murray, No. CV F 07-0799 LJO SMS, 2008 WL 2625857, at  
19 \*4 (E.D. Cal. June 25, 2008) (“A customer list acquired by lengthy and expensive efforts  
20 deserves protection as a trade secret”) (citing MAI Sys., 991 F.2d at 521; Courtesy  
21 Temp. Serv., Inc. v. Camacho, 222 Cal. App. 3d 1278, 1288 (1990)). In Morlife, Inc. v.  
22 Perry, the California Court of Appeal gave a detailed explanation of the circumstances in  
23 which a customer list is entitled to trade secret protection under California law and the  
24 CUTSA:

25 [C]ourts are reluctant to protect customer lists to the extent  
26 they embody information which is “readily available” through  
27 public sources, such as business directories. On the other  
28 hand, where the employer has expended time and effort  
identifying customers with particular needs or characteristics,  
courts will prohibit former employees from using this  
information to capture a share of the market.



1           Such lists are to be distinguished from mere identities and  
2           locations of customers where anyone could easily identify the  
3           entities as potential customers. As a general principle, the  
4           more difficult the information is to obtain, and the more time  
          and resources expended by an employer in gathering it, the  
          more likely a court will find such information constitutes a  
          trade secret.

5           56 Cal. App. 4th 1514, 1521-22 (1997).

6           Here, Plaintiffs' customer lists do not consist solely of the customers' names,  
7           birthdates, and driver's license numbers, which information would be "readily available"  
8           to the public. Rather, the customer lists contain information including names, addresses,  
9           and telephone numbers, as well as "information relating to . . . customers' insurance  
10          needs, such as the type of insurance that the customer needs, the type of cars owned,  
11          the details of their homes and other insured properties, their eligibility for discounts, and  
12          the date their insurance policies expire." (ECF No. 1 at 10.) The information also  
13          includes "social security numbers and other private information about customers, such  
14          as their employment and financial condition." (ECF No. 1 at 10.) Plaintiffs also contend  
15          that compiling their information about the customers' particular characteristics involved  
16          the expenditure of considerable amount of time and resources. Thus, the Court finds  
17          that Plaintiffs have adequately alleged that the customer lists at issue contain  
18          information that is difficult to obtain, and that Plaintiffs devoted time and effort to  
19          gathering this information.

20          As to the CUTSA requirement that the material have "economic value," the  
21          California Court of Appeal stated:

22                 The requirement that a customer list must have economic  
23                 value to qualify as a trade secret has been interpreted to  
24                 mean that the secrecy of this information provides a business  
25                 with a substantial business advantage. In this respect, a  
26                 customer list can be found to have economic value because  
27                 its disclosures would allow a competitor to direct its sales  
               efforts to those customers who have already shown a  
               willingness to use a unique type of service or product as  
               opposed to a list of people who only might be interested. Its  
               use enables the former employee to solicit both more  
               selectively and more effectively.

28          56 Cal. App. 4th at 1522 (internal citations and quotations omitted).

1 In the present case, Plaintiffs allege that the information contained in their  
2 customers lists and on the eCMS database has substantial economic value to Farmers,  
3 and would have economic value if available to Farmers' competitors because "[a]  
4 business priority is securing the annual or semi-annual policy renewals from, along with  
5 any new policies needed by, the roster of Farmers' current insureds. A high retention  
6 rate is essential to Farmers' long-term financial health and growth. Farmers make[s]  
7 every effort to renew policies and a very high percentage of its policyholders renew their  
8 policies with Farmers each year." (ECF No. 1 at 10.) The information that Farmers  
9 retains about their policyholders allows Farmers agents and District Managers "to track  
10 information about and provide services to its policyholders better than those of its  
11 competitors." (ECF No. 1 at 10-11.) Plaintiffs allege that "[c]ompetitors can far more  
12 easily solicit Farmers' insureds to change insurance providers when those competitors  
13 can unfairly access Farmers' trade secret information without having made the  
14 investment of time, labor, and capital that Farmers . . . made to compile and update the  
15 information." (ECF No. 1 at 11.)

16 Furthermore, Plaintiffs have pled facts showing that they took reasonable  
17 measures under the circumstances to maintain the secrecy of their customer lists.  
18 Plaintiffs allege that "Farmers maintains its customer information, including policy  
19 expirations, on a password and user-ID protected system." (ECF No. 1 at 12.)  
20 Furthermore, Plaintiffs allege that "Farmers protects its trade secret customer  
21 information by requiring each employee or agent or District Manager who will access the  
22 data to agree to use Farmers' trade secret customer information only in the course of  
23 their relationship with Farmers, and promise not to divulge Farmers' trade secret  
24 customer information to third parties or to use it in any way detrimental to Farmers." (Id.)  
25 "Farmers also protects its customer information by issuing company policies regarding  
26 access to and preservation of" this information, and maintains "copies of those policies  
27 on the Agency Dashboard." (Id.)

28 ///

1 When Farmers agents access “Farmers’ proprietary system through the Agency  
2 Dashboard, [the agents] agree to abide by an additional and separate ‘Legal  
3 Disclaimer.’” (Id.) This ‘Legal Disclaimer’ informs the agents that the information they  
4 are accessing is “Farmers’ proprietary, confidential[,] and trade secret information.” (Id.)  
5 Finally, Plaintiffs allege that “Farmers also periodically remind[s] agents of [Farmers’]  
6 confidentiality policies via bulletins and other communications.” (Id.)

7 These allegations are adequate to show that the relevant trade secrets are  
8 “subject of efforts that are reasonable under the circumstances to maintain [their]  
9 secrecy,” as required by the CUTSA. See Cal. Civ. Code § 3426.1(d).

10 Plaintiffs have adequately plead facts showing that the Confidential Policyholder  
11 Information is “information” that “[d]erives independent economic value, actual or  
12 potential, from not being generally known to the public or to other persons who can  
13 obtain economic value from its disclosure or use; and . . . is the subject of efforts that are  
14 reasonable under the circumstances to maintain its secrecy.” Cal. Civ. Code  
15 § 3426.1(d). As such, Plaintiffs’ have sufficiently established, for purposes of the instant  
16 motion to dismiss, that their customer lists constitute a protectable trade secret under the  
17 CUTSA.

18 The next issue is whether Plaintiffs have adequately pled the “misappropriation”  
19 prong of the CUTSA’s test. The CUTSA defines “misappropriation” as:

20 (1) Acquisition of a trade secret of another by a person who  
21 knows or has reason to know that the trade secret was  
acquired by improper means; or

22 (2) Disclosure or use of a trade secret of another without  
23 express or implied consent by a person who:

24 (A) Used improper means to acquire knowledge of the trade  
secret; or

25 (B) At the time of disclosure or use, knew or had reason to  
26 know that his or her knowledge of the trade secret was:

27 (i) Derived from or through a person who had utilized  
improper means to acquire it;

28 ///

1 (ii) Acquired under circumstances giving rise to a duty to  
2 maintain its secrecy or limit its use; or

3 (iii) Derived from or through a person who owed a duty to the  
4 person seeking relief to maintain its secrecy or limit its use;

5 . . . .

6 Cal. Civ. Code § 3426.1(b). Here, Plaintiffs allege that Defendants misappropriated  
7 Plaintiffs' trade secrets by "retaining or utilizing Farmers' Proprietary Information for the  
8 purpose of soliciting, directing, or advising Farmers' policyholders to switch their  
9 coverage away from Farmers and to Steele's competing business." (ECF No. 1 at 17.)  
10 Accordingly, Plaintiffs have adequately pled that Defendants misappropriated Farmers'  
11 trade secrets.

12 Defendants argue that Plaintiffs fail to allege that Plaintiffs actually own the trade  
13 secrets at issue, and therefore Plaintiffs fail to state a claim for trade secret  
14 misappropriation. (ECF No. 12 at 23 (citing Cytodyn, Inc. v. Amerimmune  
15 Pharmaceuticals, Inc., 160 Cal. App. 4th 288, 296 (2008)). However, as Defendants  
16 point out, Plaintiffs repeatedly allege that the trade secrets were compiled by Farmers,  
17 protected by Farmers, used by Farmers, subject to Farmers' best efforts to keep them  
18 secret, and are valuable to Farmers. (ECF No. 1 at 10-12.) The trade secrets are  
19 referred to in the complaint as "Farmers' trade secrets." (ECF No. 1 at 11 ("Farmers  
20 engages in reasonable measures to preserve its trade secret Confidential Policyholder  
21 Information . . . ."), 12 ("Farmers protects its trade secret customer information . . . .").)  
22 These allegations are sufficient to plead that Farmers owns the trade secrets at issue.<sup>6</sup>

23 Accordingly, Plaintiffs have adequately pled their claim for trade secret  
24 misappropriation under the CUTSA and Defendants' motion to dismiss this claim is  
25 denied.

26 ///

---

27 <sup>6</sup> Plaintiffs offer to amend the Complaint to include the specific allegation that Farmers owns the  
28 trade secrets at issue. While such an allegation is not necessary, as Plaintiffs' allegations are sufficient to  
show Farmers' ownership of the alleged trade secrets, Plaintiffs are nonetheless free to amend their  
Complaint to include such an allegation.

1                                   **3.     CFAA**

2

3           Plaintiffs allege that Defendants violated two sections of the CFAA. First,

4 Plaintiffs allege Defendants violated 18 USC § 1030(a)(2)(C), “which provides for

5 criminal penalties to be imposed on a person who: intentionally accesses a computer

6 without authorization or exceeds authorized access, and thereby obtains . . . information

7 from any protected computer . . . .” Brekka, 581 F.3d at 1131 (quoting 18 U.S.C.

8 § 1030(a)(2)(C)). Plaintiffs also allege Defendants violated 18 U.S.C. § 1030(a)(4).

9 Section 1030(a)(4) provides for criminal penalties to be imposed on a person who

10 “knowingly and with intent to defraud, accesses a protected computer without

11 authorization, or exceeds authorized access, and by means of such conduct furthers the

12 intended fraud and obtains anything of value, unless the object of the fraud and the thing

13 obtained consists only of the use of the computer and the value of such use is not more

14 than \$5,000 in any 1-year period.” 18 U.S.C. § 1030(a)(4).

15           Plaintiffs brought suit under subsection (g) of the CFAA, which provides a private

16 right of action for individuals injured by such crimes. See 18 U.S.C. § 1030(g).

17 Specifically, § 1030(g) provides that:

18                                   Any person who suffers damage or loss by reason of a

19 violation of this section may maintain a civil action against the

20 violator to obtain compensatory damages and injunctive relief

21 or other equitable relief. A civil action for a violation of this

22 section may be brought only if the conduct involves 1 of the

23 factors set forth in clause (I), (ii), (iii), (iv), or (v) of subsection

24 (a)(5)(B).

25 Id. “Thus, a private plaintiff must prove that the defendant violated one of the provisions

26 of § 1030(a)(1)-(7), and that the violation involved one of the factors listed in

27 § 1030(a)(5)(B).” Brekka, 581 F.3d at 1131. In the present case, Plaintiffs allege that

28 Defendants’ conduct involved the factor described in subsection (a)(5)(B)(i), which

proscribes conduct that causes “loss to 1 or more persons during any 1–year period . . .

aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(a)(5)(B)(i).

///

1           Therefore, to successfully bring an action under § 1030(g) based on a violation of  
2 § 1030(a)(4), Plaintiffs must show that Defendants: (1) accessed a “protected computer,”  
3 (2) without authorization or exceeding such authorization that was granted,  
4 (3) “knowingly” and with “intent to defraud,” and thereby (4) “further[ed] the intended  
5 fraud and obtain[ed] anything of value,” causing (5) a loss to one or more persons during  
6 any one-year period aggregating at least \$5,000 in value. Brekka, 581 F.3d 1127, 1132  
7 (9th Cir. 2009) (quoting 18 U.S.C. § 1030(a)) (citing P.C. Yonkers, Inc. v. Celebrations  
8 the Party and Seasonal Superstore, LLC, 428 F.3d 504, 508 (3d. Cir. 2005); Theofel v.  
9 Farey–Jones, 359 F.3d 1066, 1078 (9th Cir. 2004)). To successfully bring an action  
10 under § 1030(g) for a violation of § 1030(a)(2)(C), Plaintiffs must allege facts sufficient to  
11 show that Defendants: “(1) intentionally accessed a computer, (2) without authorization  
12 or exceeding authorized access, and . . . (3) thereby obtained information (4) from any  
13 protected computer . . . , and that (5) there was loss to one or more persons during any  
14 one-year period aggregating at least \$5,000 in value.” Brekka, 581 F.3d at 1132.

15           Defendants move to dismiss these causes of action on two grounds. First,  
16 Defendants argue that Plaintiffs allege neither the requisite lack of authority to access  
17 the computer(s) at issue, nor do Plaintiffs allege the requisite unauthorized access.  
18 (ECF No. 12 at 18.) Second, Defendants contend that Plaintiffs do not allege the  
19 damages or loss required to state a claim pursuant to the CFAA. (ECF No. 12 at 20.)

#### 20           Access Without Authorization/ Exceeding Authorized Access

21           The second prong of both §§ 1030(a)(2)(C) and (a)(4) requires that the defendant  
22 either “intentionally accesses a computer without authorization,” or that the defendant  
23 “exceeds [his or her] authorized access.” 18 U.S.C. §§ 1030(a)(2)(C), (a)(4). In Brekka,  
24 the Ninth Circuit stated that “an individual who is authorized to use a computer for certain  
25 purposes but goes beyond those limitations is considered by the CFAA as someone who  
26 has ‘exceed[ed] authorized access.’” 581 F.3d at 1133. By contrast, “a person who  
27 uses a computer ‘without authorization’ has no rights, limited or otherwise, to access the  
28 computer in question.” Id.

1 Thus, in Brekka, the Ninth Circuit found that “when an employer authorizes an employee  
2 to use a company computer subject to certain limitations, the employee remains  
3 authorized to use the computer even if the employee violates those limitations. It is the  
4 employer’s decision to allow or to terminate an employee’s authorization to access a  
5 computer that determines whether the employee is with or ‘without authorization.’” Id.

6 In United States v. Nosal, a case decided three years after Brekka, the Ninth  
7 Circuit clarified the scope of the CFAA and the meaning of the term “exceeds authorized  
8 access.” 676 F.3d 854. The facts of Nosal are remarkably similar to those alleged in the  
9 present case. Defendant David Nosal worked for an executive search firm. 676 F.3d at  
10 856. “Shortly after [Nosal] left the company, he convinced some of his former  
11 colleagues who were still working [there] to help him start a competing business.” Id.  
12 Just as Plaintiffs allege here, “[t]he employees used their log-in credentials to download  
13 source lists, names and contact information from a confidential database on the  
14 company’s computer, and then transferred the information to Nosal.” Id. “The  
15 employees were authorized to access the database, but [the company] had a policy that  
16 forbade disclosing confidential information.” Id. The government brought charges under  
17 the CFAA against Nosal for “aiding and abetting the [company’s] employees in  
18 ‘exceeding their authorized access’ with intent to defraud.” Id.

19 The Ninth Circuit rejected the government’s argument that the CFAA’s phrase  
20 “exceeds authorized access” “could refer to someone who has unrestricted physical  
21 access to a computer, but is limited in the use to which he can put the information.” Id.  
22 at 867. The Ninth Circuit found that the “government’s interpretation would transform the  
23 CFAA from an anti-hacking statute into an expansive misappropriation statute.” Id.  
24 Instead, the court “recognize[d] that the plain language of the CFAA ‘targets the  
25 unauthorized procurement or alteration of information, not its misuse or  
26 misappropriation.’”

27 ///

28 ///

1 Id. at 863 (quoting Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz.  
2 2008)) (internal alterations omitted) (citing Orbit One Commc'ns, Inc. v. Numerex Corp.,  
3 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Diamond Power Int'l, Inc. v. Davidson,  
4 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); Int'l Ass'n of Machinists & Aerospace  
5 Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 (D. Md. 2005)). The Ninth Circuit  
6 thus held that the phrase “‘exceeds authorized access’ in the CFAA is limited to  
7 violations of restrictions on access to information, and not restrictions on its use.” Id. at  
8 863–64 (emphasis in original). “Because Nosal’s accomplices had permission to access  
9 the company database and obtain the information contained within,” the court found that  
10 “the government’s charges fail[ed] to meet the element of ‘without authorization, or  
11 exceeds authorized access’ under 18 U.S.C. § 1030(a)(4).” Id. at 864.

12 Plaintiffs allege that Defendants accessed Plaintiffs’ computers “without  
13 authorization.” (ECF No. 1 at 21, 22.) Plaintiffs also make the blanket allegation that  
14 “Defendants were not authorized to access the Agency Dashboard and eCMS.” (ECF  
15 No. 1 at 21.) The Court must address these allegations as to each Defendant.

16 First, as to Defendant McCarren, Plaintiffs also specifically allege that he was a  
17 Farmers agent (ECF No. 1 at 12) and that the Agency Dashboard and eCMS are tools  
18 for Farmers agents (ECF No. 1 at 10-12). Thus, Defendant McCarren the Court cannot  
19 properly characterize Defendant McCarren as “a person who . . . has no rights, limited or  
20 otherwise, to access the computer in question.” See Brekka, 581 F.3d at 1133.

21 Accordingly, the facts as pled do not show that Defendant McCarren accessed Plaintiffs’  
22 computers “without authorization.” Furthermore, because Plaintiffs’ allegations reveal  
23 that Defendant McCarren, as an agent, had permission to access Farmers’ confidential  
24 proprietary information through eCMS and the Agency Dashboard, Defendant McCarren  
25 did not “exceed authorized access” by accessing such information, although he may  
26 have used such information for an improper purpose. See Nosal, 676 F.3d at 863-64.  
27 Accordingly, Plaintiffs have failed to state facts sufficient to allege the second prong of  
28 either § 1030(a)(2)(C) or § 1030(a)(4) against Defendant McCarren.



1 Plaintiffs' seventh and eighth causes of action against Defendant McCarren are  
2 therefore dismissed.

3 As to Defendants Steele and Blalock, Plaintiffs allege that each was a District  
4 Manager for Farmers. (ECF No. 1 at 12.) Plaintiffs allege that the "Agency Dashboard  
5 . . . allows Farmers insurance agents, District Managers, and employees to track  
6 information about and provide services to its policyholders," and that "eCMS is a tool  
7 used by authorized insurance agents and District Managers to Farmers Policyholders."  
8 (ECF No. 1 at 10-11.) Thus, Plaintiffs' allegations reveal that Defendants Steele and  
9 Blalock were authorized to access the Agency Dashboard and eCMS while these  
10 Defendants were District Managers. However, Plaintiffs contradict this allegation by later  
11 stating that "Defendants were not authorized to access the Agency Dashboard and  
12 eCMS" and that "Defendants have intentionally and without authorization accessed,  
13 caused others to access, and/or have utilized others' user ID and password combination  
14 to access the Agency Dashboard or eCMS . . . ." (ECF No. 1 at 21.) Thus, as with  
15 Defendant McCarren, Plaintiffs' specific factual pleadings as to Defendants Blalock and  
16 Steele show that these Defendants were indeed authorized by Farmers to access  
17 Plaintiffs' computers. As such, Plaintiffs fail to plead facts sufficient to show that  
18 Defendants Steele and Blalock were "without authorization" to access those computers.  
19 Furthermore, Plaintiffs' allegations make clear that Defendants Steele and Blalock had  
20 the authority to access eCMS and the Agency Dashboard on the computers at issue,  
21 and therefore did not "exceed [their] authorized access" under the CFAA. Accordingly,  
22 Plaintiffs fail to state a claim against Defendants Steele and Blalock for violations of the  
23 CFAA, and Defendants' motion to dismiss these claims is granted.

24 Next, as to Defendant Perkins, Plaintiffs clearly allege that she "did not have  
25 permission to . . . access Farmers' computer systems." (ECF No. 1 at 14.) This  
26 allegation is sufficient to meet the second prong of the CFAA analysis, as it sufficiently  
27 states that Defendant Perkins was "a person who . . . [had] no rights, limited or  
28 otherwise, to access the computer in question." See Brekka, 581 F.3d at 1133.

1 As to Defendant Henton, the first question is whether he accessed the  
2 computer(s) at issue “without authorization.” Plaintiffs allege that Defendant Henton  
3 “worked in his father’s office,” but was not a Farmers agent, and that Defendant Henton  
4 gave his “wife and daughter unauthorized access to Farmers’ computer system  
5 apparently for the purpose of accessing information regarding Farmers’ policyholders.”  
6 (ECF No. 1 at 14). Plaintiffs also allege that “[a]t all times relevant to this Complaint,  
7 Defendants were not authorized to access the Agency Dashboard and eCMS.” (ECF  
8 No. 1 at 21.) However, nowhere do Plaintiffs allege that Defendant Henton was not  
9 authorized to access the physical computer(s) in question. Thus, Plaintiffs fail to plead  
10 facts sufficient to show that Defendant Henton was a person “without authorization”  
11 under the CFAA. See Brekka, 581 F.3d at 1133. Thus, the next question is whether  
12 Defendant Henton “exceeded [his] authorized access” under the CFAA. Plaintiffs allege  
13 that “Defendants have intentionally and without authorization accessed . . . , and/or have  
14 utilized others’ user ID and password combination to access the Agency Dashboard or  
15 eCMS . . . .” (ECF No. 1 at 21.) As the term is used in the Complaint, “Defendants”  
16 includes Defendant Henton and thus this allegation applies to Defendant Henton. As  
17 such, Plaintiffs allege that Defendant Henton intentionally and without authorization  
18 accessed Farmers’ Agency Dashboard and eCMS. Viewed in the light most favorable to  
19 Plaintiffs, these allegations reveal that Defendant Henton “violat[ed] . . . restrictions on  
20 access to information,” see Nosal, 676 F.3d at 863-64, and therefore “exceeded his  
21 authorized access.” Plaintiffs’ allegations as to Defendant Henton therefore meet the  
22 second prong of the analysis for §§ 1030(a)(2)(C) and (a)(4).

23 Damages/ Loss

24 Defendants contend that Plaintiffs have not alleged any facts to support the “loss”  
25 element of the CFAA claims. Pursuant to §§ 1030(a)(2)(C) and (a)(4), Plaintiffs must  
26 allege facts showing that Defendants caused “a loss to one or more persons during any  
27 one-year period aggregating at least \$5,000 in value.” Brekka, 581 F.3d at 1132.

28 ///

1 The CFAA defines “loss” as “any reasonable cost to any victim, including the cost of  
2 responding to an offense, conducting a damage assessment, and restoring the data,  
3 program, system, or information to its condition prior to the offense, and any revenue  
4 lost, cost incurred, or other consequential damages incurred because of interruption of  
5 service . . . .” 18 U.S.C. § 1030(e)(11). “Loss,’ therefore, means two things: ‘any  
6 reasonable cost to the victim,’ and lost revenue or other damages incurred as a result of  
7 an interruption of service.” AtPac, Inc. v. Aptitude Solutions, 730 F. Supp. 2d 1174,  
8 1184 (E.D. Cal. 2010). The CFAA defines “damage” as “any impairment to the integrity  
9 or availability of data, a program, a system, or information . . . .” Id. § 1030(e)(8).

10 To allege a loss under the CFAA, “plaintiffs must identify impairment of or damage  
11 to the computer system that was accessed without authorization.” AtPac, Inc.,  
12 730 F. Supp. 2d at 1184 (quoting Doyle v. Taylor, No. 09-158, 2010 WL 2163521, at \*2  
13 (E.D. Wash. May 24, 2010) (holding that where plaintiff alleged defendant accessed  
14 plaintiff’s USB thumb drive and retrieved a sealed document, “[p]laintiff would have to  
15 show that the thumb drive itself was somehow damaged or impaired by Defendant’s act  
16 of accessing the drive.”)). “Cognizable costs also include the costs associated with  
17 assessing a hacked system for damage [and] upgrading a system’s defenses to prevent  
18 future unauthorized access.” Id. (citing Doyle, 2010 WL 2163521 at \*3); see also  
19 SuccessFactors, Inc. v. Softscape, Inc., 544 F. Supp. 2d 975 (N.D. Cal. 2008) (“[W]here  
20 the offense involves unauthorized access and the use of protected information . . . the  
21 cost of discovering the identity of the offender or the method by which the offender  
22 accessed the protected information [is] part of the loss for purposes of the CFAA.”).

23 Indeed, a number of courts have noted that “costs not related to computer  
24 impairment or computer damages are not compensable under the CFAA.”

25 ///

26 ///

27 ///

28 ///

1 SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 721 (N.D. Ill. 2009) (citing Civic Ctr.  
2 Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005));  
3 see also Nexans Wires S.A. v. Sark–USA, Inc., 166 F. App'x 559, 562–63 (2d Cir. 2006);  
4 Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l Inc., No. 07 C 5902, 2009  
5 WL 743215, at \*4 (N.D. Ill. Mar.19, 2009); Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314,  
6 320 (D. Conn. 2008)). In SKF USA, Inc., the plaintiff “only alleged that its business was  
7 harmed by [the] [d]efendants’ alleged violations of the [CFAA].” 636 F. Supp. 2d at 721.  
8 The court observed that “[s]uch economic losses are better addressed . . . under state  
9 contract and trade secrets law,” and held that because the plaintiff “did not plead that it  
10 suffered any costs related to its computers in responding to [the] [d]efendants’ actions  
11 nor that it suffered any service interruptions, [the plaintiff] . . . failed to show any loss  
12 redressable under the CFAA.” Id. at 721-22.

13 Here, the Court agrees that “[c]osts not related to computer impairment or  
14 computer damages are not compensable under the CFAA.” Id. at 721. As such,  
15 Plaintiffs have failed to allege losses that satisfy the CFAA’s definition of “loss.” Rather,  
16 Plaintiffs allege that they have suffered “substantial damage and harm in the form of lost  
17 present and future business revenue.” (ECF No. 1 at 22, 23.) These allegations are not  
18 sufficient to allege a “loss” under the CFAA. Accordingly, Defendants’ motion to dismiss  
19 Plaintiffs’ seventh and eighth causes of action is granted as to all defendants.

## 20 21 **CONCLUSION**

22  
23 For the reasons set forth above, it is hereby ordered that:

- 24 1. Defendants’ Motion to Dismiss Plaintiffs’ first and second claims is  
25 DENIED. (ECF No. 12.)
- 26 2. Defendants’ Motion to Dismiss Plaintiffs’ third, fourth, fifth, sixth, seventh,  
27 eighth and ninth claims is GRANTED. (ECF No. 12.) These causes of  
28 action are DISMISSED WITHOUT PREJUDICE as to all Defendants.

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

3. Not later than twenty (20) days following the date of this Memorandum and Order is electronically filed, Plaintiffs may file an amended complaint. If no amended complaint is filed within said twenty (20) day period, without further notice to the parties, the causes of action dismissed by virtue of this Memorandum and Order will be dismissed with prejudice.

IT IS SO ORDERED.

Dated: July 23, 2013

  
MORRISON C. ENGLAND, JR., CHIEF JUDGE  
UNITED STATES DISTRICT COURT