STEVEN F. GRUEL (CSBN 213148)
Attorney at Law
100 Pine Street, Suite 600
San Francisco, CA 94122
Telephone Number: (415) 989-1253
Fax Number: (415) 576-1442
attystevengruel@sbcglobal.net

DENNIS P. RIORDAN (SBN 69320)
DONALD M. HORGAN (SBN 121547)
RIORDAN & HORGAN
523 Octavia Street
San Francisco, CA 94102
Telephone Number: (415) 431-3472
Fax Number: (415) 552-2703
dennis@riordan-horgan.com
Attorneys for David Nosal

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>vs.<br><br>DAVID NOSAL, et al.,<br><br>Defendants. | No. CR-08-0237-MHP<br><br>Date: February 17, 2009<br>Time: 11:00 a.m.<br>Courtroom: Hon. Marilyn Hall Patel |

**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION TO DISMISS INDICTMENT FOR FAILURE TO STATE AN OFFENSE**

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

### CASES

**Table of Authorities continued**

**Table of Authorities continued**



**STATUTES**



**MISCELLANEOUS**

## INTRODUCTION

As the indictment alleges, defendant David Nosal was a high level executive at an international executive search firm, Korn/Ferry International (KFI), for over eight years. He left the firm in October of 2004 with a plan to eventually start his own search firm. KFI had two interests it wished to further upon Mr. Nosal's departure: (1) to have Mr. Nosal continue to generate revenue for KFI by completing ongoing searches he had been engaged in; and (2) to prevent Mr. Nosal from competing with KFI for a substantial period of time after he left the firm. KFI sought to achieve both objectives by entering into a separation agreement with Nosal under the terms of which, as an independent contractor, Nosal (a) would "cooperate with Korn/Ferry on certain ongoing search assignments" and (b) would not "perform executive search, executive placement, management assessment, management audit services, on behalf of any other entity than Korn/Ferry during the period the Nosal-Korn/Ferry agreements were in effect." (Indictment, Paragraph 2)

That agreement, attached to this Pleading as Exhibit A, was incorporated by reference into the Indictment in this matter and thus is before for the court for the purpose of assessing the facial sufficiency of the indictment.[1] The agreement expressly states that it is subject to California law and that any disputes arising between the parties will be arbitrated in California. (Exhibit A, at paragraphs 26 and 27).

As to the first objective of KFI, it is apparent that the compensation to be paid Mr. Nosal under the agreement was contingent on Mr. Nosal's exercising his best efforts to continue to make money for KFI between October 2004 and October 2005 by working on executive searches that he had been conducting when he left full-time employment with the firm. (Exhibit A, at paragraphs 2 and 3.) Nosal was to receive $25,000 a month during the year he worked as an

[1] Under the doctrine of incorporation by reference, this Court may consider the contents of the relevant separation agreements in deciding Mr. Nosal's facial challenges to the indictment. *See United States v. Ritchie*, 342 F.3d 903 (9th Cir. 2003) ("Even if a document is not attached to a complaint, it may be incorporated by reference into a complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim.").

independent contractor, but most of his compensation for that year's work was to be in the form of two large lump sum payments to be disbursed on July 31st and October 15th, 2005. (Indictment, paragraph 2).

There is no allegation in the Indictment that Mr. Nosal failed to do the work contracted for or failed to generate the income KFI anticipated it would receive. In July of 2005, however, KFI claimed that Nosal had violated the non-compete provisions of the agreement, and that he or persons associated with him had misappropriated proprietary information after Nosal left to start a competing executive search firm. On that basis, KFI stopped paying Nosal his monthly stipend of $25,000 and refused to make the initial lump sum payment due on July 31st, 2005.[2] Accordingly, and quite appropriately, the competing claims of the parties for money damages were submitted to arbitration proceeding.

Whatever the merits of the dispute between KFI and Mr. Nosal, they fundamentally involve civil matters, and matters of state law. Much to the benefit of KFI, however, the government now seeks to convert the matter into a federal criminal prosecution of Mr. Nosal. In its effort to fit a square peg into a round hole, the government has creatively charged a variety of counts under several statutory provisions.

In one set of charges, the government alleges that Mr. Nosal accessed a computer without authorization in violation of the Computer Fraud and Abuse Act. But the government only alleges misappropriation, which is not covered by statute. Those charges thus fail to state an offense.

In another set of charges, the government alleges that Mr. Nosal committed mail fraud by violating his contract with KFI, by failing to disclose the violation, and by receiving monthly stipend payments in the mail. But federal courts have held that an undisclosed breach of contract does not constitute fraud, and in this instance, the relevant contractual provision is unenforceable

---

[2] The indictment alleges Nosal defrauded KFI of eight monthly stipend payments for November of 2001 through June of 2005. (Indictment, paragraph 34). It does not allege a defrauding of the monthly payment for July of 2005 or the lump sum payment due that month (or the one due in October of 2005) because they were never made to Mr. Nosal.

as a matter of state law, as the California Supreme Court recently made strikingly clear. *See Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (2008). A failure to fulfill an invalid contract provision does not a federal fraud make. The mail fraud charges thus also fail to state an offense.

That leaves the two counts that allege theft and misappropriation of trade secrets in violation of the Economic Espionage Act. But those two counts are multiplicitous, since they allege the same crime twice. Furthermore, and perhaps more fundamentally, neither count alleges knowledge of illegality, which is an essential element of the offense. Thus, at least as currently pled, those counts also fail to state an offense.

Mr. Nosal therefore moves under Fed. R. Crim. Pro. 12 to dismiss all counts in the indictment against him.

## ARGUMENT

### I. COUNTS TWO THROUGH NINE MUST BE DISMISSED BECAUSE THE INDICTMENT ALLEGES MISAPPROPRIATION, WHICH IS NOT COVERED BY THE COMPUTER FRAUD AND ABUSE ACT

The Superseding Indictment alleges eight violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(4). That provision, in relevant part, makes it a crime for a person to "knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access." The indictment alleges that KFI employees Christian and J.F. used their employee passwords to access KFI's proprietary Searcher database, and then transferred the information to Christian & Associates. It alleges, in other words, that Nosal and his co-conspirators misappropriated information obtained from KFI's databases.

But the indictment fails to state violations of the CFAA because the CFAA does not reach misappropriation. As a result, the eight CFAA counts must be dismissed.

#### A. The Meaning of "Authorization"

The core legal question has to do with the meaning of "authorization" under the CFAA, and what it means to "exceed authorized access." The CFAA was aimed primarily at hackers. The government will argue that the CFAA also extends to cover employees who misappropriate information, and specifically that the CFAA reaches employees who violate contractual

confidentiality agreements by using employer-owned information in a manner inconsistent with those agreements.

A growing number of courts, however, have rejected such a broad interpretation of the CFAA. *See, e.g.*, *Condux Int'l, Inc. v. Haugum*, 2008 U.S. Dist. LEXIS 100949 at * 18 (D. Minn. Dec. 18, 2008) (quoting *Shamrock Foods*, 535 F. Supp. 2d at 967) ("The Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA."); *Black & Decker v. Smith*, 568 F. Supp. 2d 929, 936 n.3 (W.D. Tenn. 2008) (finding that Congress did not "intend[] to criminalize the breach of private confidentiality agreements in situations where the confidential information is accessed via a computer").[3]

The nation's leading computer crime scholar has also rejected the government's broad "misappropriation" theory of the CFAA. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. Rev. 1596, 1650-60 (2003). As Professor Kerr concluded, "[a]ccess that merely breaches a contract conditioning access should not suffice to trigger criminal liability," in part because such a broad construction of the statute would lead to absurd results and would render the statute unconstitutional. *Id*. at 1643, 1655-60.

There is a split of authority on the issue, and some courts have — in civil cases — adopted the broad "misappropriation" theory of the CFAA. *See Haugum*, 2008 U.S. Dist. LEXIS 100949 at *11 nn.3-4 (collecting cases), a development that has been criticized as opening a Pandora's Box. *Kerr*, *supra*, at 1640 ("By using the law to aid sympathetic plaintiffs, the courts [adopting the broad theory] inadvertently have handed prosecutors a broad and powerful tool to punish breaches of contracts relating to computer use.").

---

[3] The scope of the CFAA has received renewed attention recently as a result of the prosecution of Lori Drew. In that case, the government used a similarly expansive theory of liability under the CFAA to obtain criminal convictions based on evidence that the defendant used MySpace in a way that violated the website's terms of service. The validity of those convictions remains disputed. *See United States v. Lori Drew*, Case No. CR-08-582-GW (C.D. Cal.).

The Ninth Circuit has not yet ruled on the issue,[4] but this court should adopt the narrow interpretation for three reasons. First, the narrow interpretation is supported by the plain meaning of the statutory language. Second, the narrow interpretation is supported by the legislative history of the CFAA. Third, because the CFAA does not clearly cover a broader range of conduct, the rule of lenity compels adoption of the narrow interpretation.

*1. Plain Meaning*

The narrow interpretation of the CFAA is most consistent with the plain meaning of the statutory language and the structure of the statute. *See Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008). The CFAA criminalizes both accessing a computer without authorization, and also exceeding authorized access. It defines the term "exceeding authorized access" as "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).

> Section 1030(e)(6) contemplates that an "exceeds authorized access" violation occurs where the defendant first has initial "authorization" to access the computer. But, once the computer is permissibly accessed, the use of that access is improper because the defendant accesses information to which he is not entitled. Under [the broad reading of the statute], however, that distinction is overlooked. Under [that] reasoning, an employee who accesses a computer with initial authorization but later acquires (with an improper purpose) files to which he is not entitled--and in so doing, breaches his duty of loyalty--is "without authorization," despite the Act's contemplation that such a situation constitutes accessing "with authorization" but by "exceed[ing] authorized access." 18 U.S.C. § 1030(e)(6). The construction of [the broad reading] thus conflates the meaning of those two distinct phrases and overlooks their application in § 1030(e)(6).

*Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1342-43 (D. Ga. 2007).

"Thus, the plain language of § 1030(a)(2), (4), and (5)(A)(iii) target 'the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" *Gast*, 535 F.Supp. 2d at 965 (quoting *Brett Senior & Assocs*. v. *Fitzgerald*, 2007 U.S. Dist. LEXIS 50833

---

[4] In a related context, however, the Ninth Circuit has held that "[n]ot all deceit vitiates consent." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2003). Thus, under the Stored Communications Act, the mere fact that authorization is obtained by deceit does not render access "unauthorized" under the statute.

(E.D. Pa. 2007); *see also Haugum*, 2008 U.S. Dist. LEXIS 100949 at * 15 ("Had Congress intended to target how a person makes use of information, it would have explicitly provided language to that effect.").

*2. Legislative History*

The legislative history of the CFAA also confirms the narrow view. The primary purpose of the CFAA "was to create a cause of action against computer hackers (e.g., electronic trespassers)." *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 495-96 (D. Md. 2005) (citing S. Rep. No. 99-432, at 4 (1986)). As the House Report explained, the bill was aimed largely at hackers who "trespass into" computers: "[T]he conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense." H.R. Rep. No. 98-894, at 10-11, 20 (1984), as reprinted in 1984 U.S.C.C.A.N. 3689, 3695-97, 3706.

Moreover, and most importantly, the "exceeding authorized access" language and definition was added in a 1986 amendment, and the purpose of that amendment was to *narrow* the scope of liability and disavow the "murkier" theory of liability based on misappropriation.

> By enacting this amendment, and providing an express definition for "exceeds authorized access," the intent was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,'" thereby "remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization."

*Werner-Matsuda*, 390 F. Supp. 2d at 499 n.12 (quoting S. Rep. No. 99-432, at 21 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2494-95).

In short, "the legislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information." *Gast*, 535 F.Supp. 2d at 966.

*3. Rule of Lenity*

Finally, and perhaps most critically, because this is a criminal case, this Court is bound by the rule of lenity. At a minimum, the split of authority among courts demonstrates that

reasonable people could disagree about the scope of the statute. As a result, under the rule of lenity, this Court must adopt the narrower reading. *See United States v. Lanier*, 520 U.S. 559, 266 (1997) (stating that the rule of lenity "ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered").

Even if it were proper to adopt a broad reading of the CFAA in civil cases (where the rule of lenity does not apply), it would be improper to apply that broad reading to a criminal defendant such as Mr. Nosal. And indeed, there do not appear to be any reported cases applying the broad "misappropriation" theory of the CFAA to criminal defendants.

Justice Scalia recently explained, in his typically penetrating fashion, the importance of the rule of lenity:

> This venerable rule not only vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain, or subjected to punishment that is not clearly prescribed. It also places the weight of inertia upon the party that can best induce Congress to speak more clearly and keeps courts from making criminal law in Congress's stead.

*United States v. Santos*, 128 S. Ct. 2020, 2025 (2008). If Congress wishes to criminalize misappropriation under the CFAA, it may do so, and if the Department of Justice seeks the power to prosecute such conduct, it may lobby Congress to make the change. But until Congress clearly prescribes such conduct, a criminal defendant may not be held liable. Under the statutes as it is currently written, misappropriation and breach of contract are insufficient as a matter of law to trigger criminal liability.

**B. The CFAA Counts**

Under the authority discussed above, all eight CFAA counts against Mr. Nosal must be dismissed.

Count 2 alleges that, while she was still a KFI employee, Ms. Christian used her KFI computer user account to run searches, and then misappropriated the data obtained for the benefit of Christian & Associates. The count, on its face, rests entirely on a misappropriation theory, and therefore must be dismissed.

Counts 4, 5, 6, 7, and 9 allege that, while she was still a KFI employee, J.F. used her KFI

user account to run searches, and then misappropriated the data obtained for the benefit of Christian & Associates. Those counts, on their face, likewise rest entirely on a misappropriation theory, and therefore must be dismissed.

The factual bases of Counts 3 and 8 are somewhat less clear. Count 3 is based on an April 12, 2005, search using J.F.'s user account. The indictment states that the search was run "using J.F.'s Korn/Ferry username and password" (Indictment, paragraph 19(b)), but it does not specify whether J.F. herself ran the search, or whether Ms. Christian ran the search using J.F.'s access. Count 8 is based on a July 12, 2005, search using J.F.'s user account. The indictment states that on that day, "using a computer at Nosal's new offices in San Francisco, an individual remotely logged into Korn/Ferry's computer network using J.F.'s username and password" and ran a search. (Indictment, paragraph 19(f).) The indictment does not specify whether the search was run by J.F. herself or Ms. Christian. In paragraph 16 of the indictment, however, which is part of the broad conspiracy count and incorporated into the CFAA counts, it is alleged that the defendants gained access to the Korn/Ferry computers "*by using their own Korn/Ferry user names and passwords*." (Emphasis added). Read in the light of that language, Counts 3 and 8 also allege access by means of a legally obtained pass word, and misappropriation in violation of a contract provision. They also must be dismissed.

Furthermore, the indictment contains no allegations sufficient to state a crime by Mr. Nosal. The indictment does not allege that Mr. Nosal himself ran any searches using J.F.'s password, nor does it allege that he assisted anyone else in doing so. Rather, the indictment appears to allege that Mr. Nosal received information that was obtained by J.F. and Ms. Christian. Unlike other criminal provisions, the CFAA does not criminalize mere receipt of illegally-obtained information. Furthermore, the separation agreement makes apparent that Mr. Nosal would be in possession of confidential information while acting as an independent contractor for KFI. (Exhibit A, at paragraph 18). As elucidated above, misuse of any such confidential information in violation of a contract provision does not constitute a violation of the CFAA.

In short, even assuming that every allegation in the indictment is true, the indictment

contains no valid CFAA charge against Mr. Nosal. All eight CFAA counts should be dismissed.

## II. COUNTS 10 AND 11 MUST BE DISMISSED BECAUSE THEY FAIL TO ALLEGE AN ESSENTIAL ELEMENT OF THE OFFENSE — NAMELY, KNOWLEDGE OF ILLEGALITY

Counts 10 and 11 both allege violations of the Economic Espionage Act (EEA), 18 U.S.C. § 1832. The EEA was passed in 1996, and it has been prosecuted relatively rarely, so there is little case law interpreting it. It is worth noting that the United States Attorney's Manual cautions that "[t]he EEA is not intended to criminalize every theft of trade secrets for which civil remedies may exist under state law," and strongly suggests that prosecutions should be reserved for cases involving the theft by foreign agents of information important to national security.[5]

The statute created a novel definition of "trade secret" that was broader than the definitions used in most civil statutes and in the Uniform Trade Secrets Act. *See United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998). Moreover, the precise statutory definition of "trade secret" is unclear, and courts and commentators have disagreed about how it should be interpreted. *See United States v. Lange*, 312 F.3d 263, 266 (7th Cir. 2001) (Easterbrook, J.) (discussing problems with the definition). Finally, while the statute was designed to punish misuse of intangible employer property, it "was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor." *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000). The distinction is insolubly hazy.

For these reasons, two of the leading cases addressing the statute have determined that in order to survive constitutional challenges, the EEA must be interpreted to include an additional mens rea element that is not specified in the statutory text. *See United States v. Krumrei*, 258 F.3d 535 (6th Cir. 2001); *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999). The defendants in *Hsu* and *Krumrei* argued that because the statute is so broad and under-defined, it violates the void-for-vagueness doctrine. The courts rejected those challenges — but only because they found that in those cases, the defendants had knowledge of illegality. As the Sixth Circuit held, relying on *Hsu*, "[b]ecause the defendant knew that the information was proprietary

---

[5] United States Attorney's Manual, 9-59.100, Economic Espionage

and knew that his actions were illegal, the statute was constitutional as applied to him." *Krumrei*, 258 F.3d 539.

In other words, in order to avoid constitutional difficulties, the courts in *Krumrei* and *Hsu* narrowed the scope of the statute by reading into it an additional mens rea element. As interpreted by *Krumrei* and *Hsu*, the statute requires proof of the defendant's knowledge of the illegality of his actions. If the statute were not so interpreted, its lack of definition would render it constitutionally invalid.

Put simply, knowledge of illegality is a necessary element of the offense. And yet the government's indictment in this case makes no allegation that Mr. Nosal knew that his actions were illegal. *See Apprendi v. New Jersey*, 530 U.S. 466, 476 (2000) (stating that every element of a criminal offense "must be charged in an indictment, submitted to a jury, and proven beyond a reasonable doubt."). Because Counts 10 and 11 fail to allege a necessary element of the offense, they must be dismissed.

## III. BECAUSE COUNTS 10 AND 11 ARE MULTIPLICITOUS, ONE OF THEM MUST BE DISMISSED

Even aside from the failure to allege knowledge of illegality, Counts 10 and 11 are invalid because they are multiplicitous. The two counts are based on the same instance of conduct, and they are charged under different subdivisions of the EEA. But because those different subdivisions are merely different means of committing the same offense, they cannot be charged separately.

The EEA proscribes several different kinds of conduct. Subdivision (a)(1) prohibits, among other things, theft and misappropriation of trade secrets. Subdivision (a)(2) prohibits, among other things, downloading trade secrets. Subdivision (a)(3) prohibits knowing receipt of stolen trade secrets. In addition to the three substantive subdivisions, the statute also specifies two forms of derivative liability for attempt and conspiracy under subdivisions (a)(4) and (a)(5).

Both Counts 10 and 11 are based on the same instance of conduct — both counts are based on the April 12, 2005, appropriation of the CFO source lists. The government charged Count 10 as a violation of both subdivision (a)(1) and subdivision (a)(2). It charged Count 11 as

a violation of subdivision (a)(3). But because the three substantive subdivisions are simply alternative means of committing the same crime, the two counts are multiplicitous.

> In determining whether the statute at issue creates separate offenses, or simply describes alternative means to commit the same crime, we employ the analytical framework established in [*United States v. UCO Oil Co.*, 546 F.2d 833, 837 (9th Cir. 1976)]. Under *UCO Oil*, we consider "several relevant factors," including: (1) "language of the statute itself," (2) "the legislative history and statutory context," (3) the type of conduct proscribed, and (4) the "appropriateness of multiple punishment for the conduct charged in the indictment."

*United States v. Arreola*, 446 F.3d 926, 930 (9th Cir. 2006).

In this case, the statutory language and framework strongly suggest that the different subdivisions are simply alternative means to commit the same crime. All subdivisions are punished to the same degree, and the different forms of proscribed conduct tend to merge into one another. *See id*. at 930-33. Moreover, the derivative forms of liability for attempt (subdivision (a)(4)) and conspiracy (subdivision (a)(5)) also apply equally, and without any distinction, to the three substantive subdivisions.

Because the different subdivisions are simply alternative means to commit the same crime, Counts 10 and 11 are multiplicitous.[6] Two counts are multiplicitous when the same conduct forms the basis of two counts charged under the same statute. *See United States v. Zalapa*, 509 F.3d 1060, 1063-64 (9th Cir. 2007); *see also United States v. Keen*, 104 F.3d 1111, 1118 (9th Cir. 1996) (describing one species of multiplicity that appears where "a single act or transaction is alleged to have resulted in multiple violations of the same statutory provision"). The government may proceed on one count or the other, but it may not proceed on both.

---

[6] If the three subdivisions are instead interpreted as creating separate offenses, then Count 10 is duplicitous because it charges two offenses in a single count. "Either the [three] subsections create [three] distinct offenses . . . or they do not." *Williams v. Warden*, 422 F.3d 1006, 1009 (9th Cir. 2005). Either way, the government has improperly charged the crime.

Moreover, if the three subdivisions were interpreted as creating separate offenses, it would be doubtful whether Count 10 properly alleges an offense anyway, because as the indictment makes clear, the government's factual allegation is that Mr. Nosal received trade secrets that were stolen or misappropriated by Ms. Christian or J.F., not by Mr. Nosal himself.

## IV. BECAUSE THE UNDERLYING CFAA AND EEA COUNTS FAIL TO STATE OFFENSES, THE CONSPIRACY COUNT MUST BE DISMISSED AS WELL

Count 1 of the indictment alleges a conspiracy to violate the CFAA and the EEA. (Indictment, paragraph 13.) For the reasons given above, the indictment fails to state an offense under the CFAA and the EEA. As a result, the Count 1 conspiracy charge also fails to state an offense, and must be dismissed. *See United States v. Carman*, 577 F.2d 556, 567-68 (9th Cir. 1978).

## V. THE MAIL FRAUD COUNTS MUST BE DISMISSED BECAUSE AN UNDISCLOSED BREACH OF AN INVALID CONTRACTUAL PROVISION DOES NOT CONSTITUTE FRAUD

This entire prosecution is fundamentally problematic because it attempts to convert a contract dispute — which is paradigmatically a civil matter, and a matter of state law — into a federal criminal case. The mail fraud conspiracy and substantive charges (Counts 12 to 20) in particular bring that problem into the highest relief. Those counts, on their face, rest at their core on a claim that Mr. Nosal's alleged breach of contract also constituted criminal fraud.

The government alleges "in sum and substance" that Mr. Nosal committed fraud because he deceived KFI "regarding the defendant Nosal's executive search-related activities that were in violation of the Nosal-Korn/Ferry Agreements." (Indictment, paragraph 27.) It alleges that "after Nosal entered into the Nosal-Korn/Ferry Agreements, Nosal took actions to circumvent those agreements by conducting his own executive search-related activities." (Indictment, paragraph 30.) It alleges that he conducted a side business in violation of those agreements. (Indictment, paragraph 31.) And it alleges that he deceived KFI because he both falsely told KFI that he was complying with the agreements, and because he failed to disclose that he was violating the agreements. (Indictment, paragraph 32.)

In short, the government alleges that Mr. Nosal committed a fraud by violating the non-compete provision of a separation agreement by hiding his breach from the other contracting party. But as a matter of law, that allegation, even if true, does not constitute mail fraud. The government cannot convert a mere breach of contract into a federal crime, especially where the relevant contractual provision is invalid as a matter of state law. Because the government's

theory is legally invalid, all of the mail fraud counts — Counts 12 to 20 — should be dismissed.

**A. Fraud Arising From Contractual Relationships**

It is well-settled that a breach of contract does not constitute mail fraud. Every circuit to consider the matter has concluded that "[f]raud requires much more than simply not following through on contractual or other promises." *Corley v. Rosewood Care Ctr.*, 388 F.3d 990, 1007 (7th Cir. 2004); *see, e.g.*, *United States v. Chandler*, 388 F.3d 796, 803 (11th Cir. 2004) ("The government agreed that breach of contract does not support a mail fraud conviction."); *McEvoy Travel Bureau, Inc. v. Heritage Travel, Inc.*, 904 F.2d 786, 791 (1st Cir. 1990) ("[N]or does a breach of contract in itself constitute a scheme to defraud."); *United States v. Kreimer*, 609 F.2d 126, 128 (5th Cir. 1980) ("[T]he [mail fraud] statute does not reject all business practices that do not fulfill expectations, nor does it taint every breach of a business contract."); *see also United States v. Vinyard*, 266 F.3d 320, 327 (4th Cir. 2001); *Johnson Enters v. Fpl Group*, 162 F.3d 1290, 1318-19 (11th Cir. 1998); *United States v. Cochran*, 109 F.3d 660, 667 (10th Cir. 1997); *Kehr Packages v. Fidelcor, Inc.*, 926 F.2d 1406, 1417 (3d Cir. 1991).

The government's mail fraud allegations, on their face, squarely conflict with this line of authority. And the government's allegation that Mr. Nosal committed fraud by failing to disclose his breach to the other party is nothing more than a semantic trick designed to evade the holdings of all of the cases cited above. If the failure to disclose a breach of contract constituted fraud, then nearly every breach of contract would constitute fraud. That is precisely the result that these cases foreclose.

When the government seeks a mail fraud prosecution in cases arising out of contractual relationships, "much more" than a mere undisclosed breach is required. *Corley*, 388 F.3d at 1007. At a minimum, fraud "requires a showing of deception *at the time the promise is made*." *Id* (emphasis added). In this case, the government has made no such allegation. In fact, to the contrary, the language of the indictment suggests that the alleged breach and deceptions did not take place until at least the beginning of 2005, months into the contract.

The government must also show that the defendant intended to cause actual economic harm to the other contracting party, and that the defendant's actions created an "independent

business risk" to the other party. *See United States v. Pennington*, 168 F.3d 1060, 1065 (8th Cir. 1998); *United States v. Sun-Diamond Growers*, 138 F.3d 961, 973 (D.C. Cir. 1998). But once again, in this case, the government has made no such allegations. Critically, the indictment makes no allegation that Nosal failed to perform the work called for under the contract — other than the contract violation and loss of loyalty, the indictment makes no allegation of actual or intended economic harm to KFI. Indeed, what is apparent is that this entire dispute has worked to the economic benefit of KFI, as the corporation has used Mr. Nosal's alleged failure to honor the illegal non-compete clause as a rationale for refusing to pay the very substantial fees it owes him for his successful completion of executive searches while serving as an independent contractor for KFI in 2004 and 2005.

Ultimately, to support its mail fraud charges, the government has simply alleged an undisclosed breach of an employment agreement. That allegation is insufficient as a matter of law to state an offense. As the D.C. Circuit explained:

> [P]remising a felony solely on a scheme to defraud an employer of the loyal services of his employee has spawned a fierce debate about potential over-criminalization of employer-employee breakdowns, better handled in the civil courts. Carried to its logical extreme, such a theory would criminalize any intentional undisclosed breach of duty to an employer. The government appears to be arguing just such a theory here, but we are not inclined to accept it . . . .

*United States v. Lemire*, 720 F.2d 1327, 1336 (D.C. Cir. 1983) (footnote omitted). This court should similarly reject the government's novel and expansive theory of fraud liability.

**B. California Law on Noncompetition Agreements**

Even if an undisclosed breach of contract were generally tantamount to fraud, it could not possibly constitute fraud in this case, where the underlying contractual provision is invalid and unenforceable.

Under California law, which governs the separation agreements in this case, noncompetition agreements are unenforceable. Under Cal. Bus. & Prof. Code § 16600, except as otherwise provided, "every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void." California courts have

construed that provision broadly in favor of employees. In fact, the California Supreme Court recently reaffirmed that § 16600 prohibits all noncompetition agreements unless they fall within one of California's narrow statutory exceptions. *See Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (2008).

Federal courts hearing California contract disputes (in cases of diversity and supplemental jurisdiction) had construed the statute more narrowly. In a series of cases, the Ninth Circuit held that under § 16600, only agreements that entirely precluded employees from practicing their trade were invalid. *See, e.g.*, *International Business Machines Corp. v. Bajorek*, 191 F.3d 1033 (9th Cir. 1999); *General Commercial Packaging v. TPS Package*, 126 F.3d 1131 (9th Cir. 1997).

In *Edwards*, however, the California Supreme Court forcefully — even angrily — rejected those misguided federal cases. "[N]o reported California state court decision has endorsed the Ninth Circuit's reasoning, and we are of the view that California courts have been clear in their expression that section 16600 represents a strong public policy of the state which should not be diluted by judicial fiat." 44 Cal. 4th at 949. Of course, it is the California Supreme Court opinion that controls on this issue of state contract law.

Under *Edwards*, the noncompetition provisions contained in Mr. Nosal's separation agreements are unenforceable. And yet it is precisely those provisions that give rise to the government's theory of mail fraud liability. The government's apparent theory is that by violating an illegal contract provision, and by failing to disclose to KFI that he was violating that provision, Mr. Nosal committed the federal crime of mail fraud. But under California law, employees cannot be bound by such provisions — in fact, an employer may not even lawfully condition employment on an employee's willingness to sign such an agreement. *Edwards*, 44 Cal. 4th at 950. The government's theory of the mail fraud charges is simply untenable as a matter of law.

The mail fraud charges in this case rest, at their core, on an allegation of an undisclosed breach of an employment contract. Even as a general matter, such a theory is dubious. Here, where the contractual provision at issue is illegal, the government's theory cannot remotely

support a criminal charge.

**C. Principles of Federalism**

If the government's theory of mail fraud were accepted, it would amount to a federal veto of California's law on noncompetition agreements. The prosecution's implicit position is that even though such provisions are unenforceable as a matter of state civil law, they are nonetheless enforceable as a matter of federal criminal law. But the Supreme Court has warned about deploying the federal fraud statutes in ways that undermine areas of traditional state law authority.

In *Cleveland v. United States*, 531 U.S. 12 (2000), for example, the Court rejected the government's attempt to use the mail fraud statutes to punish false statements made in state license applications. According to the Court, such prosecutions would constitute a "sweeping expansion of federal criminal jurisdiction" and "would subject to federal mail fraud prosecution a wide range of conduct traditionally regulated by state and local authorities." *Id*. at 25. The Court so held even though state law also made false statements on license applications illegal. *See id*. at 23. In this case, the federal state conflict would be even worse, because rather than simply *supplementing* state law on the underlying issue, prosecution would directly *undermine* California's "strong public policy" against noncompetition agreements.

The same federalism concerns undergird the Tenth Amendment, which was enacted to allay lingering concerns about the extent of the national power and to eliminate any doubt whether the federal government possesses only limited, enumerated powers, which must yield in some instances to the sovereignty of the states. *Alden v. Maine*, 527 U.S. 706, 713-14 (1999). The Tenth Amendment works in tandem with the Commerce Clause to ensure that the federal government legislates in areas of truly national concern, while the states retain independent power to regulate areas better suited to local governance. *Conant v. Walters*, 309 F.3d 629, 647 (9th Cir.2002) (Kozinski, J., concurring). To this end, the Amendment provides an affirmative, external limitation on the federal government's exercise of its delimited powers. *See Reno v. Condon*, 528 U.S. 141, 149 (2000); *Fry v. United States*, 421 U.S. 542, 547 n. 7(1975); *ACORN v. Edwards*, 81 F.3d 1387, 1393 (5th Cir. 1996).

The Ninth Circuit already erred and upset the state-federal balance with its misguided interpretation of California state law on noncompetition agreements. It was precisely that error that led to the California Supreme Court's forceful corrective ruling in *Edwards*, which disapproves the Ninth Circuit's interpretation of Cal. Bus. & Prof. Code § 16600. This Court should not allow the federal executive to trump *Edwards* with a dubious expansion of the mail fraud statute.

Counts 12 to 20 should be dismissed for failure to allege a crime.

**CONCLUSION**

For the reasons stated, all twenty counts of the Indictment should be dismissed.

Dated: January 12, 2009

Respectfully submitted,

STEVEN F. GRUEL

DENNIS P. RIORDAN
RIORDAN & HORGAN

By/s/ Steven F. Gruel
STEVEN F. GRUEL

By /s/ Dennis P Riordan
DENNIS P. RIORDAN

Counsel for Defendant
DAVID NOSAL