EXHIBIT 53

LEXSEE 2010 U.S. DIST. LEXIS 24359

UNITED STATES OF AMERICA, Plaintiff, v. DAVID NOSAL, Defendant.

No. C 08-0237 MHP

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

2010 U.S. Dist. LEXIS 24359

January 5, 2010, Decided
January 6, 2010, Filed

COUNSEL: [*1] For David Nosal, Defendant: Steven Francis Gruel, LEAD ATTORNEY, Law Office of Steven F. Gruel, San Francisco, CA; Dennis Patrick Riordan, Riordan & Horgan, San Francisco, CA.

For Becky Christian, Defendant: Steven Mark Bauer, LEAD ATTORNEY, Danielle Andrea Lackey, Latham & Watkins, San Francisco, CA; John Francis Walsh, Hill & Robbins, PC, Denver, CO.

For USA, Plaintiff: Kyle F. Waldinger, LEAD ATTORNEY, Office of the United States Attorney, San Francisco, CA; Jaikumar Ramaswamy, U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Washington, DC.

JUDGES: MARILYN HALL PATEL, United States District Court Judge.

OPINION BY: MARILYN HALL PATEL

OPINION

MEMORANDUM & ORDER

Re: Defendant's Motion for Reconsideration and Second Motion to Dismiss

Defendant David Nosal ("Nosal") has been indicted on theft of trade secrets, illegal computer intrusion and mail fraud. On April 13, 2009, this court granted in part and denied in part Nosal's motion to dismiss a number of the counts in the twenty-count superseding indictment filed against him. The court dismissed counts twelve through twenty of the superseding indictment, which alleged violations of the federal mail fraud statute, *18 U.S.C. §§ 1341* [*2] & *2*, but denied Nosal's motion with respect to counts one through eleven. *United States v. Nosal, No. CR 08-00237 MHP, 2009 U.S. Dist. LEXIS 31423, 2009 WL 981336 (N.D. Cal. Apr. 13, 2009)* (Patel, J.). The court specifically held that counts two through nine of the superseding indictment, which allege violations of the Computer Fraud and Abuse Act ("CFAA"), *18 U.S.C. § 1030(a)(4)*, sufficiently pled the elements necessary to survive a motion to dismiss. *Nosal, 2009 U.S. Dist. LEXIS 31423, 2009 WL 981336, at *6-7*. On October 5, 2009, Nosal filed a motion for reconsideration and a second motion to dismiss, arguing that the Ninth Circuit's intervening decision in *LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009)*, requires that this court revisit its decision not to dismiss the CFAA counts in the superseding indictment. Nosal contends that *Brekka* establishes an interpretation of the phrases "without authorization" and "exceeds authorized access" in the CFAA that is contrary to this court's prior interpretation of the statute and that mandates the dismissal of counts two through nine. Having considered the parties' arguments and submissions, and for the

reasons stated below, the court issues the following memorandum and order.

BACKGROUND [*3] [1]

1 Unless otherwise noted, all cited background facts are taken from the superseding indictment, Docket No. 42.

Nosal was a high level executive at an international executive search firm, Korn/Ferry International ("Korn/Ferry"), from approximately April 1996 to October 2004. Nosal terminated his employment with Korn/Ferry in October 2004, with plans to start a competing executive search firm. Upon his departure, Nosal voluntarily entered into a separation agreement and agreed to serve as an independent contractor for Korn/Ferry. Under the terms of that Separation and General Release Agreement and an Independent Contractor Agreement (collectively "the Nosal-Korn/Ferry Agreements"), Nosal agreed to cooperate with Korn/Ferry on certain ongoing search assignments and agreed not to compete with Korn/Ferry by abstaining from performing executive search, executive placement, management assessment or management audit services on behalf of any entity other than Korn/Ferry during the period the Nosal-Korn/Ferry Agreements were in place. In exchange for his services, Nosal was to receive $ 25,000 per month during that year, as well as two lump-sum payments on July 31st and October 15, 2005.

Co-defendant [*4] Becky Christian ("Christian") was an employee of Korn/Ferry from approximately September 1999 through January 2005. An individual identified in the superseding indictment as "J.F." was employed by Korn/Ferry from approximately December 1997 to August 2005. J.F. was Nosal's executive assistant prior to Nosal's departure from Korn/Ferry. An individual identified as M.J. was employed by Korn/Ferry from approximately January 2001 until approximately March 2005. According to the superseding indictment, Christian, J.F. and M.J helped Nosal set up his new executive search firm and assisted Nosal in obtaining trade secrets and other things of value from Korn/Ferry's computer system, prior to and upon termination of their employment with Korn/Ferry by using their own Korn/Ferry password-protected user accounts. Specifically, the superseding indictment alleges that J.F., M.J. and Christian assisted Nosal in obtaining source lists and other custom reports of names and contact information from the Korn/Ferry "Searcher" database, a highly confidential and proprietary database of executives and companies.

On April 10, 2008, Nosal and Christian were charged by indictment with federal statutory violations [*5] relating to their alleged involvement in stealing confidential and proprietary information from Korn/Ferry for the purpose of assisting Nosal in his own executive search activities. On June 16, 2008, the court granted Christian's motion to sever. In a June 26, 2008, superseding indictment, Nosal was charged with twenty counts, including theft of trade secrets, illegal computer access under the CFAA, and mail fraud. As is discussed above, on April 13, 2009, this court denied Nosal's motion to dismiss charges one through eleven for failure to adequately state an offense and granted Nosal's motion to dismiss with respect to claims twelve through twenty of the superseding indictment. On October 5, 2009, Nosal filed a motion for reconsideration of the court's order refusing to dismiss the CFAA charges, counts two through nine.

LEGAL STANDARD

I. Motion for Reconsideration

A motion for reconsideration may only be granted when "[t]he district court (1) is presented with newly discovered evidence, (2) committed clear error or the initial decision was manifestly unjust, or (3) if there is an intervening change in controlling law." *School Dist. No. 1J, Multnomah County v. ACandS, Inc., 5 F.3d 1255, 1263 (9th Cir. 1993)*, [*6] *cert. denied, 512 U.S. 1236, 114 S. Ct. 2742, 129 L. Ed. 2d 861 (1994)*.

II. Motion to Dismiss

Under *Rule 12(b) of the Federal Rules of Criminal Procedure*, a party may file a motion to dismiss based on "any defense, objection, or request that the court can determine without a trial of the general issue." *Fed. R. Crim. P. 12(b)*; *United States v. Shortt Accountancy Corp., 785 F.2d 1448, 1452 (9th Cir. 1986)*. In considering a motion to dismiss, the court is limited to the face of the indictment and must accept the facts alleged in the indictment as true. *Winslow v. United States, 216 F.2d 912, 913 (9th Cir. 1955)*; *United States v. Ruiz-Castro, 125 F. Supp. 2d 411, 413 (D. Haw. 2000)*. "General conclusory allegations need not be credited, however, when they are belied by more specific

allegations in the [indictment]." *Hirsch v. Arthur Andersen & Co., 72 F.3d 1085, 1092 (2d Cir. 1995)*. "An indictment will withstand a motion to dismiss 'if it contains the elements of the charged offense in sufficient detail (1) to enable the defendant to prepare his defense; (2) to ensure him that he is being prosecuted on the basis of facts presented to the grand jury; (3) to enable him to plead double jeopardy; and (4) to inform the court of [*7] the alleged facts so that it can determine the sufficiency of the charge.'" *United States v. Rosi, 27 F.3d 409, 414 (9th Cir. 1994)* (quoting *United States v. Bernhardt, 840 F.2d 1441, 1445 (9th Cir. 1988)*). A court must decide such a motion before trial "unless it finds good cause to defer a ruling." *Fed. R. Crim. P. 12(d)*; *Shortt Accountancy, 785 F.2d at 1452* (*citing* former *Fed. R. Crim. P. 12(e)*).

DISCUSSION

Nosal argues that the Ninth Circuit's intervening decision in *Brekka*, requires this court to reconsider its decision to allow the government to proceed on the CFAA counts alleged against Nosal. In particular, Nosal asserts that under *Brekka*, the conduct that the superseding indictment alleges Nosal committed no longer constitutes a violation of the CFAA.

I. The CFAA Charges and this Court's April 13, 2009 Order

The provision of the CFAA in question makes it a crime 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 . . . ." *18. U.S.C. § 1030(a)(4)* (emphasis added). The CFAA does not define the term authorization. [*8] The term "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)*.

There are no allegations in the superseding indictment that Nosal personally accessed any protected computers "without authorization" or "exceed[ed] authorized access." Rather, the government alleges that three Korn/Ferry employees, defendant Christian and non-defendants J.F. and M.J., used their employee user accounts and passwords to access a protected computer belonging to Korn/Ferry, and, without authorization and by exceeding authorized access, downloaded, copied and duplicated source lists and other contact information from Korn/Ferry's proprietary "Searcher" database, and gave that information to Nosal. These actions were allegedly performed for Nosal's benefit and for the purpose of retaining clients and placing candidates as part of non-Korn/Ferry executive search activities.

In resolving Nosal's initial motion to dismiss the CFAA charges, the court was confronted with a central question: does an employee "act 'without authorization' or 'in excess [*9] of authorized access'" if he "accesses confidential and proprietary business information from his employer's computer that he has permission to access, but then uses that information in a manner inconsistent with the employer's interests or in violation of other contractual obligations, and . . . intended to use the information in that manner at the time of access"? *Nosal, 2009 U.S. Dist. LEXIS 31423, 2009 WL 981336, at *4*.

At the time, the question was one of first impression in the Ninth Circuit and there existed "two lines of diverging case law" outside of the Circuit. *2009 U.S. Dist. LEXIS 31423, [WL] at *5*. Courts advocating for a broad interpretation of the CFAA,

> [i]ncluding two courts of appeal, have . . . construed the [statute] to hold an employee acting to access an employer's computer to obtain business information with intent to defraud, i.e., for their own personal benefit or the benefit of a competitor, act 'without authorization' or 'exceed authorization' in violation of the statute.

Id. "These courts," the court wrote, "have generally held that authorized access to a company computer terminated once an employee acted with adverse or nefarious interests and against the duty of loyalty imposed on an employee in an agency relationship [*10] with his or her employer or former employer." *Id*. In contrast, those courts in favor of the narrow interpretation of the CFAA "[h]ave refused to hold employees with access and nefarious interests within the statute, concluding that a violation for accessing a protected computer . . . occurs only when initial access or the access of certain information is not permitted in the first instance." *Id*. The court recognized that these "[c]ourts have generally reasoned that the CFAA is intended to punish computer

hackers, electronic trespassers and other 'outsiders' but not employees who abuse computer access privileges to misuse information derived from their employment." *Id.* For a variety of reasons explained in the order, this court ultimately adopted the broader interpretation of the CFAA. *2009 U.S. Dist. LEXIS 31423, [WL] at *6-7.* Because the superseding indictment plainly alleged that Nosal and his co-conspirators accessed Korn/Ferry's computer system with nefarious intents, the court denied Nosal's motion to dismiss counts two through nine.

II. *LVRC Holdings, LLC v. Brekka*

On September 15, 2009, the Ninth Circuit decided *Brekka*, the case upon which Nosal exclusively relies in his motion for reconsideration. Brekka [*11] was employed by LVRC, a residential treatment center for addicted persons, to "oversee a number of aspects about the facility." *Brekka, 581 F.3d at 1129.* LVRC provided Brekka with an administrator's log-in so that he could access information about LVRC's website; through his employment, Brekka also had access to confidential lists of past and current LVRC patients, as well as to LVRC's financial statements, marketing reports and admissions reports. Prior to his separation from LVRC, Brekka emailed himself a number of these documents, which he later shared with his wife. On one occasion after Brekka ceased working for LVRC, someone used Brekka's administrator log-in to access the LVRC website; it was uncontested, however, that other individuals had access to Brekka's log-in username and password. Upon discovering that Brekka had retained the documents he emailed himself and allegedly attempted to access the LVRC website, LVRC brought a civil suit against him under the CFAA for violations of *18 U.S.C. sections 1030(a)(2)* and *(a)(4). See 18 U.S.C. § 1030(g)* (creating a private right of action for individuals or entities injured by conduct in violation of the CFAA). The district court [*12] granted Brekka's motion for summary judgment, and LVRC appealed. On appeal, LVRC argued solely that the district court erred by adopting an overly narrow interpretation of the term "without authorization." *See Brekka, 581 F.3d at 1135 n.7* ("On appeal, LVRC argues only that Brekka was 'without authorization' to access LVRC's computer and documents.").

The Ninth Circuit, surveying the statutory landscape created by the CFAA, held that to bring a successful action under *section 1030(a)(4)*, a plaintiff "must show that [the defendant]: (1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value' . . . ." [2] *Id. at 1131.* Unlike this court and other courts adopting the broader interpretation of the CFAA, the Ninth Circuit elected to separate the second and third elements of the prima facie case; in other words, whether an individual accesses a protected computer with or without an intent to defraud has no bearing on whether the individual acts with or "without authorization." Instead, "[a] person uses a computer 'without [*13] authorization' under *[section 1030(a)(4)* only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id. 1135*; *see also id. at 1133* ("[A] person who 'intentionally accesses a computer without authorization,' accesses a computer without any permission at all . . . .") (citations omitted).

> 2 Because *Brekka* was a civil suit, to establish liability, LVRC was also required to show that the Brekka's violation of the CFAA had caused LVRC a loss "during any one-year period aggregating at least $ 5,000 in value." *Brekka, 581 F.3d at 1132*; *see 18 U.S.C. § 1030(g)*

In so holding the court explicitly rejected the broader interpretation of "without authorization," most clearly articulated in *International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)*, a case upon which this court relied in denying Nosal's initial motion to dismiss. In *Citrin*, the Seventh Circuit held that an employee loses authorization to access a computer protected by the CFAA as soon as "the employee [*14] resolves to act contrary to the employer's interest." *Brekka, 581 F.3d at 1133-34.* In this way, *Citrin* predicates CFAA liability on an employee's duty of loyalty to their employer under state law; once an employee violates that duty while accessing a protected computer, the employee's authorization to access the computer is implicitly and immediately revoked. The Ninth Circuit elected not to follow *Citrin*, holding that the rule of lenity mandated that *section 1030(a)(4)* be interpreted narrowly. The rule of lenity counsels strongly against interpreting "criminal statutes in surprising and novel ways that impose unexpected burdens on defendants." *Id. at 1134. Section 1030(a)(4)* creates both

civil and criminal liability, meaning that the Ninth Circuit's interpretation of the provision would be "equally applicable in the criminal context." *Id*. Since nothing in the plain language of the CFAA "suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer . . . the defendant would have no reason to know that making personal use of the company computer" against the employer's interest "would [*15] constitute a criminal violation of the CFAA." *Id. at 1135*. In order to avoid this "surprising and novel result" and to ensure that individuals have clear notice of the conduct proscribed by the CFAA, the Ninth Circuit held that authorization hinges on the employer's conduct--has the employer granted the employee permission to access the computer?--not the employee's state of mind when accessing information or documents on the employer's computer. *Id. at 1133* ("It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'"); *id. at 1135* ("The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer.").

Because LVRC focused its appeal exclusively on whether the district court erred in its interpretation of the term "without authorization," *Brekka* provides less guidance regarding the meaning of the term "exceeds authorized access." Fortunately, as is mentioned above, the CFAA defines the term "exceeds authorized access." *Section 1030(e)(6) of the CFAA* states that an individual "exceeds authorized access" if he "access[es] [*16] 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)*. Interpreting that definition in dicta, the *Brekka* court recognized that "[a] person who 'exceeds authorized access,' has permission to access the computer, but accesses information on the computer that the person is not entitled to access." *Brekka, 581 F.3d at 1133* (citation omitted); *id. at 1135* ("The definition of the term 'exceeds authorized access' . . . implies that an employee can violate employer-placed limits on accessing information stored on the computer and still have authorization to access the computer.").

Reading *Brekka* in tandem with the statutory definition of "exceeds authorized access" makes clear that, as with those who access computers 'without authorization," intent and authorization are independent elements of the CFAA. In other words, 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. Thus, for example, if a person is authorized to access the "F" drive [*17] on a computer or network but is not authorized to access the "G" drive of that same computer or network, the individual would "exceed authorized access" if he obtained or altered anything on the "G" drive. Along these lines, the *Brekka* court wrote in dicta that it would have affirmed the district court had LVRC appealed the district court's holding that Brekka had not "exceed[ed his] authorized access" to LVRC's computer system. *Id. at 1135 n.7*.

III. Nosal's Motion to Reconsider

Quite clearly, *Brekka* implicates the reasoning employed by this court in initially denying Nosal's motion to dismiss the CFAA charges levied against him. Consequently, this court must reexamine its conclusion with respect to counts two through nine. This court previously held that the superseding indictment properly alleged that Nosal, Christian (Nosal's indicted co-conspirator) and J.F. and M.J. (his unindicted co-conspirators) accessed Korn/Ferry's computer system "without authorization" and "exceed[ed] authorized access." Central to the court's analysis was the conclusion that Christian, J.F and M.J.'s authorizations to access Korn/Ferry's computers were withdrawn the instant they intended to misappropriate [*18] the information they were obtaining. *Brekka* holds explicitly that an employee's intent in accessing a computer to which his employer has granted him access is irrelevant for determining whether the employee acted "without authorization," and holds implicitly that the same rule applies to the "exceeds authorized access" prong of *section 1030(a)(4)*. Therefore, to the extent that the superseding indictment is predicated on Christian, J.F. or M.J. accessing Korn/Ferry's computers while they were still employed by Korn/Ferry and still were permitted to access the Searcher database (in the form of valid, non-rescinded usernames and passwords), Nosal's motion to dismiss is granted.

The government argues that circumstances in *Brekka* are distinguishable from the allegations in the instant case and that this court could still hold that Nosal "exceed[ed] authorized access." They contend that whereas in *Brekka*,

there was an absence of any employment agreement or express company policy limiting the scope of his authorization to access the company's computer system, here there were a number of policies regulating the manner in which Nosal, Christian, J.F and M.J. could access and use the Korn/Ferry [*19] system. The superseding indictment alleges that "Korn/Ferry required all of its employees -- including the defendants David Nosal and Becky Christian -- to enter into agreements that both explained the proprietary nature of information disclosed or made available to Korn/Ferry employees (including the information contained in the Searcher database) and restricted the use and disclosure of all such information, except for legitimate Korn/Ferry business." Superseding Indictment P 10. Korn/Ferry also allegedly "declared the confidentiality of information in the Searcher database by placing the phrase 'Korn/Ferry Proprietary and Confidential' on every Custom Report generated from the Searcher database." *Id.* P 11. Finally, each time an individual logged in to a Korn/Ferry computer, a notice would appear explaining "[t]his computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without relevant authority can lead to disciplinary action or criminal prosecution." *Id.* The government argues that these notices and agreements defined the extent of a Korn/Ferry employee's access [*20] to the computer network. Therefore, when Nosal and his confederates violated these provisions, they "exceed[ed] authorized access."

Admittedly, *Brekka* provides some indication, in dicta, that an employer might be able to define the scope of an employee's access in terms of how the employee uses the information obtained from the computer system. *See Brekka, 581 F.3d at 1133* ("An individual who is authorized to use a computer for certain *purposes* but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.' ") (emphasis added). And *Brekka* is quite clear that it is the employer who determines whether or not an employee has access. *Id. at 1133, 1135*. However, in light of the rest of *Brekka*, a plain reading of the definition of "exceeds authorized access" compels a different conclusion. An 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 [*21] 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 [*22] that access and intent are separate elements. Accordingly, to the extent that the superseding indictment alleges that Christian, J.F or M.J. exceeded their authorization to access the Korn/Ferry system by violating Korn/Ferry's confidentiality and terms of use agreements, the superseding indictment would also fail to state a violation of *section 1030(a)(4)*. Christian, J.F. or M.J. only "exceed [] authorized access" to the extent the superseding indictment alleges they accessed information on Korn/Ferry's computer system that they did not have permission to access.

Applying *Brekka* to the superseding indictment, the court holds that some, but not all, counts must be dismissed. Counts two and four through seven allege that the Christian and J.F. were the individuals who accessed the Korn/Ferry computer system. In those counts, it is clear that when Christian and J.F. accessed the Korn/Ferry system, they did so *with* authorization and did not "exceed [] authorized access." In all five of those instances, the individual alleged to have accessed the computer was (1) still a Korn/Ferry employee (2) who had permission to access the entire Searcher database and (3) did not "obtain or alter information [*23] in the computer that the [he or she was] not entitled so to obtain or alter." [3] Under *Brekka*, such conduct does not violate

section 1030(a)(4). Accordingly, counts two and four through seven are DISMISSED.

> 3 In count two, the government alleges that Christian accessed the Searcher database in December 2004 with the intent to aid Nosal in defrauding Korn/Ferry; Christian was employed with Korn/Ferry until January 2005 and possessed authorization to access the Searcher database until that time. Similarly, in counts four through seven, the government alleges that J.F. accessed the Searcher database once in April, once in May, and twice in June 2005, with the intent to aid Nosal in defrauding Korn/Ferry; J.F. remained employed with Korn/Ferry until August 2005 and had Korn/Ferry's permission to access the Searcher database until that time. Thus, in each of these instances, neither Christian nor J.F. acted "without authorization" or "exceed[ed] authorized access".

Counts three, eight and nine present more complicated questions. In count three, the government alleges that on or about April 12, 2005, someone downloaded three Korn/Ferry "source lists" of chief financial officers ("CFOs") from [*24] the Searcher database using J.F.'s username and password and then emailed the source lists to Nosal. Superseding Indictment P 19b. The superseding indictment does not identify the individual who logged in to the Searcher system or whether the individual accessed parts of the system that they were not authorized to access. At the hearing on this motion, the government proffered that at trial, it would establish that Christian used J.F.'s username and password to log-in to the Korn/Ferry system and run the queries. In count eight, the government alleges that on or about July 12, 2005, someone located in Nosal's new offices used J.F.'s username and password to log-in to Korn/Ferry's computer network to run two queries on specific candidates for a CFO position. *Id.* P 19f. Again, the superseding indictment does not specify who logged in to the system or whether the individual accessed parts of the system that they were not authorized to access. At the hearing, the government stated that at trial, it would introduce evidence that J.F. logged in to the system, but that Christian ran the queries. Although generally, the court must only consider the contents of the indictment on a motion to [*25] dismiss, the court will allow these counts to proceed to trial. If the government can establish that in counts three and eight Christian accessed the Korn/Ferry system after her employment with Korn/Ferry had terminated, then the government would meet its burden; Christian would have accessed a protected computer "without authorization." If, however, the government fails at trial to introduce evidence identifying who accessed the Korn/Ferry system in counts three and eight, the court will consider dismissing those counts. Further, if, as in counts two and four through seven, the evidence indicates that the individual who accessed the system and ran the queries in the Searcher database was authorized to do so at the time, the court will consider dismissing counts three and eight. Accordingly, Nosal's motion to reconsider the dismissal of counts three and eight is DENIED without prejudice to renewing the motion after the government has presented its case.

Count nine is the only count, in light of *Brekka*, in which the government clearly alleges that an individual "without authorization" to access the Korn/Ferry system actually accessed the system. The superseding indictment alleges that [*26] on or about July 29, 2005, "using M.J.'s computer located in Nosal's new offices in San Francisco, J.F. remotely logged into Korn/Ferry's computer network with her Korn/Ferry username and password. Once logged in, J.F. returned control of the computer to M.J. M.J. then proceeded to query Korn/Ferry's Searcher database and download information, including 25 Korn/Ferry source lists, from that database onto the computer." Superseding Indictment P 19o. At that time, M.J. was no longer a Korn/Ferry employee. Thus, in this instance, M.J., an individual who lacked permission to access the system, did in fact access the Korn/Ferry network, conduct that if proven at trial would be sufficient to establish a "without authorization" violation of *section 1030(a)(4)*. Accordingly, Nosal's motion to reconsider is DENIED with respect to count nine.

CONCLUSION

For the foregoing reasons, defendant Nosal's motion for reconsideration is GRANTED in part and DENIED in part. Counts two and four through seven are DISMISSED.

IT IS SO ORDERED.

Dated: January 5, 2010

/s/ Marilyn Hall Patel

MARILYN HALL PATEL

United States District Court Judge Northern District of California