

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
NORTHERN DISTRICT OF CALIFORNIA

SUNPOWER CORPORATION,
Plaintiff,
v.
SUNEDISON, INC., et al.,
Defendants.

Case No. [15-cv-02462-WHO](#)

**ORDER GRANTING MOTION TO
DISMISS WITH LEAVE TO AMEND**

Re: Dkt. No. 20

INTRODUCTION

The central issue in defendants SunEdison, Inc., Shane Messer, Kendall Fong, and Vikas Desai’s motion to dismiss is whether current employees violate the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, if they breach their employer’s computer use policies while accessing files that they were authorized to use. Because the CFAA is an anti-hacking statute, not a misappropriation statute, I GRANT the motion to dismiss because Messer and Fong accessed the disputed information with authorization while they were SunPower’s employees. Lacking another federal claim, SunPower’s complaint is DISMISSED for lack of subject matter jurisdiction under 29 U.S.C. § 1331.

BACKGROUND

I accept the allegations pleaded in the complaint as true for purposes of SunEdison’s motion to dismiss. SunPower is an energy services provider that manufactures, installs, and distributes solar panel systems for residential and commercial markets. Messer and Fong were once employed by SunPower as Area Sales Manager and Senior Director of Global Brand, respectively. SunPower asserts that Messer and Fong, prior to leaving SunPower, accessed thousands of its files and likely copied them onto one or more devices such as a personal Universal Serial Bus (“USB”) drive or other non-SunPower owned device. After their departures from SunPower, they began to work for SunEdison.

SunPower identifies two specific instances of illegal copying. It contends that Messer

1 accessed and copied over 4,300 files from a SunPower computer or server during a fifteen-minute
2 span on July 30, 2011. In the weeks preceding his departure, Fong allegedly accessed over 9,500
3 SunPower files over an 80-minute span. The accessed files purportedly contained SunPower’s
4 highly confidential information and trade secrets.

5 SunPower also alleges that Desai, a former Vice President at SunPower, encouraged Fong
6 and Messer to leave SunPower and to share SunPower’s confidential information with SunEdison,
7 where Desai was employed as the company’s Chief Executive Officer. SunPower believes that
8 SunEdison has used and continues to use SunPower’s proprietary information for its own benefit
9 and to the detriment of SunPower.

10 SunPower contends that Messer and Fong’s actions violated SunPower’s computer use
11 policies that prohibited its employees from connecting any non-SunPower devices to SunPower’s
12 network or from using personal USB drives for file storage or transfer. It also claims that Messer
13 and Fong violated their employment confidentiality agreement by transferring the allegedly stolen
14 SunPower files to SunEdison. These agreements obliged Messer and Fong to keep SunPower’s
15 information confidential and to protect it from outside disclosures or use for others’ benefit.

16 SunPower brings fourteen causes of action: (1) violation of the CFAA; (2) trade secret
17 misappropriation under the California Uniform Trade Secrets Act (“CUTSA”); (3) breach of
18 contract; (4) breach of confidence; (5) conversion; (6) trespass to chattels; (7) interference with
19 prospective business advantage; (8) breach of implied covenant of good faith and fair dealing; (9)
20 tortious interference with contractual relationship; (10) induced breach of contract; (11)
21 conspiracy to breach contract; (12) breach of duty of loyalty; (13) unfair competition, and (14)
22 statutory unfair competition. Thirteen of SunPower’s fourteen causes of action arise under state
23 law. Its only federal cause of action is based on the purported violation of the CFAA. Defendants
24 move to dismiss the first, fourth, fifth, sixth, seventh, ninth, tenth, eleventh, twelfth, thirteenth, and
25 fourteenth causes of action for failure to state a claim upon which relief may be granted under
26 Federal Rule of Civil Procedure 12(b)(6). I heard argument on September 9, 2015.

27 **LEGAL STANDARD**

28 Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint

1 if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion to
2 dismiss, the plaintiff must allege “enough facts to state a claim to relief that is plausible on its
3 face.” *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007). A claim is facially plausible
4 when the plaintiff pleads facts that “allow the court to draw the reasonable inference that the
5 defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)
6 (citation omitted). There must be “more than a sheer possibility that a defendant has acted
7 unlawfully.” *Id.* While courts do not require “heightened fact pleading of specifics,” a plaintiff
8 must allege facts sufficient to “raise a right to relief above the speculative level.” *Twombly*, 550
9 U.S. at 555, 570.

10 In deciding whether the plaintiff has stated a claim upon which relief can be granted, the
11 Court accepts the plaintiff’s allegations as true and draws all reasonable inferences in favor of the
12 plaintiff. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court
13 is not required to accept as true “allegations that are merely conclusory, unwarranted deductions of
14 fact, or unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir.
15 2008).

16 If the court dismisses the complaint, it “should grant leave to amend even if no request to
17 amend the pleading was made, unless it determines that the pleading could not possibly be cured
18 by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000).

19 **DISCUSSION**

20 Defendants raise three arguments in their motion to dismiss: (i) SunPower fails to state a
21 claim under CFAA; (ii) CUTSA preempts all non-contractual claims based on misappropriation of
22 confidential information; and (iii) SunPower fails to state a claim for interference with business
23 advantage. Because I find that SunPower’s complaint fails to state a claim under CFAA, its only
24 federal cause of action, I will not address the state law claims. If there is no federal claim, I will
25 not exercise supplemental jurisdiction.

26 The CFAA prohibits various computer-related crimes, including accessing a computer
27 without authorization or exceeding authorized access. 18 U.S.C. § 1030(a)(1). It was enacted in
28 1984 to “target hackers who accessed computers to steal information or to disrupt or destroy

1 computer functionality, as well as criminals who possessed the capacity to access and control high
2 technology processes vital to our everyday lives.” See *LVRC Holdings LLC v. Brekka*, 581 F.3d
3 1127, 1130 (9th Cir. 2009)(internal quotations and citations omitted). “The CFAA prohibits a
4 number of different computer crimes, the majority of which involve accessing computers without
5 authorization or in excess of authorization, and then taking specified forbidden actions, ranging
6 from obtaining information to damaging a computer or computer data.” *Id.* at 1131.

7 SunPower alleges that the defendants’ behavior violated 18 U.S.C. § 1030(a)(2)(c), (a)(4)
8 and (g). Compl. ¶ 1. (Dkt. No. 33). Section 1030(a)(2)(c) provides for criminal penalties when a
9 person “[i]ntentionally accesses a computer without authorization or exceeds authorized access,
10 and thereby obtains...information from any protected computer.” Section 1030(a)(4) provides for
11 penalties if a person:

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

18 18 U.S.C. § 1030(a)(4).

19 In addition to criminal penalties, the CFAA creates a private right of action for “[a]ny
20 person who suffers damage or loss by reason of a violation” of the statute. 18 U.S.C. § 1030(g).
21 However, a claim may only be brought if the conduct involves the factors delineated in subclause
22 (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). *Id.* Therefore, to bring a successful CFAA
23 claim based on this subsection, a plaintiff must show:

- 24 (I) loss to 1 or more persons during any 1-year period (and, for
25 purposes of an investigation, prosecution, or other proceeding
26 brought by the United States only, loss resulting from a related
27 course of conduct affecting 1 or more other protected computers)
28 aggregating at least \$5,000 in value;
(II) the modification or impairment, or potential modification or
impairment, of the medical examination, diagnosis, treatment, or
care of 1 or more individuals;
(III) physical injury to any person;
(IV) a threat to public health or safety;
(V) damage affecting a computer used by or for an entity of the
United States Government in furtherance of the administration of
justice, national defense, or national security.

1 18 U.S.C. § 1030(c)(4)(A)(i).¹

2 A plausible claim under either 18 U.S.C. § 1030(a)(2)(c) or (a)(4) requires SunPower to
3 allege that the defendants acted “without authorization” or by “exceed[ing] authorized access.”
4 The CFAA defines “exceeds authorized access” as “to access a computer with authorization and to
5 use such access to obtain or alter information in the computer that the accesser is not entitled so to
6 obtain or alter.” 18 U.S.C. § 1030(e)(6). The term “without authorization” is not defined within
7 the statute.

8 The Ninth Circuit has determined that a person uses a computer “without authorization”
9 when “the person has not received permission to use the computer for any purpose (such as when
10 a hacker accesses someone's computer without any permission), or when the employer has
11 rescinded permission to access the computer and the defendant uses the computer anyway.”
12 *Brekka*, 581 F.3d at 1135. Specifically, the Ninth Circuit has articulated a “sensible interpretation
13 of §§ 1030(a)(2) and (4), which gives effect to both the phrase ‘without authorization’ and the
14 phrase ‘exceeds authorized access’: a person who ‘intentionally accesses a computer without
15 authorization’ accesses a computer without any permission at all, while a person who ‘exceeds
16 authorized access’ has permission to access the computer, but accesses information on the
17 computer that the person is not entitled to access.” *Brekka*, 581 F.3d at 1133 (internal citations
18 omitted).

19 The Ninth Circuit has held that the plain language of the CFAA targets “the unauthorized
20 procurement or alteration of information, not its misuse or misappropriation.” *United States v.*
21 *Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (internal quotation and citations omitted). Specifically,
22 “the phrase ‘exceeds authorized access’ in the CFAA does not extend to violations of use
23 restrictions.” *Id.* The Ninth Circuit’s narrow reading intentionally focused the statute’s application
24 to its purpose of punishing hackers and not misappropriating trade secrets. *Id.* at 863. Subsequent
25 cases have similarly limited their interpretation of the CFAA. *See, e.g., Koninklijke Philips N.V. v.*

26 _____
27 ¹ Although SunPower does not allege which of the specific 18 U.S.C. § 1030(c)(4)(A)(i) factors is
28 triggered by SunEdison’s behavior, it does claim that its losses and damages amount to over
\$5,000 over a one year period. Comp. ¶ 79. This is sufficient to implicate 18 U.S.C. §
1030(c)(4)(A)(i)(I).

1 *Elec-Tech In'l Co.*, 14-cv-02737-BLF, 2015 WL 1289984, at *4 (N.D. Cal. Mar. 20, 2015)
2 (following Ninth Circuit precedent in *Nosal* and dismissing plaintiff's CFAA claim based in part
3 on the fact that the statute targets hacking, not trade secret misappropriation); *Quad Knopf, Inc. v.*
4 *S. Valley Biology Consulting, LLC*, 13-cv-01262, 2014 WL 1333999, at *3 (E.D. Cal. Apr. 3,
5 2014) (same); *Synopsys, Inc. v. ATopTech, Inc.*, 13-cv-02965 SC, 2013 WL 5770542, at *9 (N.D.
6 Cal. Oct. 24, 2013) (same).

7 Here, SunPower does not allege that Fong and Messer were not authorized to access a
8 computer or certain information. Instead, SunPower claims that Fong and Messer violated the
9 CFAA by breaching SunPower's computer use policies when they connected USB drives or other
10 non-SunPower owned equipment to SunPower's network, copied files onto these devices, and
11 stored them on an unauthorized device.² Comp. ¶¶ 30 - 45. To support its argument, SunPower
12 relies on *Brekka* for the proposition that the phrase "exceeds authorized access" includes
13 violations of employer-placed limitations on use. Opp. at 6. (Dkt. No. 26) .

14 I do not read *Brekka* in that manner. In *Brekka*, the employer alleged that one of its former
15 employees, Christopher Brekka, violated the CFAA by accessing the employer's computer
16 "without authorization" and in excess of authorization both while Brekka was employed and after
17 he left. 581 F.3d at 1129. The Ninth Circuit affirmed summary judgment in favor of Brekka and
18 the other defendants. It found, in part, that Brekka was authorized to use his employer's computer
19 while he was employed and therefore downloading his employer's files and emailing the
20 documents to his personal email did not violate the CFAA. *Id.* at 1137. The court explicitly held
21 that "for purposes of the CFAA, when an employer authorizes an employee to use a computer
22

23 ² For the first time at oral argument, SunPower pointed to two specific provisions of its computer
24 use policies that it alleges are access restrictions. See SunPower Ex. F at 1.1, SunPower Ex. C at
25 6.2.2. It argued that it is limiting its claims only to violations of these provisions. The extent to
26 which these isolated uses of the word "access" would qualify these subsections as access
27 restrictions defined by *Nosal* and *Brekka* is, at best, unclear and should have been briefed.
28 SunPower's policies do not seem to be consistent in their terminology. On the very same pages
where SunPower's alleged access restrictions are located, the company employs the word "use" in
related subsections. See SunPower Ex. C at 1.1 (clarifying that the purpose and scope of this
chapter of SunPower's policy is to avoid damages resulting from "[I]nadvertent or intentional
misuse"), SunPower Ex. F at 6.1.1 (prohibiting the "use" of USB drives for file storage or
transfer). Simply using one word or another does not control the categorization of the restriction.

1 subject to certain limitations, the employee remains authorized to use the computer even if the
2 employee violates these limitations.” *Id.* at 1133.

3 Under *Brekka*, a CFAA claim hinges not on the use of the information but on whether or
4 not the employee is authorized to access the information in the first place. *Id.*, see also *Nosal*, 676
5 F.3d at 857 (rejecting the government’s suggestion that unauthorized access encompasses
6 situations involving limitations on use when an employee has unrestricted physical access to the
7 information). Accordingly, it held that *Brekka* did not violate the CFAA because “there is no
8 dispute that *Brekka* was given permission to access [the defendant’s] computer.” *Brekka*,
9 581F.3d, at 1135. Under *Brekka*, a prohibited action, such as copying or transferring the accessed
10 files onto a USB, does not by itself transform an employee’s access from authorized to
11 unauthorized. SunPower’s contention that *Brekka* holds otherwise is incorrect.

12 SunPower’s assertion that subsequent cases have interpreted *Brekka* to allow violations of
13 employer-placed non-technical restrictions to form the basis of “unauthorized access” ignores the
14 important differences between those cases and its own. *Opp.* at 6. SunPower relies on two cases
15 involving former employees who exceeded their authorized access by accessing information after
16 their employment ended. See *NetApp, Inc. v. Nimble Storage, Inc.* 41 F. Supp. 3d 816 (N.D. Cal.
17 2014); *Weingand v. Harland Fin. Solutions, Inc.*, 11-cv-03109-EMC, 2012 WL 2327660 (N.D.
18 Cal. June 19, 2012). The key to both courts’ analyses was timing-- the employees had gained
19 accessed to their previous employers’ networks *after* their access to those networks had been
20 revoked. *NetApp*, 41 F. Supp. 3d, at 831-32 (holding that the Ninth Circuit has not precluded
21 applying CFAA to situations where an individual access a former employer’s network); *Weingard*,
22 2012 WL 2327660, at *3 (same). Because Messer and Fong were current employees at the time of
23 the alleged access, their access was not unauthorized in the same manner as the plaintiffs in
24 *NetApp* and *Weingand*.

25 SunPower’s argument that Messer and Fond violated “technological barriers” by
26 physically plugging in USB drives or other non-SunPower equipment into SunPower’s computer
27 is similarly unpersuasive. SunPower cites to an inapposite example given by the Ninth Circuit in
28 *Nosal*. An employer keeps information in a separate database that can be viewed on a computer

1 screen but not copied or downloaded. If the employee circumvents the employer’s security
2 measures, copies information on to a USB drive and takes it out of the building, that would have
3 exceeded her authorization in violation of the CFAA. *Nosal*, 676 F.3d at 858. But that is not the
4 situation here. SunPower has not alleged that either Messer or Fong circumvented any security
5 measures or accessed unauthorized information; instead, they allegedly misappropriated
6 information to which they had access in violation of SunPower’s policies.

7 A more apt comparison would be to another example that the Ninth Circuit discussed in
8 *Nosal*. The government argued that the CFAA should apply to an employee who is “authorized to
9 access customer lists in order to do his job but not to send them to a competitor,” but nevertheless
10 sends the competitor lists to a competitor. *Nosal*, 676 F.3d at 857. The court disagreed, observing
11 that applying CFAA to any unauthorized use of information obtained from a computer would
12 “make criminals of large groups of people who would have little reason to suspect they are
13 committing a federal crime.” *Id.* at 859. Punishing this type of behavior would be incongruent
14 with the statute’s focus on prohibiting hacking and other high technology related crimes. That is
15 true here as well.

16 SunPower relies on *American Furukawa, Inc. v. Hossain*, 14-cv-13633, 2015 WL 2124794
17 (E.D. Mich. May 6, 2015) to argue that other cases have followed *Nosal*’s approach while holding
18 that downloading files to removable media constitutes a violation under CFAA. *Opp.* at 7. In
19 *American Furukawa*, a company sued a former employee alleging that the employee emailed and
20 downloaded the company’s files in violation of the CFAA both while he was employed and during
21 a leave of absence. 2015 WL 2124794, at *1-2. The court held that the company properly alleged
22 that the employee took some files “without authorization” during his leave of absence. *Id.* at * 11.
23 Additionally, because the company’s computer use policy specified that an employee needs
24 permission from a manager before accessing files with removable media, the court also held that
25 the employee exceeded authorized access because he did not seek permission and therefore
26 violated this access restriction. *Id.* at *19.

27 *American Furukawa* does not help SunPower. Fundamentally, it comes from a district
28 court in Michigan that appropriately followed its Sixth Circuit precedent. It explicitly discussed

1 and disagreed with the approach of the Ninth Circuit in *Nosal*, which binds me. *Id.* at *18.
2 Moreover, the decision is consistent with this one in that the court rejected the employer's
3 argument that the employee's misappropriation of its files while he was actively employed was a
4 violation of the CFAA because he breached the employer's Secrecy Agreement; the court found
5 the CFAA violation only for the period when the employee was out on leave and violated a
6 condition of his leave--that he could not do any work during that time. *Id.* at *11. All of the
7 alleged behavior here occurred while Messer and Fong were current employees. Restrictions
8 related to an employee's leave of absence are not at play in this case.

9 In sum, SunPower's allegations describe misappropriation of its confidential information.
10 They do not constitute a violation of the CFAA. While it is not clear to me how it can
11 successfully plead a plausible CFAA cause of action in light of the allegations it has already made,
12 if it wishes it may amend its complaint within 20 days. If it chooses not to do so, I will remand
13 this case to the California Superior Court for further proceedings since no other basis for federal
14 jurisdiction is alleged.

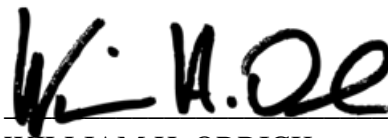
15
16 **CONCLUSION**

17 Defendants' motion to dismiss is GRANTED. SunPower's complaint is DISMISSED
18 WITH LEAVE TO AMEND. Any amended complaint shall be filed within 20 days of this Order.

19 If an amended complaint is not filed within that timeframe, I decline to exercise
20 supplemental jurisdiction over any remaining state law claims under 28 U.S.C. § 1367(c) and will
21 remand the case to state court. If an amended complaint is filed, I will retain jurisdiction as
22 appropriate.

23 **IT IS SO ORDERED.**

24 Dated: September 11, 2015

25 

26 WILLIAM H. ORRICK
27 United States District Judge
28