United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., et al.,

Defendants.

Case No. 17-cv-00561-WHO

ORDER ON PENDING MOTIONS

Re: Dkt. Nos. 77, 79, 80

This case stems from the purported interest of defendants Ubiquiti Network, Inc., Ubiquiti Networks International Limited (UNIL), and Ching-Han Tsai to review and evaluate for licensing plaintiff Synopsys, Inc.'s semiconductor electronic design and automation software. In its Second Amended Complaint, Synopsys alleges that defendants fraudulently gained access to its copyrighted software and related support materials and used evaluation license keys and counterfeit keys to repeatedly and illegally access and copy those programs and materials over the course of three years. When defendants' alleged conduct was discovered by Synopsys – through embedded "piracy tracking" tools (as described by Synopsys) or "spyware" (as described by defendants) – Synopsys sued.

Ubiquiti and UNIL counterclaimed based on Synopsys's use of the piracy tracking tools. They argue that Synopsys's conduct – hiding or failing to disclose the presence and operation of the anti-piracy software, using the anti-piracy software to access information on defendants' systems, and then sharing defendants' confidential information with third-parties – violated the parties' master non-disclosure agreement (MNDA) as well as federal and state computer abuse and common laws. UNIL alleges the following counterclaims: (1) declaratory relief; (2) violation of 18 U.S.C. § 1030, Computer Fraud and Abuse Act; (3) violation of Cal. Penal Code § 502, Computer Data Access Fraud Act; (4) Trespass to Personal Property and Chattels; (5) Conversion; (6) violation of 18 U.S.C. §

1962(c), Civil RICO; (7) violation of 18 U.S.C. § 1962(d), RICO Conspiracy; and (8) Fraud. Ubiquiti currently has counterclaimed only for declaratory relief and breach of contract, but seeks leave to amend to match the counterclaims asserted by UNIL (*e.g.*, adding the federal and state computer abuse and common law claims).[1]

Synopsys moves to dismiss UNIL's counterclaims, arguing that the counterclaims are either barred or inadequately pleaded. Similarly, Synopsys argues Ubiquiti's motion for leave to amend should be denied because of undue delay and prejudice in seeking leave, but also because amendment would be futile because the claims Ubiquiti seeks to allege (like UNIL's) are barred or inadequately pleaded. Finally, Synopsys moves to strike the state law counterclaims asserted by UNIL under California's anti-SLAPP statute, because those claims are based on Synopsys' privileged pre-litigation conduct in identifying what it believed were defendants' acts of piracy and seeking pre-litigation settlement of those claims.

As discussed below, defendants' theory of fraud is implausible and I agree in many respects with the arguments in Synopsys's motion. I GRANT the motion to dismiss UNIL's counterclaims. I DENY Ubiquiti's motion for leave to amend its counterclaims without prejudice and DENY Synopsys's motion to strike without prejudice.

BACKGROUND

The background to Synopsys's claims against defendants are laid out in full in my August 2017 Order. For purposes of ruling on the pending motions, I will focus on the allegations in Ubiquiti's existing counterclaims and those made in UNIL's counterclaims.

As part of the parties' agreement to allow Ubiquiti to review Synopsys's software, the parties entered into a master non-disclosure agreement (MNDA) to allow for the confidential exchange of information between the parties. UNIL Counterclaims ¶¶ 30 - 31, 34-35, 40.[2] Ubiquiti signed the MNDA on October 15, 2013, and Synopsys executed it on November 25,

[1] Because UNIL initially moved to dismiss for lack of jurisdiction, UNIL's answer and counterclaims were not filed until September 19, 2017. Dkt. No. 76.

[2] The factual allegations and claims Ubiquiti seeks leave to add are similar (in most respects) to the allegations and claims asserted in UNIL's counterclaims.

2013. UNIL Counterclaims ¶ 40; *see also* Second Amended Complaint (SAC) ¶ 40.

Defendants allege that Synopsys formed an "Enterprise" with QuatreWave LLC d/b/a SmartFlow Compliance Solutions (SmartFlow) and related-entity IT Compliance Association ("ITCA"), and the founders and current officers of those companies (Ted Miracco and Chris Luijten). The Enterprise placed SmartFlow's "phone-home" "spyware" in Synopsys' software programs. UNIL Counterclaims ¶¶ 8-16.[3] UNIL alleges that SmartFlow and ITCA "work in partnership in schemes to generate revenue for software companies by targeting supposed unlicensed uses of their customers' software." UNIL Counterclaims ¶ 11. As part of that effort:

> SmartFlow's spyware is embedded at least into that company's software and subsequently used to monitor and collect data from computers, servers, and unsuspecting individuals who use or have access to that software. The data includes individuals' personally identifiable information, such as user names and email addresses, the software programs and features accessed by users, and the locations, dates, and times of access. SmartFlow then shares the data that it collects and the identity of the suspected unlicensed users with its software customers. SmartFlow also offers the services of its sister company ITCA, who uses various coercive techniques to pressure individuals to pay exorbitant fees or other compensation to the software company for the alleged unlicensed uses.

UNIL Counterclaim ¶ 11.

UNIL asserts (and Ubiquiti wants to allege) that Synopsys concealed the presence of the spyware in the products that was downloaded pursuant to the parties' agreements onto Ubiquiti and UNIL's servers and computers. UNIL contends that Synopsys's license evaluation and MNDA agreements fail to disclose the presence and operation of this spyware in its products. UNIL Counterclaims ¶¶ 17, 47.

UNIL states that Synopsys together with ITCA and SmartFlow use the spyware to identify, often mistakenly, unauthorized users of Synopsys's software in order to "extract exorbitant license fees under the threat of litigation." UNIL Counterclaims ¶¶ 14, 18-25. UNIL identifies five lawsuits Synopsys filed based on unlicensed use of its software and alleges on information and belief that the facts regarding unauthorized use in those suits were obtained from phone-home

[3] The co-founder and current CEO of SmartFlow (Ted Miracco) and the co-founder of SmartFlow, founder of ITCA, and ITCA's current CEO (Chris Luijten) are repeatedly identified in UNIL's Counterclaims at ¶¶ 8-9,13-14.

spyware and that the Enterprise monitored, collected, and transmitted the confidential information of the defendants in those cases. *Id*. ¶¶ 18-25.

UNIL asserts that the Enterprise likewise monitored, collected, and transmitted UNIL and Ubiquiti's confidential information through the spyware in violation of the MNDA, unbeknownst to UNIL or Ubiquiti, and without their consent. *Id*. ¶¶ 29-36, 40, 52-53. That confidential information includes "IP addresses, MAC addresses, user names, host names, user accounts, email addresses, workstation information, system administrators, IT system logs, and other confidential information." *Id*. ¶ 47.

UNIL and Ubiquiti became aware of the spyware and the activities of the Enterprise in May 2016, when ITCA emailed Ubiquiti's CEO as an agent of Synopsys and disclosed its possession of the confidential UNIL and Ubiquiti information it had gathered through the spyware. ITCA made that disclosure and contact in order to convince Ubiquiti to pay "exorbitant fees" for the Synopsys software programs allegedly accessed by UNIL and Ubiquiti employees. *Id*. ¶¶ 51-52. Ubiquiti and UNIL argue that Synopsys delayed notifying them of the matter until two and one-half years after Synopsys had notice in order to allow the Enterprise to keep collecting confidential information and enlarge the period over which Synopsys could claim damages in the form of retroactive license fees. *Id*. ¶ 55.

In opposing Ubiquiti's motion for leave to amend and in support of its separate motion to strike UNIL's state law counterclaims, Synopsys relies on evidence that in order for Tsai to download Synopsys' software in December 2013 (which is when Tsai admits he downloaded Synopsys software initially: UNIL Counterclaim ¶ 41; Ubiquiti's Proposed Counterclaims ¶ 42), Tsai would have had to "click through" a notice and agreement that disclosed that "Licensed Products communicate with Synopsys services for the purpose of . . . detecting software piracy and verifying that customers are using Licensed Products in conformity with the applicable License Key" and that Synopsys will use that information to "pursue software pirates and infringers." Declaration of Norman F. Kelly [Dkt. No. 78-1], Ex. 2. Similarly, when an unnamed UNIL employee admittedly downloaded Synopsys software in April 2014, UNIL Counterclaim ¶ 44, he or she would have had to click through the same notice. Kelly Decl. ¶ 5.[4]

LEGAL STANDARD

I. MOTION TO DISMISS FOR FAILURE TO STATE A CLAIM

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

Under Federal Rule of Civil Procedure 9(b), a party must "state with particularity the circumstances constituting fraud or mistake," including "the who, what, when, where, and how of the misconduct charged." *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003) (internal quotation marks omitted). However, "Rule 9(b) requires only that the circumstances of fraud be stated with particularity; other facts may be pleaded generally, or in accordance with Rule 8." *United States ex rel. Lee v. Corinthian Colls.*, 655 F.3d 984, 992 (9th Cir. 2011). In deciding a motion to dismiss for failure to state a claim, the court accepts all of the factual allegations as true

[4] While Synopsys contends that I may rely on this outside-the-pleadings-evidence in support of its futility arguments in opposing the motion for leave to amend, the authorities Synopsys relies on are not persuasive. *Gaspard v. DEA Task Force*, 2016 WL 2586182, at *1 (C.D. Cal., April 4, 2016) (deciding issue without analysis and misstating cited reference); *Haney v. Baker*, 2012 WL 2521895, at *3 (E.D. Cal. June 28, 2012) (relying on evidence in support of a motion to dismiss for failure to exhaust administrative remedies). I conclude that I may rely on this evidence only in support of Synopsys' special motion to strike UNIL's state law counterclaims. In that regard, defendants contest whether there is proof Ubiquiti "clicked" assent to the terms of use and argue even if it did, it has alleged conduct that could not be consented to (*e.g.*, that the piracy software surveilled "areas of Ubiquiti's and/or UNIL's computers and servers wholly unconnected to the areas where Synopsys' evaluation software operated, and to monitor, collect, and transmit confidential, proprietary information with no connection to Synopsys' evaluation software."). UNIL Counterclaim ¶ 48.

and draws all reasonable inferences in favor of the plaintiff. *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). But the court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

II. SPECIAL MOTION TO STRIKE

California Code of Civil Procedure section 425.16 is California's response to "strategic lawsuits against public participation," or SLAPP lawsuits. It was enacted "to provide a procedure for expeditiously resolving nonmeritorious litigation meant to chill the valid exercise of the constitutional rights of freedom of speech and petition in connection with a public issue." *Hansen v. California Dep't of Corr. & Rehab.*, 171 Cal. App. 4th 1537, 1542-43 (2008). It provides that a cause of action against a person "arising from any act of that person in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue shall be subject to a special motion to strike, unless the court determines that the plaintiff has established that there is a probability that the plaintiff will prevail on the claim." Cal. Civ. Proc. Code § 425.16(b)(1). An "act in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connection with a public issue" includes:

> (1) any written or oral statement or writing made before a legislative, executive, or judicial proceeding, or any other official proceeding authorized by law,
>
> (2) any written or oral statement or writing made in connection with an issue under consideration or review by a legislative, executive, or judicial body, or any other official proceeding authorized by law,
>
> (3) any written or oral statement or writing made in a place open to the public or a public forum in connection with an issue of public interest, or
>
> (4) any other conduct in furtherance of the exercise of the constitutional right of petition or the constitutional right of free speech in connection with a public issue or an issue of public interest.

Cal. Civ. Proc. Code § 425.16(e).

"When served with a SLAPP suit, the defendant may immediately move to strike the complaint under Section 425.16." *Id.* at 1543. That motion is known as an anti-SLAPP motion. To determine whether an anti-SLAPP motion should be granted, the trial court must engage in a two-step process. "First, the defendant must make a prima facie showing that the plaintiff's suit arises from an act in furtherance of the defendant's rights of petition or free speech." *Mindys Cosmetics, Inc. v. Dakar*, 611 F.3d 590, 595 (9th Cir. 2010) (citation and internal quotation marks omitted). "Second, once the defendant has made a prima facie showing, the burden shifts to the plaintiff to demonstrate a probability of prevailing on the challenged claims." *Id.*

"At [the] second step of the anti-SLAPP inquiry, the required probability that [a party] will prevail need not be high." *Hilton v. Hallmark Cards*, 599 F.3d 894, 908 (9th Cir. 2009). A plaintiff must show "only a 'minimum level of legal sufficiency and triability.'" *Mindys*, 611 F.3d at 598 (quoting *Linder v. Thrifty Oil Co.*, 23 Cal. 4th 429, 438 n.5 (2000)). The plaintiff need only "state and substantiate a legally sufficient claim." *Id.* at 598-99 (citation and internal quotation marks omitted). In conducting its analysis, the "court 'does not weigh the credibility or comparative probative strength of competing evidence,' but 'should grant the motion if, as a matter of law, the defendant's evidence supporting the motion defeats the plaintiff's attempt to establish evidentiary support for the claim.'" *Id.* at 599 (quoting *Wilson v. Parker, Covert & Chidester*, 28 Cal. 4th 811, 821 (2002). At this stage, the court considers "the pleadings, and supporting and opposing affidavits stating the facts upon which the liability or defense is based." *Id.* at 598 (quoting Cal. Civ. Proc. Code § 425.16(b)(2)).

"[T]he anti-SLAPP statute cannot be used to strike federal causes of action." *Hilton v. Hallmark Cards*, 599 F.3d 894, 901 (9th Cir. 2010).

III. MOTION FOR LEAVE

Under Federal Rule of Civil Procedure 15(a), leave to amend "shall be freely given when justice so requires." Fed. R. Civ. P. 15(a). However, it "is not to be granted automatically." *Jackson v. bank of Hawaii*, 902 F. 2d 1385, 1387 (9th Cir. 1990). Courts generally weigh the following factors to determine whether leave should be granted: "(1) bad faith, (2) undue delay, (3) prejudice to the opposing party, (4) futility of amendment; and (5) whether plaintiff has previously amended his complaint." *In re W. States Wholesale Natural Gas Antitrust Litig.*, 715

F.3d 716, 738 (9th Cir. 2013).

A lack of diligence may warrant denying leave under Rule 15. "Where the party seeking amendment knows or should know of the facts upon which the proposed amendment is based but fails to include them in the original complaint, the motion to amend may be denied." *Jordan v. County of Los Angeles*, 669 F.2d 1311, 1324 (9th Cir. 1982), vacated on other grounds, 459 U.S. 810 (1982).

DISCUSSION

I. UBIQUITI MOTION FOR LEAVE TO AMEND

Ubiquiti seeks leave to amend its counterclaims to add the computer abuse and related state law counterclaims; essentially the identical counterclaims UNIL asserts against Synopsys.[5] Synopsys opposes on grounds of undue delay, prejudice, and futility.

A. Delay

Synopsys argues that Ubiquiti has unduly delayed moving to amend because Ubiquiti knew the factual basis underlying the current claims at least as of March 2017 when it filed its initial counterclaims, and arguably even earlier in May 2016 when ITCA confronted Ubiquiti with its evidence that Ubiquiti was illegally accessing and using Synopsys' software. Proposed Counterclaims ¶ 45. However, while the facts could have been suspected in May 2016, they were not known until March 2017. Given that this case is still very much in its infancy, I will not deny leave to amend based on undue delay.

B. Prejudice/Futility

The parties have agreed to an aggressive schedule, with close of fact discovery in April 2018. Synopsys contends that adding in these counterclaims now will cause significant delay to that schedule, especially given the allegations against the two "conspirators" ITCA and SmartFlow (as part of RICO enterprise) may require their joinder and, in any event, significant additional discovery. However, this third-party discovery (or motion practice) will arguably be required if UNIL's counterclaims stand after Synopsys's motion to dismiss, irrespective of whether Ubiquiti

[5] UNIL does not assert a breach of contract counterclaim, because UNIL was not a signatory to the MNDA signed by Ubiquiti and Synopsys.

is given leave to amend. Therefore, prejudice could be demonstrated only if UNIL's counterclaims are dismissed and then Ubiquiti was given leave to amend. Whether that is warranted depends on whether that leave would be futile, which will be considered below in conjunction with Synopsys's motion to dismiss UNIL's counterclaims.

II. MOTION TO DISMISS UNIL COUNTERCLAIMS/FUTILITY OF UBIQUITI'S PROPOSED COUNTERCLAIMS

Synopsys moves to dismiss UNIL's second through eighth counterclaims, arguing the claims are either barred as a matter of law or inadequately pleaded.[6] Similarly, Synopsys argues that allowing Ubiquiti leave to add its proposed counterclaims is futile as those claims fail on essentially the same grounds as UNIL's.

A. Computer Fraud and Abuse Act – 18 U.S.C. § 1030 *et seq*.

The "CFAA was enacted in 1984 to enhance the government's ability to prosecute computer crimes. The act was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives. . . .' [] The CFAA prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1130–31 (9th Cir. 2009).

UNIL alleges (and Ubiquiti seeks to allege) three violations under the Computer Fraud and Abuse Act: a violation of 28 U.S.C. § 1030(a)(2) – prohibiting "intentionally accesses a computer without authorization or exceeds authorized access" and thereby obtaining "information from any protected computer if the conduct involved an interstate or foreign communication"; a violation of § 1030(a)(4) – prohibiting "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers [a] intended fraud and obtains anything of value"; and violation of § 1030(a)(5)(A-C) –prohibiting

[6] Synopsys does not move to dismiss UNIL's first counterclaim, seeking declaratory relief that any use of plaintiff's software programs by UNIL did not constitute a violation of 17 U.S.C. § 1201.

> (A) knowingly causing the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer,
>
> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage, or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Under § 1030(g), in order to bring a private right of action under any of these provisions, defendants must *also* allege one of the following forms of damage, under § 1030(c)(4)(A)(i):

> (I) loss to 1 or more persons during any 1-year period . . . 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;

Synopsys contends that the CFAA counterclaims fail for a number of reasons, as discussed below.

1. Unauthorized Access

All CFAA claims asserted require "unauthorized access." Synopsys argues that cannot be shown here where defendants intentionally visited Synopsys's website and voluntarily downloaded Synopsys's software. *See, e.g., In re Sony PS3 Other OS Litigation*, 551 Fed.Appx. 916, 923 (9th Cir. 2014) ("As lower courts have reasoned, users who had 'voluntarily installed' software that allegedly caused harm cannot plead unauthorized 'access' under the CFAA."); *see also In re iPhone Application Litigation*, 844 F.Supp.2d 1040, 1066 (N.D. Cal. 2012) ("Voluntary installation of software that allegedly harmed the phone was voluntarily downloaded by the user. Other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation."); *see also Flextronics International, Ltd. v. Parametric Technology Corporation*, 2014 WL 2213910, at *5 (N.D. Cal., May 28, 2014, No. 5:13-CV-00034-PSG) (interpreting the California CDAFA and holding "that an unknown file or subroutine of otherwise voluntarily installed software cannot be said to have been installed on the computer 'without permission' in violation of the CDAFA.").

These unauthorized access cases are not helpful to Synopsys. Defendants' theory is that Synopsys *exceeded* any authorization it may have had by using the hidden anti-piracy software to access their confidential information. *See, e.g., Flextronics International, Ltd*., 2014 WL 2213910, at *3 (denying motion to dismiss "exceed authorization" CFAA claim where plaintiff alleged defendants concealed embedded technology in their software and used that technology to "access, obtain, and transmit information" in plaintiff's computers that defendants were not entitled to access, obtain, or transmit). UNIL has alleged and Ubiquiti can (if otherwise sufficient) allege an "exceeds authorization" claim under the CFAA.[7]

2. Use Versus Access to Data

Synopsys argues that because defendants' complaints are about the *use* of the data secured by Synopsys – as opposed to the access to that information by its anti-piracy software – defendants cannot plead a CFAA claim focused on the impermissible "access" to computers. As explained by the Ninth Circuit, "the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *U.S. v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). The court so held in the context of narrowly interpreting the statute to not criminalize the conduct of users who simply exceed corporate "terms of use" to hold "that the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." *Id.*

As noted above, this case fits within the "exceeds authorization" line of cases because the allegations are not based on violation of generally applicable "terms of use" but based on the

[7] Synopsys contends that because Ubiquiti consented to its terms of use when Ubiquiti downloaded the software – relying on its outside-the-allegations evidence – Ubiquiti expressly consented to and had notice of Synopsys's anti-piracy efforts and therefore cannot allege a CFAA claim. Opposition to Motion for Leave to Amend (Synopsys Oppo.) at 7-9. That may be true, but this evidence cannot be relied on in support of the opposition for leave to amend. The same is true of Synopsys's attempt to rely on this evidence in support of its opposition on Ubiquiti's proposed Section 502, trespass, and conversion claims discussed below.

hidden presence of software that accesses, obtains, and transmits information that a party was not entitled to access, obtain, or transmit. *See Flextronics International, Ltd*., 2014 WL 2213910, at *3. Synopsys's argument does not work.

3. Damage and Loss

Synopsys contends that defendants fail to allege facts to show that defendants suffered a "loss" of more than $5,000 in a one year period as a result of Synopsys' conduct. A mere conclusion of damage or loss is insufficient. *See, e.g., NovelPoster v. Javitch Canfield Group*, 140 F.Supp.3d 938, 949 (N.D. Cal. 2014).[8] There are two problems with the defendants' counterclaim allegations. While defendants are correct that courts have considered the "cost of investigating the source of a breach and remedying it" as a loss appropriately counted towards the $5,000 mark,[9] there are no facts alleged that defendants incurred $5,000 of loss in *responding* to Synopsys' alleged illegal conduct.[10] Further, while defendants have no doubt incurred costs investigating how Synopsys learned about defendants' alleged piracy, those expenses would necessarily have been incurred as part of defendants' investigation of and response to Synopsys's affirmative allegations against them. Defendants must plead *facts* showing that they incurred costs above and beyond those needed to respond to Synopsys's affirmative claims to state a separate claim for damages recoverable under the CFAA.

In addition, there are no allegations that the presence of Synopsys' anti-piracy software

[8] "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." § 1030(e)(11). "Damage" is defined "any impairment to the integrity or availability of data, a program, a system, or information." § 1030(e)(8).

[9] *See, e.g., Enki Corporation v. Freedman*, No. 5:13-CV-02201-PSG, 2014 WL 261798, at *2 (N.D. Cal., Jan. 23, 2014) ("the cost of investigating the source of the breach and remedying it would qualify as 'loss' within that definition, as they would be required to return the system to its secured state").

[10] UNIL alleges only Synopsys's actions have "imposed unknown costs by depriving Ubiquiti and UNIL of the economic value of confidential information taken without their consent or knowledge, and causing undue expenditures of resources to investigate access to proprietary information" and then that they have been damaged of an unknown total "but aggregating more than $5,000." UNIL Counterclaims ¶¶ 49, 66.

caused any disruption or other damage to defendants' computer systems. *See, e.g., In re iPhone Application Litigation*, 844 F.Supp.2d 1040, 1067 (N.D. Cal. 2012) (while "Plaintiffs have alleged that the location files consume valuable memory space on their iDevices, Plaintiffs have not plausibly alleged that the location file impairs Plaintiffs' devices or interrupts service, or otherwise fits within the statutory requirements of "loss" and "economic damage" as defined by the statute").[11]

Finally, defendants have not plausibly alleged that accessing the types of information secured by Synopsys – IP addresses, MAC addresses, user names, host names, user accounts, email addresses, workstation information, system administrators, and IT system logs – caused economic damage to defendants under the CFAA. *In re iPhone Application Litigation*, 844 F.Supp.2d at 1068 ("courts have tended to reject the contention that personal information—such as the information collected by the Mobile Industry Defendants—constitutes economic damages under the CFAA.").[12] The categories of information identified do not, on their face, appear to convey or create any economic value to defendants (or create harm to defendants' customers and hence defendants).

Finally, the claim under § 1030(a)(5) requires a showing of *damage* to the computer systems – *e.g.*, some impairment of the functioning of those systems. Defendants have not pleaded such a claim.

UNIL's failure to adequately allege damage and loss under the CFAA requires the dismissal of those counterclaims. Ubiquiti's failure to allege the same makes their proposed

[11] Defendants vaguely plead "damage and loss" from impairment of integrity of defendants' information and "otherwise causing damage to protected computers." UNIL Counterclaims ¶ 63.

[12] Defendants assert only that "confidential and proprietary information that was collected by the Enterprise has economic value to Ubiquiti, UNIL, their competitors, and those who trade in such information, and is information that Ubiquiti and UNIL use as an economic asset." UNIL Counterclaim ¶ 64. However, as Synopsys points out, there are no facts supporting that allegation and numerous cases in this District have rejected the argument that IP addresses and other categories of information defendants contend were unlawfully accessed and transmitted have any proprietary value. Defendants' reliance on *U.S. v. Ivanov*, 175 F.Supp.2d 367, 371 (D. Conn. 2001) is misplaced. In that case, by obtaining "root access" a hacker had complete control over the victim's information (credit card numbers and merchant account numbers) and systems. The value of credit card and merchant account numbers to a hacker is obvious.

amendment futile.

4. Fraud

For the § 1030(a)(4) claim, defendants must also allege facts supporting a knowing intent to defraud defendants with particularity under Rule 9. *See, e.g., Oracle America, Inc. v. Service Key, LLC*, 2012 WL 6019580, at *6 (N.D. Cal. 2012) ("Rule 9(b) plainly applies to section 1030(a)(4)'s requirement that the defendant's acts further the intended fraud.").[13] Synopsys initially challenges the failure of defendants to plead the who, what, where, when of a knowing intent to defraud. Read generously, the essence of defendants' allegations is that Ubiquiti was misled by the failure of Synopsys to disclose in the negotiations with Ubiquiti and the signing of the MNDA that Synopsys would embed and access the piracy tools in the software defendants intended to download.

More problematic is that defendants' fraud theory rests on an implausible chain of inferences: Synopsys induced Ubiquiti (not UNIL) to enter into the MNDA with the expectation that Ubiquiti's confidential information would be kept confidential -> Synopsys expected defendants would download its software -> defendants would (without any alleged encouragement by Synopsys) continue to use that software after the evaluation licenses expired -> Synopsys would uncover that continued use through its hidden anti-piracy software -> and Synopsys would then be able to "defraud" defendants by demanding exorbitant licensing fees.[14] The heart of the fraud allegations are not plausible as alleged.

UNIL has a separate and threshhold problem. It was not a party to the MNDA. It is unclear whether (and if so, how) UNIL's fraud claim could be based on the subsequent conversations UNIL had with Synopsys regarding UNIL's evaluation license.

[13] Because defendants' § 1030(a)(4) counterclaim expressly pleads fraudulent action by Synopsys, even its own authorities recognize the need to meet the 9(b) standard. *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F.Supp.3d 816, 834 (N.D. Cal. 2014) (when "read together, the foregoing precedents require that CFAA claims under § 1030(a)(4) be pleaded with specificity only when fraudulent conduct is specifically alleged as the basis for the wrongdoing.").

[14] The fraud allegations in the stand-alone fraud and RICO counterclaims suffer from the same implausibility as discussed in more detail below.

UNIL's §§ 1030(a)(2) and (a)(5) counterclaims are DISMISSED with leave to amend to plead facts regarding loss and damages, and the § 1030(a)(4) counterclaim based on fraud is DISMISSED with leave to amend to attempt to plead a plausible claim. Ubiquiti's motion for leave to amend is DENIED as to the CFAA, without prejudice. Ubiquiti may move for leave to amend again, if it can plausibly allege loss and damage under §§ 1030(a)(2) and (a)(5) and fraud under § 1030(a)(4).

B. California Penal Code Section 502 - the Comprehensive Computer Data Access and Fraud Act ("CCDAFA")

1. Pleading deficiencies

Defendants allege that Synopsys violated several subsections of California Penal Code § 502(c), which prohibits one who: § 502(c) (1) –"[k]nowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data"; § 502(c)(2) – "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network"; § 502(c)(3) –"[k]nowingly and without permission uses or causes to be used computer services"; § 502(c)(6) –"[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section"; § 502(c)(7) –"[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network"; and § 502(c)(8) –"[k]nowingly introduces any computer contaminant into any computer, computer system, or computer network."

Synopsys argues that there is substantial overlap between the CFAA and CCDAFA except for one respect: "A plain reading of the [CCDAFA] demonstrates that its focus is on unauthorized taking or use of information. In contrast, the CFAA criminalizes unauthorized *access*, not subsequent unauthorized *use*." *U.S. v. Christensen*, 801 F.3d 970, 994 (9th Cir. 2015) (emphasis in original). More generally, Synopsys contends that the CCDAFA claims fail for the same reasons as the CFAA claims. For the reasons discussed above, I agree with Synopsys concerning the fraud-based allegations and damage/loss allegations. *See, e.g., Perkins v. LinkedIn Corporation*, 53 F.Supp.3d 1190, 1219 (N.D. Cal. 2014) ("Plaintiffs must plead some injury emanating from LinkedIn's alleged Section 502 violations to survive the Motion to Dismiss. *See* Cal.Penal Code § 502(e)(1) (noting that only an individual 'who suffers damage or loss by reason of a violation' may bring a private action)."). Its other arguments on this cause of action, discussed below, are not well taken.

a. Without Permission

With respect to the claims that require actions to be "without permission," (*i.e*., (2), (3), (6), and (7)), some courts in this District have concluded that "when software containing 'surreptitious code' is installed voluntarily by a plaintiff, a defendant has not accessed the plaintiff's computer 'without permission,' even if the plaintiff was unaware of the 'surreptitious code' when he or she installed the software." *Flextronics International, Ltd. v. Parametric Technology Corporation*, 2014 WL 2213910, at *4 (N.D. Cal., May 28, 2014, No. 5:13-CV-00034-PSG); *In re iPhone Application Litig*., 2011 WL 4403963, at *12 (N.D. Cal., Sept. 20, 2011, No. 11-MD-02250-LHK) ("Plaintiffs' own allegations, the iOS and third party apps—which contain the alleged 'surreptitious code'—were all installed or updated voluntarily by Plaintiffs."). However, other courts faced with allegations that embedded software was "deeply hidden" so that plaintiffs had no notice it "was operating, and they had no way to remove the software or to opt-out of its functionality" have concluded that voluntary installation does not defeat the CCDAFA claim. *In re Carrier IQ, Inc*., 78 F.Supp.3d 1051, 1101 (N.D. Cal. 2015).

Defendants argue that this case is more similar to *In re Carrier IQ* and goes beyond the "voluntary installation" cases because not only do they allege that the anti-piracy software was deeply hidden, but they assert that the areas of their systems accessed and "surveilled" by the anti-piracy software had nothing to do with the use or running of Synopsys' EDA software. UNIL Counterclaim ¶ 106. These allegations adequately allege access was "without permission" under the CCDAFA to the areas of defendants' systems "wholly unconnected to the areas where Synopsys' evaluation software operated." *Id.*

b. Knowing Access

As an additional ground to dismiss under CCDAFA, Synopsys argues that defendants need to but have not pleaded facts that could show that Synopsys *subjectively* believed that it lacked permission to access defendants' computers in the way it did given defendants' voluntary actions downloading Synopsys's software, including the anti-piracy component. With particular respect to UNIL, Synopsys argues there are no allegations that UNIL and Synopsys had an agreement (like the MNDA with Ubiquiti) to not disclose information that it secured, no allegations of breach of terms of use, and no allegation that Synopsys did anything to circumvent technical barriers. However, this argument ignores defendants' claims that the hidden anti-piracy exceeded the contemplated and authorized use of defendants' data by Synopsys' software. Defendants could not have given permission for activities that Synopsys knew (or were alleged to have known) were hidden from defendants' knowledge.

c. Contaminant

Defendants also argue that they have separately pleaded a claim under Section 502(c)(8), which does not contain a "without permission" requirement, but does require a "contaminant" to have been placed in defendants' computers. As explained in *Flextronics International, Ltd. v. Parametric Technology Corporation*, 2014 WL 2213910, at *5 (N.D. Cal., May 28, 2014), in order to state a claim under this subsection "plaintiff need only allege that the actions of the contaminant (modify/damage/destroy/record/ transmit) were undertaken by overcoming a technical barrier without the permission of the owner; the introduction of the contaminant to the system need not surmount the same hurdle." In *Flextronics*, the plaintiff was able to state a claim where defendant was alleged to have embedded hidden technology in plaintiff's system (even though initial access was with permission) but thereafter used the embedded technology to transmit information within the computer system without the intent or permission of the owners of the information. *Id*. at *6. Defendants have made similar allegations here.

2. Use of Data and CUTSA

In addition to the pleading deficiency arguments, Synopsys contends that to the extent that defendants' CCDAFA claims are based on misappropriation of confidential and proprietary information, the claims are preempted by California's Uniform Trade Secrets Act (CUTSA). Synopsys points to a line of cases holding that where there are allegations of misappropriation of information, even if that information does not meet the high standard of a protectable trade secret, any claim based on the misappropriation of that information is nonetheless preempted. *See, e.g., Waymo LLC v. Uber Technologies, Inc*., 256 F.Supp.3d 1059, 1063 (N.D. Cal. 2017) ("CUTSA also supersedes claims based on alleged misappropriation of non-trade secret information unless some other provision of positive law grants a property right in that information.").

However, the cases relied on by Synopsys address preemption of common law and unfair competition claims and do not explicitly address whether CUTSA would preempt a *statutory* claim arising under the California Penal Code. *See, e.g., Waymo LLC v. Uber Technologies, Inc*., 256 F.Supp.3d 1059, 1064 (N.D. Cal. 2017) (preempts Cal. Bus. & Prof. Code § 17200 claim based on misappropriation of information); *Avago Technologies U.S. Inc. v. Nanoprecision Products, Inc*., 2017 WL 412524, at *8 (N.D. Cal., Jan. 31, 2017) (conversion claim prerempted); *Heller v. Cepia, L.L.C.*, 2012 WL 13572, at *7 (N.D. Cal. Jan. 4, 2012) (finding misappropriation, conversion, unjust enrichment, and trespass to chattels claims based on misappropriate of information superseded by CUTSA); *SunPower Corp. v. SolarCity Corp*., 2012 WL 6160472, at *3 (N.D. Cal. Dec. 11, 2012) (listing common law claims); *see also Regents v. Aisen*, 2016 WL 4097072, *8 (S.D. Cal., Apr. 18, 2016) (rejecting preemption of CCDAFA claim).[15] Absent additional authority or persuasive argument, I will not find the CCDAFA claim preempted even if based in part on the misappropriation and subsequent use of defendants' information.

3. *Noerr-Pennington* and Litigation Privilege

Finally, Synopsys argues that defendants cannot assert a CCDAFA claim based on the *use* of the information secured by Synopsys because that use, as alleged by defendants, constitutes

[15] I recognize that the court in *Henry Schein, Inc. v. Cook*, 2017 WL 783617, at *5 (N.D. Cal., Mar. 1, 2017, No. 16-CV-03166-JST), found in passing that a Section 502 claim was preempted under CUTSA. However, the court did not analyze how CUTSA could preempt a specific provision of the California Penal Code that provides a private right of action for use of misappropriated information secured from a computer "hack," as opposed to common law claims based on misappropriation of business information.

pre-litigation conduct protected under the *Noerr-Pennington* doctrine as petitioning activity and protected activity under California's litigation privilege. Cal. Civil Code § 47(b).

The *Noerr-Pennington* doctrine "provides that concerted efforts to petition the government that would otherwise be illegal may nonetheless be protected by the First Amendment's Petition Clause when certain criteria are met." *United Nurses Associations of California v. National Labor Relations Board*, 871 F.3d 767, 786–87 (9th Cir. 2017). Protected conduct includes conduct "incidental" to litigation, such as "sending a pre-litigation settlement demand letter." *Id*. at 788; *see also Sosa v. DIRECTV, Inc*., 437 F.3d 923, 940 (9th Cir. 2006) ("presuit letters threatening legal action and making legal representations" are protected under the *Noerr-Pennington* doctrine "absent representations so baseless that the threatened litigation would be a sham.").

However, it is not the *use* of defendants' data by SmartFlow and Synopsys, resulting in ITCA sending its demand letter to Ubiquiti, that underlays the CCDAFA claims. The CCDAFA claims hinge on the use of the hidden anti-piracy software that allegedly exceeded defendants' understanding of what Synopsys' software would do and defendants' authorization, and then Synopsys disclosure of that allegedly confidential information to SmartFlow and ITCA. The *Noerr-Pennington* doctrine does not immunize Synopsys from these claims.[16]

In sum, UNIL's CCDAFA claims are DISMISSED with leave to amend the damage/loss and fraud allegations, and Ubiquiti's motion for leave to amend is DENIED without prejudice.

C. RICO

Synopsys argues that defendants' Racketeer Influenced and Corrupt Organizations Act (RICO) counterclaims are deficient because of their failure to adequately plead: (i) an enterprise, (ii) a pattern of racketeering activity, (iii) proximate cause, and (iv) for UNIL, a domestic injury.[17] Even if those deficiencies could be cured, Synopsys argues that the RICO claims are also barred

[16] Synopsys's argument under California's litigation privilege – which similarly protects communications made in connection with contemplated or ongoing litigation – fails for the same reasons. *See, e.g., Rohde v. Wolf*, 154 Cal.App.4th 28, 36 (2007) (pre-litigation communication is privileged only when it relates to litigation that is contemplated in good faith and under serious consideration).

[17] UNIL has pleaded and Ubiquiti seeks to plead a substantive RICO claim under 18 U.S.C. § 1962(c) and a RICO conspiracy claim under § 1962(d).

United States District Court
Northern District of California

because they are inextricably based on pre-litigation petitioning activity protected under the *Noerr-Pennington* doctrine.

1. Pleading deficiencies

The RICO statute, 18 U.S.C. § 1962(c), requires a plaintiff to prove that each defendant participated: in (1) the conduct of (2) an enterprise that affects interstate commerce (3) through a pattern (4) of racketeering activity which (5) the proximately harmed the victim. *See Eclectic Properties E., LLC v. Marcus & Millichap Co*., 751 F.3d 990, 997 (9th Cir. 2014). To show an enterprise, "plaintiffs must plead that the enterprise has (A) a common purpose, (B) a structure or organization, and (C) longevity necessary to accomplish the purpose." *Id*. The purpose here is the implementation of a "compliance program for Synopsys to recover license fees and to convert suspected unlicensed users of Synopsys' EDA software to licensed customers." UNIL Counterclaims ¶ 95.

"Racketeering activity," as defined in 18 U.S.C. § 1961(1)(B), is the commission of a predicate act that is one of an enumerated list of federal crimes; here the only predicate acts identified are wire fraud under 18 U.S.C. § 1343. The acts of wire fraud as part of the pattern of racketeering activity alleged are:

> (a) September 11, 2013 and September 16, 2013 emails from Synopsys's manager to Tsai and Ubiquiti's general counsel representing Synopsys' proposed MNDA terms, which were false or misleading when made because Synopsys did not intend to protect Defendants' confidential information disclosed from computers in California and Taiwan pursuant to the MNDA, but rather intended to monitor and collect it via embedded spyware;
>
> (b) November 15, 2013 and November 25, 2013 emails from Synopsys's manager to Tsai and Ubiquiti's in-house counsel with Synopsys executed copies of the MNDA, which were false or misleading when made because Synopsys did not intend to protect Defendants' confidential information disclosed from computers in California and Taiwan pursuant to the MNDA;
>
> (c) Transmission of Synopsys's software installation, documentation, and license files from Synopsys's electronic file transfer website hosted on California servers to Tsai in December 2013, which resulted in SmartFlow's spyware being installed on Ubiquiti's and UNIL's servers in California and Taiwan;
>
> (d) Transmission of Synopsys's software installation,

> documentation, and license files from Synopsys's electronic file transfer website hosted on California servers to UNIL in April 2014, which resulted in SmartFlow's spyware being installed on Ubiquiti's and UNIL's servers in California and Taiwan;
>
> (e) The Enterprise's continual monitoring, collection, and transmittal of Defendants' confidential information through spyware from Ubiquiti's and UNIL's servers in California and Taiwan between November 2013 and approximately May 2016, representing a 2.5-year period during which the Enterprise conspired to avoid detection of the spyware, thereby extending the time period over which Synopsys could claim damages in the form of retroactive license fees; and
>
> (f) May 10, 2016 email from ITCA, containing a letter from its chief executive officer Chris Luijten based in Netherlands to Ubiquiti's chief executive officer in the United States, with a settlement demand on behalf of Synopsys, followed by subsequent email demands to Ubiquiti to recover Synopsys' fees over a 2.5-year period for unlicensed users alleged by ITCA to have accessed Synopsys' EDA software, but who had no reason to ever use or access the software for an evaluation or any other purpose.

UNIL Counterclaims ¶ 100.

a. Enterprise/Purpose

A RICO enterprise has three elements: (1) a common purpose, (2) an ongoing organization, and (3) a continuing unit. *United States v. Christensen*, 828 F.3d 763, 780 (9th Cir. 2015). Synopsys argues, first, that defendants have not pleaded these elements because they have only pleaded (and can only plead) facts showing legitimate and arms-length business dealings between Synopsys, the supplier of its anti-piracy software, and its enforcement agent ITCA, all of whom are engaged in permissible anti-piracy endeavors. Because all three's endeavors are consistent with a legitimate business purpose, there can be no inference of a RICO enterprise with a common, illegal purpose. Synopsys MTD at 15. The cases relied on by Synopsys for this point are well-taken as to the RICO conspiracy claim, but do not preclude a direct RICO claim.

However, other deficiencies in the enterprise allegations exist. For example, defendants have failed to plead that anyone other than Synopsys had knowledge of the only predicate act – the wire fraud – because there are no allegations that SmartFlow or ITCA were aware of the MNDA and negotiations regarding access to Synopsys' software. MTD at 15-16. The existence of the MNDA is key to the effectuation of the enterprise's fraud (enticing victims to download Synopsys' software with false assurances the victims' confidential information will not be used against them). Similarly, Synopsys points out that there is no evidence that SmartFlow or ITCA were involved in the litigations filed by Synopsys against alleged unlicensed users of its software, yet these "improper" litigations are really the only facts supporting the purpose and longevity elements. Defendants' enterprise allegations are deficient.

b. Predicate Acts/Pattern of Racketeering Activity

To plead a RICO pattern, at least two predicate acts of racketeering activity need to be alleged. 18 U.S.C. § 1961(5). Synopsys argues that only one instance of wire fraud has been alleged – the entering into the MNDA by Ubiquiti – which is insufficient to allege a pattern. Defendants discuss other "wire acts," including the actual downloading of the Synopsys software, but defendants identify no *additional* representations or omissions that occurred in connection with those downloads. The downloads are merely the effectuation of the initial fraud. As to the May 2016 communications from ITCA (by letter and subsequent email), defendants do not assert that the ITCA communications were fraudulent in and of themselves (*e.g.*, they intentionally misstated or overstated the use of Synopsys's software by defendants), only that they were part of the otherwise fraudulent scheme.

Defendants might also intend to rely on the "information and belief" conduct that Synopsys and its Enterprise associates undertook with respect to the other lawsuits identified, in support of the pattern of racketeering element. UNIL Counterclaims ¶¶ 19-23. But information and belief is insufficient. Facts must be stated to support a charge that Synopsys or its Enterprise associates committed acts of wire *fraud* with respect to those lawsuits.[18]

As currently stated, the one predicate act of wire fraud identified – the initial discussion about and provision of the MNDA that was "false and misleading" – is insufficient to establish the requisite number of predicate acts or the pattern of racketeering activity.

c. Proximate Cause

Another significant flaw with UNIL's RICO claim is the lack of proximate cause between

[18] Synopsys questions whether, consistent with Rule 11, defendants will be able to allege fraud in connection with the other lawsuits, as publicly filed pleadings in those cases do not disclose the existence of MNDAs in those cases. Oppo. at 16 & n.6.

the fraud alleged and the harm suffered. Under RICO, there must be a "direct relation" between the injury asserted and the conduct alleged, and that link cannot be "too remote," "purely contingent," or "indirect." *Hemi Group, LLC v. City of New York, N.Y.*, 559 U.S. 1, 9 (2010) (internal quotations omitted).

As pleaded, the fraudulent scheme hinges on the MNDA – signed by Ubiquiti but not UNIL – that allegedly gave Ubiquiti confidence that its confidential information would not be disclosed and that was allegedly violated when Synopsys included the anti-piracy tools in its software. Because UNIL did not sign the MNDA, because UNIL voluntarily downloaded Synopsys's software, because UNIL then (allegedly) continued to use that software after the evaluation license period, and because the ITCA communications were sent to Ubiquiti (not UNIL), any harm to *UNIL* is too remote and indirect from the fraudulent conduct alleged.

d. Injury to Business or Property/Domestic Injury

In order to state a RICO claim, a plaintiff must "allege and prove a domestic injury to business or property" because RICO "does not allow recovery for foreign injuries." *RJR Nabisco, Inc. v. European Community*, 136 S.Ct. 2090, 2111 (2016). UNIL's RICO counterclaims fail for this independent reason; it fails to plead injury to its business or property in the United States, as opposed to a "foreign injury." Mindful of UNIL's repeated protestations in this case that it has no presence in California and did no business in California, facts supporting a domestic injury have not been alleged.[19]

More generally, Synopsys argues that both defendants have failed to allege facts showing they were "injured" in their business or property by the alleged RICO conduct. Defendants counter that because the "extent" of the information secured by the anti-piracy tools in Synopsys's software is currently unknown, the extent of defendants' injuries are unknown. UNIL Counterclaims ¶¶ 105-106. Defendants, however, are required to allege more than they were "damaged" by the RICO conduct. Facts must be alleged to show how and why those assertions

[19] UNIL's only authority, *Tatung Company, Ltd. v. Shu Tze Hsu*, 217 F.Supp.3d 1138, 1155 (C.D. Cal. 2016), is not apposite on the facts here. There, while the plaintiff was a foreign corporation, it was doing business in the United States through a wholly owned corporation and maintained a "hub" in the United States.

are plausible given the information currently available to defendants.

2. Noerr-Pennington

In addition to the pleading deficiencies identified above, Synopsys contends that UNIL's current and Ubiquiti's contemplated RICO counterclaims are barred as a matter of law because the alleged "target" of the claim is Synopsys's *Noerr-Pennington* protected pre-litigation licensing and settlement negotiations. As noted above, *Noerr-Pennington* does not bar the CCDAFA claims. But the result is different for RICO, given the nature of RICO scheme as pleaded by defendants (a fraudulent scheme to extort license fees). *See* UNIL Counterclaim ¶ 14 ("the purpose of exploiting personal and proprietary information from Synopsys's software users to generate revenue for Synopsys, SmartFlow, and ITCA based on the 'recovery' of Synopsys's license fees"); ¶ 95 ("the common purpose of implementing a compliance program for Synopsys to recover license fees and to convert suspected unlicensed users of Synopsys' EDA software to licensed customers"); ¶ 104 ("exploited for the purpose of making exorbitant license fee demands to those users. In cases where Synopsys escalated to filing lawsuits against users who had their personally identifiable information or confidential information unlawfully obtained by the Enterprise, each case settled shortly thereafter.").

In support of their allegations, defendants rely not only on the ITCA demand letter and Synopsys's subsequent lawsuit based on defendants' use of its software post the evaluation license period but also on *other* litigation Synopsys has filed seeking damages from unlicensed users. UNIL Counterclaims ¶¶ 19-25. What defendants have not done is claim that *any of* these license demands and the subsequent litigations *were shams*. *Sosa v. DIRECTV, Inc.,* 437 F.3d 923, 934 (9th Cir. 2006) (*Noerr-Pennington* protects litigation and related pre-litigation conduct, unless the contemplated or actual litigation was a sham, meaning it was "both objective[ly] baselessness and [based on] an improper motive").

Given how they have chosen to frame their RICO claims, the pre-petitioning and petitioning activities of Synopsys are at the heart of the fraudulent scheme alleged. As such, defendants must plead facts showing that the pre-suit license demands and subsequent litigations they rely on as evidence of the RICO Enterprise's purpose were objectively baseless *and* based on improper motives. All that has been alleged to date is that the Enterprise associates (Synopsys, SmartFlow, ITCA, Luijten, and Miracco) have sought to enforce Synopsys's software rights, and that in some instances the information relied on by the Enterprise associates to enforce those rights might not have been "accurate." UNIL Counterclaim ¶ 12. That is insufficient.

UNIL's RICO claims are DISMISSED with leave to amend and Ubiquiti's motion for leave to amend is DENIED. If defendants can allege facts to plausibly suggest that Synopsys's (and its Enterprise associates') demand letters and litigation to "extort" license fees were objectively and subjectively baseless (and then if defendants can cure the *additional* pleading deficiencies identified above), then defendants may be able to clear the *Noerr-Pennington* hurdle and state a RICO claim. Separately, UNIL will also have to allege additional facts in support of proximate cause and domestic injury with respect to the harms caused to it by the RICO enterprise.

D. Trespass to Chattels

Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350–51 (2003). In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case [sic], and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." *Id*. at 1351 (internal quotations and citations omitted). Further, "while a harmless use or touching of personal property may be a technical trespass (*see* Rest.2d Torts, § 217), an interference (not amounting to dispossession) is not actionable, under modern California and broader American law, without a showing of harm." *Id.*; *see also In re iPhone Application Litigation*, 844 F.Supp.2d 1040, 1069 (N.D. Cal. 2012) (dismissing allegations of harm that "do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass.").

To the extent defendants base their trespass claims on the accessing of their systems by the anti-piracy software, they must *but have not* alleged facts showing that access *impaired* the intended functioning of defendants' systems. And to the extent that defendants base their trespass claim on the anti-piracy software's securing of and use of defendants' data, that common law claim would be preempted by CUTSA. *See, e.g., Heller v. Cepia, L.L.C.*, 2012 WL 13572, at *7 (N.D. Cal., Jan. 4, 2012) (common law claims, including trespass, "premised on the wrongful taking and use of confidential business and proprietary information, regardless of whether such information constitutes trade secrets, are superseded by the CUTSA").

Therefore, UNIL's trespass counterclaim is dismissed with leave to state facts showing the trespass caused some harm to its computer systems. Ubiquiti's motion to amend is denied without prejudice.

E. Conversion

As to conversion, "if the only property identified in the complaint is confidential or proprietary information, and the only basis for any property right is trade secrets law, then a conversion claim predicated on the theft of that property is preempted" by CUTSA. *Avago Technologies U.S. Inc. v. Nanoprecision Products, Inc.*, 2017 WL 412524, at *7 (N.D. Cal. Jan. 31, 2017). Defendants' claim is preempted and DISMISSED as to UNIL; leave to amend DENIED as to Ubiquiti.

F. Fraud

Synopsys makes a number of well-taken attacks on UNIL's fraud claims, primarily that UNIL was not a party to the MNDA and has not identified any fraudulent misstatements directed to it, as opposed to Ubiquiti. Those omissions are significant in the context of this case, where UNIL has repeatedly emphasized that it is a separate legal entity from Ubiquiti and that Tsai (the primary negotiator with Synopsys) did not work for UNIL. Given that context, it is questionable whether UNIL could plead reliance on the MNDA or on representations made by Synopsys, or damages suffered from a breach of the MNDA.[20]

As to both defendants, Synopsys relies on the actual text of the MNDA – which is

[20] While UNIL argues in its opposition that it was an expected third-party-beneficiary of the MDNA in light of actions taken by Ubiquiti and Synopsys, those allegations are not currently included in UNIL's Counterclaims.

incorporated by reference given the repeated reference to it in UNIL's existing and Ubiquiti's proposed counterclaims. Synopsys argues that the information allegedly fraudulently procured from defendants – IP addresses, MAC addresses, user names, host names, user accounts, email addresses, workstation information, system administrators, IT system logs – is not included within the MNDA's definition of "confidential information" nor covered by the "purpose" of the MNDA. MTD 23-24; Oppo. at 13-15.

However, I need not analyze the language of the MNDA. The fatal problem with defendants' theory of fraud has been identified above; the current allegations are implausible because they rely on too many intervening steps that were beyond the control of Synopsys. Synopsys did not force either defendant to use its software beyond the period of the evaluation licenses. But that conduct – defendants voluntary use of Synopsys's software that defendants do not deny – lies at the heart of the fraudulent scheme alleged. As to plausibility, defendants offer no real response. At most they argue that because Synopsys let defendants impermissibly use its software for two years after the expiration of the evaluation licenses before it decided to have ITCA go after defendants, their theory is somehow plausible. MTD at 25. It is not.

UNIL's fraud claim is DISMISSED with leave to amend. Ubiquiti's motion for leave to include a fraud counterclaim is DENIED without prejudice.

For the foregoing reasons, Synopsys's motion to dismiss UNIL's counterclaims is GRANTED. UNIL's second through eighth counterclaims are DISMISSED with leave to amend. Ubiquiti's motion for leave to amend its existing counterclaims to assert ones consistent with UNIL's is DENIED without prejudice due to futility.

III. SPECIAL MOTION TO STRIKE

Synopsys also moves to strike UNIL's state law counterclaims. It argues that it satisfies the first prong of the anti-SLAPP statute because the elements of UNIL's state law counterclaims demonstrate that those claims are aimed at chilling Synopsys's right to enforce its copyrights through pre-litigation demand letters and litigation. On the second prong, Synopsys argues that UNIL's state law claims are barred by the litigation privilege and that UNIL cannot otherwise prevail on those claims because Synopsys's terms of use in place during the relevant timeframe

United States District Court
Northern District of California

disclosed that Synopsys's software would communicate with Synopsys' servers to detect software piracy and verify only licensed use of its software. *See* Declaration Norman F. Kelly [Dkt. No. 801-1] ¶¶ 3, 5 & Exs 1&2.

However, as noted above, because all of the challenged state law counterclaims have been dismissed (albeit, with leave to amend), I need not reach the separate anti-SLAPP motion to strike. Synopsys's motion to strike is DENIED without prejudice. If UNIL amends, its amendments must clarify whether any of the counterclaims are based on the *use* of the data by Synopsys and ITCA (*e.g*., implicating Synopsys's protected pre-litigation activities) or are based on conduct that pre-dates any use of the data.

CONCLUSION

Synopsys's motion to dismiss UNIL's counterclaims is GRANTED with leave to amend. Ubiquiti's motion for leave to amend its counterclaims is DENIED for futility without prejudice. Synopsys's motion to strike is DENIED without prejudice. Defendants' further motions to amend, if any should be filed within twenty days of the date below.

IT IS SO ORDERED.

Dated: March 13, 2018

William H. Orrick
United States District Judge