IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

ACCENTURE, LLP,

Plaintiff,

v.

HARDEV SIDHU,

Defendant.

NO. C10-2977 TEH

ORDER GRANTING MOTION TO DISMISS

This matter came before the Court on October 18, 2010, on the motion to dismiss filed by Defendant Hardev Sidhu ("Sidhu"). For the reasons set forth below, the motion is GRANTED.

BACKGROUND

This lawsuit arises from a dispute between Sidhu and his former employer, Plaintiff Accenture, LLP ("Accenture"), in which Accenture contends that Sidhu violated various sections of the Computer Fraud and Abuse Act ("CFAA"), misappropriated trade secrets, converted Accenture's secret information, and breached his contract with Accenture. On September 3, 2010, Sidhu moved to dismiss Accenture's causes of action under the CFAA; Accenture opposed the motion.

Sidhu is a former employee of Accenture-Australia, Ltd., a sister company to Plaintiff Accenture. Sidhu went to work for Plaintiff Accenture in San Francisco, California, on or about October 2006. Sidhu remained employed by Accenture during the years that followed, and on March 27, 2009, Sidhu began a medical leave of absence. Sidhu continued to receive full pay and benefits while on leave, and he performed services for Accenture's clients. On several occasions during his medical leave, Sidhu confirmed that his illness required extended bed rest, prompting him to take additional leave. His period of leave continued until

Accenture officials determined that Sidhu had fabricated the medical condition upon which he premised his leave of absence, and had started working for HCL, Accenture's direct competitor, in June 2009. Sidhu resigned from Accenture several days later, on April 27, 2010.

For the duration of Sidhu's medical leave, Accenture made available to Sidhu its secure online network containing confidential and proprietary information, known as Accenture's Knowledge Exchange ("KX"). Sidhu downloaded more than 900 documents from the KX system while on medical leave, the "vast majority" of them after he began working for HCL. Pl.'s Opp. 4:13, Sept. 27, 2010. Sidhu did so despite having acknowledged and agreed to comply with various policies, including Accenture's "Confidentiality Policy," "Security Policy," "Dual Employment Policy," "Workstation Security Standard," and "Mobile Device Policy." Accenture contends that these policies proscribed Sidhu's conduct while on medical leave.

LEGAL STANDARD

Dismissal is appropriate under Federal Rule of Civil Procedure 12(b)(6) when a plaintiff's allegations fail "to state a claim upon which relief can be granted." In ruling on a motion to dismiss, the Court must "accept all material allegations of fact as true and construe the complaint in a light most favorable to the non-moving party." *Vasquez v. L.A. County*, 487 F.3d 1246, 1249 (9th Cir. 2007). Courts are not, however, "bound to accept as true a legal conclusion couched as a factual allegation." *Ashcroft v. Iqbal*, – U.S. –, 129 S. Ct. 1937, 1949-50 (2009).

A Rule 12(b)(6) dismissal "can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). To survive a motion to dismiss, a plaintiff must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). Plausibility does not equate to probability, but it requires "more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 129

S. Ct. at 1949. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Dismissal of claims that fail to meet this standard should be with leave to amend unless it is clear that amendment could not possibly cure the complaint's deficiencies. *Steckman v. Hart Brewing, Inc.*, 143 F.3d 1293, 1296 (9th Cir. 1998).

DISCUSSION

I. Violation of the CFAA

Count One of Accenture's First Amended Complaint ("FAC") alleges that Sidhu violated three provisions of the CFAA. According to the Ninth Circuit,

> [t]he 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 . . ." H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). 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). The CFAA is not strictly a criminal statute; it also allows plaintiffs to bring civil actions under its provisions. *See* 18 U.S.C. § 1030(g).

Count One of Accenture's FAC alleges that Sidhu violated 18 U.S.C. sections 1030(a)(2)(C), (a)(4), and (a)(5)(A)(iii) of the CFAA. Section 1030(a)(2)(C) makes it unlawful if a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." Section 1030(a)(4) makes it unlawful if a person "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ." Section 1030(a)(5)(A)(iii) does not correspond to a current section of the CFAA, but

according to Accenture's FAC, the statute makes it unlawful if a person "intentionally accessed a protected computer network without authorization and/or exceeded authority, and, as a result of such conduct, caused damage . . . ."[1] This language seems to correspond with 18 U.S.C. section 1030(a)(5)(C), a current section of the CFAA that makes it unlawful if a person "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss." The Court assumes that Accenture intended to cite the latter statutory section, and thus all of Accenture's allegations under the CFAA share the element of authority – Sidhu must have acted "without authorization" or "exceed[ed] authorized access" to have violated sections 1030(a)(2)(C) and 1030(a)(4), and "without authorization" to have violated section 1030(a)(5)(C).

The CFAA does not define the phrase "without authorization." In *Brekka*, the Ninth Circuit held that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it."[2] *Brekka*, 581 F.3d at 1133. Under the CFAA, the phrase "exceeds authorized access" "means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This statutory definition "implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access that computer," the Brekka court wrote in dicta. *Brekka*, 581 F.3d at 1135. Our sister court endorsed this interpretation in *United States v. Nosal*, determining after thorough analysis that employees "exceed[] authorized access" when they access computer information beyond what the employer has made available to them. *Nosal*, 2010 WL 934257, at *7 (N.D. Cal. Jan. 6, 2010). As the court reasoned,

---

[1] 18 U.S.C. section 1030(a)(5)(A)(iii) is a valid citation to the 2002 version of the CFAA, and it applies to a person who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage."

[2] *Brekka* did not consider amendments to the CFAA enacted in 2008. *Brekka*, 581 F.3d at 1131 n.3 (citing Pub. L. 110-136, §§ 203-208). However, these amendments do not change the meaning of "without authorization" and "exceeds authorized access," nor does Accenture argue that they have this effect.

> [a]n individual only "exceeds authorized access" if he has permission to access a portion of the computer system but uses that access to "*obtain* or *alter* information in the computer that [he or she] is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (emphasis added). There is simply no way to read that definition to incorporate corporate policies governing use of information unless the word alter is interpreted to mean misappropriate. Such an interpretation would defy the plain meaning of the word alter, as well as common sense. A person does not necessarily alter information on a computer when they access it with a nefarious intent. Furthermore, the government's proposed interpretation of "exceeds authorized access" would create an uncomfortable dissonance within section 1030(a)(4). Pursuant to the government's reading of the statute, an individual's intent would be irrelevant in determining whether that person accessed a computer "without authorization," but as long as the company had policies governing the use of the information stored in its computer system, that same individual's intent could be dispositive in determining whether they "exceed[ed] authorized access." Finally, the government's proposed interpretation of "exceeds authorized access" raises the same rule of lenity concerns with which the Ninth Circuit already grappled regarding the "without authorization" prong of the statute. Thus, although *Brekka* does not squarely address the reach of the "exceeds authorized access" prong of section 1030(a)(4), it emphasizes that access and intent are separate elements.

Id. For these reasons, the court in *Nosal* held that an employee "exceeds authorized access" when he accesses information without permission, not when he violates company policies. *Id.* This Court agrees.

Accenture argues that *Brekka* is distinguishable because the former-employer plaintiff in that case had not implemented written agreements or policies governing the defendant's conduct, which involved e-mailing documents to a personal computer. *See Brekka*, 581 F.3d at 1129. However, district courts interpreting *Brekka* have not recognized this distinction. For example, in *Nosal*, the court dismissed charges under CFAA where the defendant, an independent contractor, obtained proprietary information from the plaintiff employer in violation of disclosure policies. *Nosal*, 2010 WL 934257, at *1-2, *6. In another post-*Brekka* case, *National City Bank, N.A. v. Prime Lending, Inc.*, a district court held that *Brekka* required dismissal of CFAA claims where an employee allegedly took confidential information from computers he was permitted to use for work and used that information to compete with the employer. 2010 WL 2854247, at *4 (E.D. Wash July 19, 2010). The court

reached this holding despite the fact that the employee had agreed not to engage in the activities he allegedly undertook – recruiting his employer's employees, using his employer's trade secrets, and soliciting his employer's customers for a period of time after leaving the company. *Id.* at *1. The Court finds these cases – which hold that access is not established by employers' policies, but by the extent the employer makes the computer system available to the employee – to be persuasive. The cases Accenture cites to the contrary predate *Brekka*, are from outside the Ninth Circuit, or both.

Accenture also attempts to distinguish Sidhu's alleged violation of the company's Dual Employment Policy from other alleged violations, arguing that because Sidhu lied to human resources personnel and began working for HCL, he was no longer authorized to access the KX system. But for Sidhu's deception he would not have been an employee of Accenture, Accenture contends, and thus he was not authorized to access Accenture's computer network. The Court is not persuaded by this reasoning. Not only does it undermine *Brekka* by incorporating corporate policy into the substance of the CFAA, but it also asks courts to determine which employee conduct is deceptive, and whether that deception, if known to the employer, would have resulted in the employee's termination. The courts in *Nosal* and *National City Bank* engage in no such inquiry, even though the conduct alleged in those cases was arguably deceptive and, if known, might have resulted in the employees' termination. As the court noted in *Nosal*, "an individual's intent in accessing a computer, be it to defraud or otherwise, is irrelevant in determining whether an individual has permission or is authorized to access the computer." *Nosal*, 2010 WL 934257, at *6. The court in *National City Bank* agreed, observing that an "employee's subjective state of mind, the purpose for which the employee accesses the documents, and whether the employee breaches a state law duty of loyalty to the employer by doing so are irrelevant to whether he exceeds the scope of authorization." *National City Bank*, 2010 WL 2854247, at *4. The relevant inquiry is whether the employer allowed the employee use the computer system, irrespective of whether the employer would have revoked permission if it understood the employees' intent, or knew about the employee's conduct. Here, Sidhu was an Accenture employee with

permission to use its computer system. Whether Sidhu was deceptive, and whether he would have been fired pursuant to Accenture's Dual Employment Policy had Accenture learned of his deception, are irrelevant.

The only post-*Brekka* case from within the Ninth Circuit that Accenture cites regarding interpretation of the CFAA is *Atpac, Inc. v. Aptitude Solutions, Inc.*, 2010 WL 1779901 (E.D. Cal. Apr. 29, 2010). In *Atpac*, a company that licensed software to a county agency sued the agency and an agency employee under the CFAA for allegedly sharing the contents of the software with a third party in violation of the license agreement. *Id.* at *1. In a parenthetical citation within a section discussing third party liability under the CFAA, the court in *Atpac* noted that the CFAA "presumably" "provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access." *Id.* at *6. Accenture argues that Sidhu exploited a known mistake regarding his dual employment, and thus is liable under the CFAA. Tellingly, however, Accenture does not cite portions of *Atpac* that analyze plaintiff's CFAA claims against the county agency and its employee, which alleged that they acted "without authorization"or "exceed[ed] authorized access." The court in *Atpac* held that the agency and employee did not act "without authorization" because they were "authorized to use the computer at issue for at least some purposes." *Id.* at *4. It further held that they did not "exceed authorized access" because the licensing agreement did not limit access, but merely "how [the county] could *use* [the software] by making copies of it or disclosing it to third parties." *Id.* (emphasis in original). Thus rather than support Accenture's reading of the CFAA, *Atpac* stands for the principle that written agreements and policies do not dictate liability under the statute.

In light of the foregoing analysis, the Court finds that Accenture has alleged no facts that would support a finding that Sidhu acted "without authorization" or "exceed[ed] authorized access" under the CFAA.

II. Leave to Amend

Leave to amend should be granted unless the Court determines that no set of facts could possibly cure the pleading. *Steckman*, 143 F.3d at 1296. In the FAC, Accenture averred

that "[w]hile employed by Accenture-Australia and thereafter Accenture . . . Sidhu was given access to and was responsible for the further development of Accenture's trade secrets and confidential information." First Am. Compl. 9:7-9, Aug. 19, 2010. When asked at hearing what additional facts Accenture would allege in an amended complaint, Accenture offered none. The Court therefore finds that amendment could not cure the FAC's deficiencies.

This is true even if the Court has incorrectly assumed that when Accenture pleaded a violation of section 1030(a)(5)(A)(iii) in the FAC, it intended to plead a violation of section 1030(a)(5)(C). The language of the FAC indicates that the statutory section Accenture intended to cite requires Sidhu to have acted "without authorization" and/or "exceed[ed] authorized access." Therefore, if amendment could not cure the properly pleaded sections of the CFAA, amendment could not cure the improperly pleaded one.

CONCLUSION

For the reasons set forth above, Plaintiff's motion to dismiss is GRANTED. Count One of the First Amended Complaint is DISMISSED with prejudice.

IT IS SO ORDERED.

Dated: 11/9/10

THELTON E. HENDERSON, JUDGE
UNITED STATES DISTRICT COURT