

1 SCOTT N. SCHOOLS (SC 9990)
Associate Deputy Attorney General
2 Acting United States Attorney

3 KYLE F. WALDINGER (ILSB 6238304)
Assistant United States Attorney

4 450 Golden Gate Avenue, 11th Floor
5 San Francisco, California 94102
6 Telephone: (415) 436-6830
Facsimile: (415) 436-7234

7 Attorneys for Plaintiff

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA,)
12 Plaintiff,)
13 v.)
14 DAVID NOSAL,)
15 Defendant.)
16 _____)

No. CR 08-0237 MHP

**UNITED STATES' OPPOSITION TO
DEFENDANT NOSAL'S SECOND
MOTION TO DISMISS INDICTMENT**

Hrg. Date: February 17, 2009
Time: 10:00 a.m.
Crtrm. 15: Hon. Marilyn Hall Patel

17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

1

2 INTRODUCTION..... 1

3 ARGUMENT..... 3

4 I. DISMISSAL OF INDICTMENTS IS GENERALLY DISFAVORED..... 3

5 II. COUNTS TWO THROUGH NINE PROPERLY ALLEGE THAT THE

6 DEFENDANT ACCESSED KORN/FERRY’S COMPUTER SYSTEM

7 WITHOUT AUTHORIZATION, AND IN EXCESS OF AUTHORIZED

8 ACCESS. 3

9 A. Summary of Counts Two through Nine of the Indictment. 4

10 B. The Defendant’s Liability for the Offenses Alleged in

11 Counts Two through Nine. 6

12 C. Counts Two through Nine Properly Allege that the Defendant

13 Accessed Korn/Ferry’s Computer System Without Authorization,

14 and in Excess of Authorized Access. 7

15 III. SECTION 1832 DOES NOT REQUIRE THAT THE INDICTMENT

16 ALLEGE, OR THAT THE GOVERNMENT PROVE, THAT THE

17 DEFENDANT HAD KNOWLEDGE THAT HIS ACTIONS

18 WERE ILLEGAL..... 12

19 A. The Economic Espionage Act and Its *Mens Rea* Requirements. 12

20 B. Counts Ten and Eleven are Properly Pleaded. 14

21 IV. COUNTS TEN AND ELEVEN ARE NOT MULTIPLICITOUS 17

22 A. Legal Standard Regarding Multiplicitous Indictments. 17

23 B. Counts Ten and Eleven are not Multiplicitous. 17

24 V. THE MAIL FRAUD CHARGES PROPERLY STATE AN OFFENSE..... 19

25 A. The Indictment Alleges a Scheme to Defraud under the Mail

26 Fraud Statute. 20

27 B. California Law Does Not, and Cannot, Preclude the Mail

28 Fraud Charges. 22

CONCLUSION..... 24

TABLE OF AUTHORITIES

FEDERAL CASES

1

2

3 *Albernaz v. United States*, 450 U.S. 333 (1981). 17

4 *Allied North Am. Ins. v. Woodruff-Sawyer*, 2005 WL 2354119 (N.D. Cal. 2005). 11

5 *Ball v. United States*, 470 U.S. 85 (1985). 19

6 *Blockburger v. United States*, 284 U.S. 299 (1932).. . . . 17

7 *Boyce Motor Lines v. United States*, 342 U.S. 337 (1952). 14

8 *Bryan v. United States*, 524 U. S. 184 (1998). 14, 15

9 *Chapman v. United States*, 500 U.S. 453 (1991).. . . . 11

10 *Charles Schwab & Co. v. Carter*, 2005 WL 2369815 (N.D. Ill. Sept. 27, 2005). 10

11 *Cleveland v. United States*, 531 U.S. 12 (2000). 23

12 *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004). 9

13 *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001). 9

14 *Guam v. Muna*, 999 F.2d 397 (9th Cir. 1993). 3

15 *Hamling v. United States*, 418 U.S. 87 (1974).. . . . 3

16 *Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*,
556 F. Supp.2d 1122 (E.D. Cal. 2008).. . . . 10

17 *HUB Group v. Clancy*, 2006 WL 208684, at *3–*4 (E.D. Pa. Jan. 25, 2006). 10

18 *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006). 8, 9

19 *Kehr Packages v. Fidelcor, Inc.*, 926 F.2d 1406 (3d Cir. 1991). 21

20 *Lasco Foods, Inc. v. Hall & Shaw Sales*, 2009 WL 151687 (E.D. Mo. Jan. 22, 2009).. . . . 10

21 *McEvoy Travel Bureau, Inc. v. Heritage Travel, Inc.*, 904 F.2d 786 (1st Cir. 1990). 21

22 *Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp.2d 1188 (E.D. Wash. 2003). 10

23 *Pinkerton v. United States*, 328 U.S. 640 (1946).. . . . 7

24 *Ratzlaf v. United States*, 510 U.S. 137 (1994).. . . . 15

25 *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*,
119 F. Supp.2d 1121 (W.D. Wash. 2000). 9, 11

26 *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).. . . . 9, 10

27 *United States v. Armstrong*, 909 F.2d 1238 (9th Cir. 1989).. . . . 6

28

1 *United States v. Bostic*, 168 F.3d 718 (4th Cir. 1999). 14

2 *United States v. Fernandez*, 388 F.3d 1199 (9th Cir. 2004). 3

3 *United States v. Garlick*, 240 F.3d 789 (9th Cir. 2001). 17

4 *United States v. Genovese*, 409 F. Supp.2d 253 (S.D.N.Y. 2005). 13

5 *United States v. Hsu*, 40 F. Supp.2d 623 (E.D. Pa. 1999). 2, 15, 16

6 *United States v. Jackson*, 72 F.3d 1370 (9th Cir. 1995). 3, 14

7 *United States v. Kafka*, 222 F.3d 1129 (9th Cir. 2000). 14

8 *United States v. Krumrei*, 258 F.3d 535 (6th Cir. 2001). 2, 15, 16

9 *United States v. Lanier*, 520 U.S. 259 (1997). 11

10 *United States v. Louderman*, 576 F.2d 1383 (9th Cir. 1978). 23

11 *United States v. Luskin*, 926 F.2d 372 (4th Cir. 1991).. 19

12 *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000).. 12

13 *United States v. Mitra*, 405 F.3d 492 (7th Cir. 2005). 5

14 *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991). 10

15 *United States v. Muhammad*, 120 F.2d 688, (7th Cir. 1997). 18

16 *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007).. 10, 11

17 *United States v. Ramirez-Martinez*, 273 F.3d 915 (9th Cir. 2001). 19

18 *United States v. Robinson*, 651 F.2d 1188 (6th Cir. 1981). 19

19 *United States v. Rogers*, 751 F.2d 1074 (9th Cir. 1985). 3

20 *United States v. Selby*, — F.3d —, 2009 WL 102711 (9th Cir. 2009). 20

21 *United States v. Summit Refrigeration Group, Inc.*, 2006 WL 3009111
 (E.D. Wisc. Oct. 26, 2006).. 18

22 *United States v. Tavelman*, 650 F.2d 1133 (9th Cir. 1981). 3

23 *United States v. Vaanderling*, 50 F.3d 696 (9th Cir. 1995). 6

24 *United States v. Weyhrauch*, 548 F.3d 1237 (9th Cir. 2008). 23

25 *United States v. Zalapa*, 509 F.3d 1060 (9th Cir. 2007). 19

26 *US Bioservices Corp. v. Lugo*, 2009 WL 151577 (D. Kan. Jan. 21, 2009)). 10, 11

27 *ViCHIP Corp. v. Lee*, 438 F. Supp.2d 1087 (N.D. Cal. 2006). 10

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

STATE CASES

Edwards v. Arthur Andersen LLP, 44 Cal. 4th 937 (2008). 22

FEDERAL STATUTES

18 U.S.C. § 1030(a)(4). 3, 4, 6, 7
18 U.S.C. § 1832. 12
18 U.S.C. § 1839(3). 13
18 U.S.C. § 2. 6
142 Cong. Rec. *S12213, (1996) 1996 WL 559474 13, 14
S. Rep. 104-357, 104th Cong., 2d Sess. (1996) 5
S. Rep. 104-359, 104th Cong., 2d Sess. (1996) 12, 13
H. Rep. No. 104-788, 104th Cong., 2d Sess. (1996) 12

STATE STATUTES

California Business and Professions Code 16600. 22

FEDERAL RULES

Fed. R. Crim. P. 7(c). 3

1 SCOTT N. SCHOOLS (SC 9990)
 Associate Deputy Attorney General
 Acting United States Attorney

2

3 KYLE F. WALDINGER (ILSB 6238304)
 Assistant United States Attorney

4

5 450 Golden Gate Avenue, 11th Floor
 San Francisco, California 94102
 Telephone: (415) 436-6830
 Facsimile: (415) 436-7234

7 Attorneys for Plaintiff

8 UNITED STATES DISTRICT COURT

9 NORTHERN DISTRICT OF CALIFORNIA

10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA,)	No. CR 08-0237 MHP
)	
12 Plaintiff,)	UNITED STATES' OPPOSITION TO
)	DEFENDANT NOSAL'S SECOND
13 v.)	MOTION TO DISMISS INDICTMENT
)	
14 DAVID NOSAL,)	Hrg. Date: February 17, 2009
)	Time: 10:00 a.m.
15)	Crtrm. 15: Hon. Marilyn Hall Patel
16 Defendant.)	

17 **INTRODUCTION**

18 The defendant David Nosal has filed a second motion seeking to dismiss the Superseding
19 Indictment ("Indictment"). The Court should deny the defendant's motion in its entirety.

20 Much of the defendant's motion relies on a mischaracterization of the charged offenses,
 21 as well as a failure to squarely address the allegations that knock the legs out from under his
 22 arguments. For example, Nosal argues that Counts Two through Nine "only" allege
 23 "misappropriation" on behalf of Christian & Associates, and that the unauthorized computer
 24 access alleged in those charges "merely breaches a contract conditioning access." *See* Def. Mtn.,
 25 at 3-8. In truth, however, Counts Two through Nine allege that the defendant and others
 26 fraudulently accessed the computer system of his former employer Korn/Ferry International
 27 ("Korn/Ferry") on specific dates for the purpose of obtaining valuable information. Those
 28 charges do *not* allege that the defendant and others merely misappropriated information that they

1 happened already to have in their possession. In addition, the Indictment is clear that these
2 actions were taken for the purpose of assisting *Nosal* in his executive search activities (and were
3 not merely for the benefit of Christian & Associates). Further, the Indictment relates to much
4 more than a breach of an agreement relating to computer use. Rather, the case relates to a
5 scheme — fraudulent from bark to core — to steal confidential and proprietary information from
6 Korn/Ferry’s computer system.

7 The defendant also mischaracterizes the trade secret charges alleged in Counts Ten and
8 Eleven. Those charges do *not* relate, as *Nosal* claims, to “the same instance of conduct.” *Id.* at
9 10:17–18. On the contrary, as the allegations in the Indictment make clear, the criminal acts
10 alleged in Counts Ten and Eleven occurred at different times on April 12, 2005. Moreover, each
11 charge pertains to different conduct (essentially, theft and copying on the one hand versus receipt
12 and possession on the other), and each charge relates to differing sets of data. Accordingly,
13 Counts Ten and Eleven are not multiplicitous, because each requires proof of an additional fact
14 that the other does not.

15 With respect to the *mens rea* requirement of Counts Ten and Eleven, the defendant
16 incorrectly states the court’s holdings in *United States v. Krumrei* and *United States v. Hsu*.
17 Neither of those cases “determined” that the Economic Espionage Act (EEA) “must be
18 interpreted to include an additional mens rea element [of knowledge of illegality] that is not
19 specified in the statutory text,” *id.* at 9:19–21, as the defendant argues. Rather, the cases simply
20 upheld void-for-vagueness challenges to the EEA; neither announced a rule of pleading.

21 Finally, in arguing that the mail fraud charges are based merely on an “undisclosed
22 breach” of contract, *id.* at 12:7–9 & 12:23 – 26, the defendant largely ignores the allegations that
23 the defendant devised and participated in a scheme to defraud Korn/Ferry of \$25,000 per month
24 (as well as other payments) and of information in Korn/Ferry’s computer system, and that he did
25 so by making affirmative misrepresentations to Korn/Ferry on a regular basis, by using a
26 fictitious name in his business dealings, and by stealing proprietary and confidential information
27 from Korn/Ferry’s computer system, among other actions. Simply put, the Indictment’s mail
28 fraud charges are based on much more than *Nosal*’s “undisclosed breach” of contract.

ARGUMENT**I. DISMISSAL OF INDICTMENTS IS GENERALLY DISFAVORED.**

In this case, the defendant seeks an order dismissing each and every one of the charges against him. However, “[t]he dismissal of an indictment is considered a ‘drastic step’ and is generally disfavored as a remedy.” *Guam v. Muna*, 999 F.2d 397, 399 (9th Cir. 1993) (quoting *United States v. Rogers*, 751 F.2d 1074 (9th Cir. 1985)).

The pleading standards with which the government must comply are well known: Rule 7(c) provides in relevant part that an indictment shall contain a “plain, concise, and definite written statement of the essential facts constituting the offense charged.” Fed. R. Crim. P. 7(c). In order to be legally sufficient, an indictment must contain the elements of the offense charged, fairly inform the defendant of the charge, and enable the defendant to plead double jeopardy as a defense to future prosecution for the same offense. *See Hamling v. United States*, 418 U.S. 87, 117 (1974); *United States v. Fernandez*, 388 F.3d 1199, 1217–18 (9th Cir. 2004). Under Ninth Circuit law, an indictment need do little more than track the language of the statute, include “implied, necessary elements, not present in the statutory language,” and state the approximate time and place of the alleged crime. *See United States v. Jackson*, 72 F.3d 1370, 1380 (9th Cir. 1995); *United States v. Tavelman*, 650 F.2d 1133, 1137 (9th Cir. 1981).

With these principles in mind, the government turns to the defendant’s various arguments in support of his motion to dismiss the Indictment.

II. COUNTS TWO THROUGH NINE PROPERLY ALLEGE THAT THE DEFENDANT ACCESSED KORN/FERRY’S COMPUTER SYSTEM WITHOUT AUTHORIZATION, AND IN EXCESS OF AUTHORIZED ACCESS.

The defendant argues that Counts Two through Nine of the Indictment must be dismissed because the statutory provision under which they are brought — 18 U.S.C. § 1030(a)(4) — does not encompass the facts of this case, *i.e.*, the use of a Korn/Ferry employees’ usernames and passwords to access Korn/Ferry’s computer system for the purpose of obtaining information to be used in the defendant Nosal’s competing business. As set forth in more detail below, the defendant’s proffered interpretation of Section 1030(a)(4) is not supported by common sense, or by the weight of authority.

1 **A. Summary of Counts Two through Nine of the Indictment.**

2 Counts Two through Nine charge the defendant David Nosal with accessing with the
3 intent to defraud the computer system of Korn/Ferry — without authorization and in excess of
4 authorized access — and obtaining something of value as a result of such access.

5 Counts Two through Nine incorporate the introductory allegations in the Indictment set
6 out in ¶¶ 1–11, as well as the allegations regarding the charged conspiracy set out in ¶¶ 13–19.
7 As such, those counts allege that the defendant was employed at the executive search firm
8 Korn/Ferry International until October 2004. Indictment, ¶ 2. After he left Korn/Ferry, Nosal
9 was assisted in setting up his own executive search firm by his co-defendant Becky Christian
10 (who left Korn/Ferry’s employment in January 2005), by an individual identified as “M.J.” (who
11 left Korn/Ferry’s employment in March 2005), and by an individual identified as “J.F.” (who left
12 Korn/Ferry’s employment in August 2005). *Id.*, ¶¶ 3–5.

13 The Indictment contains numerous allegations regarding Korn/Ferry’s computer system
14 and the confidentiality of the information contained therein. Significantly, the Indictment alleges
15 that Korn/Ferry employees “received unique usernames and created passwords for use on the
16 company’s computer systems,” which were intended to be used by the Korn/Ferry employee
17 only. Indictment, ¶ 9. The Indictment also alleges that Nosal, Christian, M.J., and J.F. each
18 entered into a confidentiality agreement with Korn/Ferry. Each agreement explained that the
19 information in Korn/Ferry’s computer system was owned by Korn/Ferry, and restricted the use
20 and disclosure of all information, except for legitimate Korn/Ferry business. *Id.*, ¶ 10. Finally,
21 each time a Korn/Ferry employee logged onto the computer system, he was informed that he
22 needed “specific authority to access any Korn/Ferry system or information.” Indictment, ¶ 11.

23 The charges in Counts Two through Nine relate to instances in which the Korn/Ferry
24 computer user account of Christian or J.F. was used to access Korn/Ferry’s computer system to
25 obtain information regarding potential candidates for corporate executive positions, which
26 information was to be used in Nosal’s competing business. The Indictment alleges that these
27 instances of access were performed by individual conspirators (1) “prior to and upon termination
28 of their employment with Korn/Ferry by using their own Korn/Ferry” credentials, and (2) after

1 their separation from Korn/Ferry by using — either directly or through J.F. — J.F.’s Korn/Ferry
 2 credentials. *See* Indictment, ¶¶ 16–17. The government expects to prove that (1) Christian used
 3 her own credentials to access Korn/Ferry’s computer system in the instance alleged in Count
 4 Two; (2) Christian used J.F.’s credentials to access the computer system in the instance alleged in
 5 Count Three; (3) Christian asked J.F. to access the computer system in the instances alleged in
 6 Counts Four, Seven, and Eight; (4) M.J. asked J.F. to access the computer system in the instances
 7 alleged in Counts Five and Six; and (5) M.J. used J.F.’s credentials to access the computer
 8 system in the instance alleged in Count Nine.¹

9 The government will present evidence that Nosal directed Christian, M.J., and J.F. to
 10 obtain information from Korn/Ferry’s computers, and that he entered into a conspiracy with those
 11 individuals to access Korn/Ferry’s computer system for that purpose.²

12 ///

13
 14
 15 ¹The defendant’s motion incorrectly suggests that the Indictment alleges only that “the
 16 defendants gained access to the Korn/Ferry computers ‘*by using their own Korn/Ferry user*
 17 *names and passwords.*” Def. Mtn., at 8 (quoting Indictment, ¶ 16) (emphasis in defendant’s
 18 motion). However, he ignores the next paragraph of the Indictment, which alleges that the
 19 conspirators *also* gained access to Korn/Ferry’s computer system “by using, either *directly* or
 20 through J.F., J.F.’s Korn/Ferry username and password.” Indictment, ¶ 17 (emphasis added).
 Given that J.F.’s password was used on at least two occasions by someone other than J.F. to
 access Korn/Ferry’s computer system (*e.g.*, Counts Three and Nine), even the defendant
 apparently would concede that those counts properly allege unauthorized access to Korn/Ferry’s
 computer system, since they relate to access to that computer system by an outsider.

21 ²In labeling this prosecution an “expansive theory of liability,” Def. Mtn., at 4 n.3, Nosal
 22 fails to acknowledge other prosecutions employing such a theory, including one in this Court.
 23 *See, e.g., United States v. Zenaida Smith*, CR 07-0246 MHP; *United States v. Robinson*, CR 07-
 24 0596 JF; *United States v. Williams et al.*, CR 04-40018 CW. Thus, far from representing an
 25 “expansive” theory, this case represents a typical criminal action brought under Section 1030.
 26 Indeed, the CFAA was enacted in an effort to create an omnibus criminal statute to address
 27 computer-related crimes. S. Rep. 104-357, 104th Cong., 2d Sess. 5 (1996) (“the Computer Fraud
 28 and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather
 than identifying and amending every potentially applicable statute affected by advances in
 computer technology”). “Section 1030 is general.” *United States v. Mitra*, 405 F.3d 492, 495
 (7th Cir. 2005). As technology changes, the effective scope of Section 1030 may grow, but this
 does not mean that the statute should be given “less coverage than its language portends.” *Id.*

1 **B. The Defendant's Liability for the Offenses Alleged in Counts Two through Nine.**

2 Before turning to the defendant's substantive arguments regarding Counts Two through
3 Nine, the government first addresses the various comments made in the defendant's brief
4 questioning how he could possibly be liable for actions that are alleged in the Indictment to have
5 been taken by others. *See, e.g.*, Def. Mtn., at 8:18–27 (“The indictment does not allege that Mr.
6 Nosal himself ran any searches using J.F.’s password, nor does it allege that he assisted anyone
7 else in doing so.”); *cf. also id.*, at 11 n.6 (arguing that Count Ten does not properly allege an
8 offense because it does not allege that trade secrets were stolen “by Mr. Nosal himself”). The
9 defendant fails to consider familiar principles of criminal liability.

10 Here, the Indictment alleges liability in Counts Two through Nine under both the
11 substantive statutes and 18 U.S.C. § 2. Section 2 “eliminates the common law distinction
12 between ‘principal’ and ‘accessory’ and makes one who aids and abets or causes the commission
13 of a crime punishable as a principal.” *United States v. Armstrong*, 909 F.2d 1238, 1241 n.1 (9th
14 Cir. 1989). All indictments are read to embody this statute. *See United States v. Vaanderling*, 50
15 F.3d 696, 702 (9th Cir. 1995). Section 2 provides criminal liability for a defendant who “aids,
16 abets, counsels, commands, induces or procures” the commission of an offense or who “willfully
17 causes an act to be done which if directly performed by him or another would be an offense
18 against the United States.” Thus, Nosal may be found guilty of the Indictment’s substantive
19 crimes, even if he did not personally commit the acts constituting those crimes, but aided and
20 abetted in their commission. Indeed, Nosal’s co-conspirators have admitted in their plea
21 colloquys that Nosal directed them to take items from Korn/Ferry’s computer system. *See, e.g.*,
22 Plea Agrm., ¶ 2, CR 07-0568 MHP (“I also understood [Nosal] to be directing me to take from
23 Korn/Ferry whatever I thought would be necessary or helpful for [Nosal’s] new company. . . .”);
24 Plea Agrm., ¶ 2, CR 07-0337 MHP (“[Nosal] asked me to retrieve position specifications for a
25 particular job function from Korn/Ferry’s computer system.”).

26 Nosal can also be found guilty under the law of conspiracy because

27 [e]ach member of the conspiracy is responsible for the actions of the other
28 conspirators performed during the course and in furtherance of the conspiracy. If
one member of a conspiracy commits a crime in furtherance of a conspiracy, the

1 other members have also, under the law, committed that crime. . . .

2 9th Cir. Model Jury Instr., 8.20. This so-called “*Pinkerton*” charge

3 derives its name from *Pinkerton v. United States*, 328 U.S. 640 (1946), which
4 held that a defendant could be held liable for a substantive offense committed by a
5 co-conspiracy as long as the offense occurred within the course of the
conspiracy, was within the scope of the agreement, and could reasonably have
been foreseen as a necessary or natural consequence of the unlawful agreement.

6 9th Cir. Model Jury Instr., 8.20, comment (citation omitted). Because Count One of the
7 Indictment alleges that Nosal entered into a conspiracy to commit computer fraud, and because
8 the instances alleged in Counts Two through Nine were crimes committed as part of that
9 conspiracy, Nosal can be liable under a *Pinkerton* theory for those crimes.

10 **C. Counts Two through Nine Properly Allege that the Defendant Accessed**
11 **Korn/Ferry’s Computer System Without Authorization, and in Excess of**
12 **Authorized Access.**

13 The defendant first argues that the statute under which Counts Two through Nine are
14 brought — Section 1030(a)(4) of the Computer Fraud and Abuse Act (CFAA) — prohibits only
15 “unauthorized access” or “exceeding authorized access” and that it does not prohibit
16 “misappropriation.” The gravamen of the defendant’s argument is that employees who are given
17 physical and electronic access to their employer’s computer systems, and who then steal
18 information that might be available to them pursuant to that access, cannot be found to have
19 accessed those computer systems without authorization (or to have done so in excess of their
authorized access). The defendant’s argument fails on several grounds.

20 As an initial matter, the defendant’s argument that Section 1030(a)(4) does not “cover”
21 misappropriation misses the mark. Notably, in quoting what he argues is the “relevant part” of
22 Section 1030(a)(4), the defendant states only that the statute ““makes it a crime for a person to
23 ‘knowingly and with intent to defraud, access[] a protected computer without authorization, or
24 exceed[] authorized access.’” Def. Mtn., at 3 (quoting Section 1030(a)(4)). The defendant fails,
25 however, to cite the *other* elements set out in the statute, namely, that the defendant “further[] the
26 intended fraud and *obtain[] anything of value.*” 18 U.S.C. § 1030(a)(4) (emphasis added).
27 Accordingly, whatever term one applies — “misappropriation” or “obtaining anything of value”
28 — the statute clearly covers situations in which information is taken from a computer system.

1 Indeed, the statute *requires* the government to prove that something was taken; mere “access” to
2 a computer system is not enough to trigger liability. Accordingly, the Indictment’s allegations
3 that items were taken from Korn/Ferry is part and parcel of a Section 1030(a)(4) charge.

4 Second, Counts Two through Nine allege that Nosal is culpable for having accessed
5 Korn/Ferry’s computer system on eight dates *after* his separation from Korn/Ferry in October
6 2004. Accordingly, even assuming that the Korn/Ferry employee user accounts of Christian and
7 J.F. were used by those individuals to obtain information at a time when they were still employed
8 at Korn/Ferry, the Indictment alleges those items were obtained for the purpose of assisting Nosal
9 and his co-conspirators in their own business activities. *See* Indictment, ¶ 18. Clearly, if an
10 individual *steals* the password of a competitor’s employee and thereafter fraudulently accesses
11 that competitor’s computer system and obtains something of value using that password, such
12 access would be “without authorization” under Section 1030, regardless of whether the employee
13 from whom he stole the password was otherwise “authorized” to do so. Under the defendant’s
14 theory, however, if that same individual *paid* the competitor’s employee to access the
15 competitor’s computer systems and obtain information, there would be no “unauthorized access,”
16 regardless of whether the employee’s actions violated his agreements with, or duty of loyalty to,
17 his employer. This result is not consistent with a fair reading of the statute.

18 Third, although some courts have held that Section 1030 does not cover an employee’s
19 access to his employer’s computer system using log-in credentials provided to him by that
20 employer, the weight of authority supports the opposite view. Notably, the only federal *appellate*
21 courts to have ruled on this issue have agreed with the government’s interpretation of the statute.³
22 For example, in *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the
23 Seventh Circuit held that employees who access their employer’s computers to obtain or delete
24 business information for their own personal benefit or the benefit of a competitor act “without
25 authorization” or “exceed authorization” within the meaning of the statute. *See Citrin*, 440 F.3d

26
27 ³Section 1030(g) provides for a civil cause of action for violations of Section 1030.
28 Because of that provision, many of the cases construing Section 1030 have arisen in the civil, as
opposed to the criminal, context.

1 at 420–21 (finding employee acted without authorization because the employee’s “breach of his
2 duty of loyalty [in deleting computer files] terminated his agency relationship . . . and with it his
3 authority to access the laptop”). As the Seventh Circuit recognized, even when “authorization”
4 exists, it can be withdrawn or can lapse under well-accepted principles of agency law. *See also*
5 *Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp.2d 1121, 1124 (W.D.
6 Wash. 2000) (finding that insiders with authorization to use a system can lose that authorization
7 when they act as agents of an outside organization).⁴

8 Similarly, in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the
9 First Circuit held that a former employee of a travel agent could be found to have exceeded his
10 authorization to obtain information from his former employer’s website because, in violation of
11 his confidentiality agreement with the employer, he used confidential information he had
12 obtained as an employee to create a program that enabled his new travel company to obtain
13 information from that website that he could not have obtained as efficiently without the use of
14 that confidential information. *Id.* at 583–84.

15 Further, although the question at issue here was not directly addressed in the case, the
16 Ninth Circuit upheld a jury verdict on behalf of a plaintiff in a civil action brought under Section
17 1030 where one of the allegations was that the defendant had

18 hired away a [plaintiff’s] employee who had given [the defendant] an
19 unauthorized tour of the [plaintiff’s] website. This employee, while still working
20 for [the plaintiff], accessed confidential information regarding several thousand of
21 [the plaintiff’s] customers. He downloaded, and sent to his home email account,
22 the confidential address to [the plaintiff’s website’s] server so that he could access
23 the server from home and retrieve customer lists.

24 *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 932 (9th Cir. 2004); *id.* (noting that
25 plaintiff prohibited competitors’ access to its website). These facts are similar to those alleged in
26 the instant case. *Cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004) (stating that use

27 ⁴In *Shurgard*, employees were found to have acted “without authorization” when they
28 accessed their employer’s computers to obtain trade secrets for the benefit of a competitor.
Applying principles of agency law, the court concluded that the employees’ authorized access to
the employer’s computers ended when they became agents of the competitor. *Shurgard*, 119
F. Supp.2d at 1124–25.

1 of authorized third party's password by outside hacker to gain access to mail server fell within
2 "the paradigm of what [Congress] sought to prohibit [under Stored Communications Act]".

3 Other appellate courts have upheld criminal convictions under Section 1030 where the
4 theory of "unauthorized access" was based on the defendant's non-compliance with the intended
5 function of the computer system at issue. For example, in the first appellate decision to use
6 either term, the Second Circuit found that a defendant had gained "unauthorized access" to
7 computers on "INTERNET" based on the fact that he did not use the features of the computer to
8 which he did have access "in any way related to [those features'] intended function." *United*
9 *States v. Morris*, 928 F.2d 504, 510 (2^d Cir. 1991); *see also id.* at 511 (rejecting argument that
10 Section 1030 was aimed only at "outsiders"); *United States v. Phillips*, 477 F.3d 215, 219–21 (5th
11 Cir. 2007) (holding that evidence was sufficient to find defendant guilty of "unauthorized access"
12 where defendant violated university's "acceptable use" computer policy and accessed portions of
13 computer system he was never authorized to access under policy).

14 Several trial courts have agreed with the holdings reached in *Citrin*, *EF Cultural Travel*,
15 and *Shurgard*. *See, e.g., Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556
16 F. Supp.2d 1122, 1131 (E.D. Cal. 2008) ("Both former employees and their new companies who
17 seek a competitive edge through wrongful use of information from the former employer's
18 computer system face liability under § 1030.") (citing *Pac. Aerospace & Elecs., Inc. v. Taylor*,
19 295 F. Supp.2d 1188 (E.D. Wash. 2003)); *ViCHIP Corp. v. Lee*, 438 F. Supp.2d 1087, 1100
20 (N.D. Cal. 2006) (rejecting employee's argument that his access to plaintiff's system was
21 "technically authorized, since he deleted the [] files while still an officer and director"); *HUB*
22 *Group v. Clancy*, 2006 WL 208684, at *3–*4 (E.D. Pa. Jan. 25, 2006) (holding that, if defendant
23 accessed employer's database, not for use as an employee of that company, but for future use as
24 competitor's employee, a violation of CFAA properly could be alleged); *cf. also Charles Schwab*
25 *& Co. v. Carter*, 2005 WL 2369815, at *5–*7 (N.D. Ill. Sept. 27, 2005) (holding that if employee
26 accessed computer user account for purpose of assisting future employer, liability could be
27 established against employee and future employer under CFAA). *But see, e.g., Lasco Foods, Inc.*
28 *v. Hall & Shaw Sales*, 2009 WL 151687 (E.D. Mo. Jan. 22, 2009); *US Bioservices Corp. v. Lugo*,

1 2009 WL 151577 (D. Kan. Jan. 21, 2009); *Allied North Am. Ins. v. Woodruff-Sawyer*, 2005 WL
2 2354119 (N.D. Cal. 2005); Def. Mtn., at 4–6 (citing cases).

3 * * *

4 Courts typically analyze “the scope of a user’s authorization to access a protected
5 computer on the basis of the expected norms of intended use or the nature of the relationship
6 established between the computer owner and the user.” *Phillips*, 477 F.3d at 219. Based on a
7 plain reading of the statute, common sense, and the case law authority cited above, this Court
8 should conclude that an employee may act “without authorization” or “in excess of authorized
9 access” when he accesses his employer’s computers (which he has permission to access) with the
10 intent to defraud, or where, as here, he aids and abets, or is part of a conspiracy with, such an
11 employee. *Cf. Shurgard*, 119 F. Supp.2d at 1126 (“‘fraud’ simply means wrongdoing and not
12 proof of the common law elements of fraud”). In particular, the Court should reach that
13 conclusion in this case based upon the detailed allegations regarding (1) the permitted uses of
14 employee usernames and passwords at Korn/Ferry, *see* Indictment, ¶ 9; (2) the confidentiality
15 agreements entered into between the conspirators and Korn/Ferry regarding the information in
16 Korn/Ferry’s computer system, *see id.*, ¶ 10; and (3) the notification given to employees each
17 time that they logged onto Korn/Ferry’s computer system, which stated that they needed “specific
18 authority to access any Korn/Ferry system or information,” *id.*, ¶ 11.⁵

19 For these reasons, and for all of the reasons set forth above, the defendant’s motion to
20

21 ⁵The defendant argues that, simply because “reasonable people could disagree about the
22 scope of [Section 1030(a)(4)],” Def. Mtn., at 7, this Court should apply the “rule of lenity” and
23 adopt *his* proffered interpretation. However, the rule of lenity is applicable only where “there is a
24 grievous ambiguity or uncertainty in the language and structure of [an] Act, such that even after a
25 court has seize[d] every thing from which aid can be derived, it is still left with an ambiguous
26 statute.” *Chapman v. United States*, 500 U.S. 453, 463 (1991) (second alteration in original,
27 internal quotation marks and citations omitted); *see also United States v. Lanier*, 520 U.S. 259,
28 266 (1997) (noting that rule of lenity resolves ambiguity in criminal statutes). Here, the
defendant does not argue that Section 1030 is ambiguous. As argued above, the government
submits that the statute, plainly read, prohibits employees from using their usernames and
passwords to access their employer’s computers for the purpose of obtaining information to be
used by a competitor. Because the statute is not ambiguous, the rule of lenity is inapplicable.

1 dismiss Counts Two through Nine (and the corresponding portions of the conspiracy charge in
2 Count One) should be denied.

3 **III. SECTION 1832 DOES NOT REQUIRE THAT THE INDICTMENT ALLEGE, OR**
4 **THAT THE GOVERNMENT PROVE, THAT THE DEFENDANT HAD**
5 **KNOWLEDGE THAT HIS ACTIONS WERE ILLEGAL.**

6 The defendant next argues that Counts Ten and Eleven must be dismissed because they
7 fail to allege that the defendant knew that his actions were illegal. However, proof that the
8 defendant knew that his actions were illegal is not an element of the trade secret offenses charged
9 in the Indictment.

10 **A. The Economic Espionage Act and Its *Mens Rea* Requirements.**

11 Counts Ten and Eleven of the Indictment are brought pursuant to 18 U.S.C. § 1832,
12 which was enacted as part of the Economic Espionage Act (EEA). The EEA was enacted in part
13 to protect our country's economic interests. As a House Report explained:

14 For many years federal law has protected intellectual property through the patent
15 and copyright laws. With this legislation, Congress will extend vital federal
16 protection to another form of proprietary economic information — trade secrets.
17 There can be no question that the development of proprietary economic
18 information is an integral part of America's economic well-being.

19 H. Rep. No. 104-788, 104th Cong., 2d Sess. 4 (1996); *see also id.* (noting that “intangible assets
20 have become more and more important to the prosperity of companies”). Although the defendant
21 correctly notes that the EEA ““was not designed to punish competition, even when such
22 competition relies on the know-how of former employees of a direct competitor,”” Def. Mtn., at 9
23 (quoting *United States v. Martin*, 228 F.3d 1 (1st Cir. 2000)), he does not complete the rest of the
24 *Martin* court's description, *i.e.*, that the EEA *was* designed to prevent employees and their future
25 employers “from taking advantage of confidential information gained, discovered, copied, or
26 taken while employed elsewhere.” *Martin*, 228 F.3d at 11. This distinction is not, as Nosal
27 claims, “insolubly hazy.” Def. Mtn., at 9. As *Martin* noted, the EEA specifically addresses
28 situations, similar to the one here, in which a disgruntled employee walks out of his “company
with a computer diskette full of engineering schematics.” *Martin*, 228 F.3d at 11; *see also* S.
Rep. 104-359, 104th Cong., 2d Sess. 6 (1996) (“A great deal of theft is committed by disgruntled
individuals or employees who hope to harm their former company or line their own pockets.”).

1 The three *mens rea* requirements set out in Section 1832(a) are that the defendant,
2 “[/] with intent to convert a trade secret . . . to the economic benefit of anyone other than the
3 owner thereof, and [2] intending or knowing that the offense will injure any owner of that trade
4 secret, [3] knowingly” engages in misappropriation. “A knowing state of mind with respect to an
5 element of the offense is (1) an awareness of the nature of one’s conduct, and (2) an awareness of
6 or a firm belief in or knowledge to a substantial certainty of the existence of a relevant
7 circumstance, such as whether the information is proprietary economic information as defined by
8 this statute.” S. Rep. No. 104-359, at 16. Because criminal statutes covering the theft of tangible
9 property generally require the government to provide that the defendant “[knew] that the object
10 he [stole was] indeed a piece of property that he [had] no lawful right to convert for his personal
11 use,” the government generally must show that the defendant knew or had a firm belief that the
12 information he or she was taking was a trade secret in cases brought pursuant to Section 1832 as
13 well. 142 Cong. Rec. *S12213 (1996), 1996 WL 559474 (EEA legislative history); *see also*
14 *United States v. Genovese*, 409 F. Supp.2d 253, 258 (S.D.N.Y. 2005) (discussing alleged
15 circumstances that would indicate that EEA defendant knew the information was a trade secret).

16 It is well established, however, that ignorance of the law is no defense. The government
17 need not prove that a defendant himself had concluded that the information he took fit the legal
18 definition of a “trade secret” set forth in 18 U.S.C. § 1839(3). If the government had to prove
19 this, Section 1832 violations would be nearly impossible to prosecute, and Congress’s intent
20 would be contravened:

21 This [knowledge] requirement should not prove to be a great barrier to legitimate
22 and warranted prosecutions. Most companies go to considerable pains to protect
23 their trade secrets. Documents are marked proprietary; security measures put in
place; and employees often sign confidentiality agreements.

24 142 Cong. Rec. *S12213 (1996), 1996 WL 559474. Based on this legislative history, the
25 government can prove that a defendant knew that the information was a trade secret by proving
26 that he was aware that it was protected by proprietary markings, security measures, and
27 confidentiality agreements. *Id.* More generally, the government could simply prove that a
28 defendant knew or had a firm belief that the information was valuable to its owner because it was

1 not generally known to the public, and that its owner had taken measures to protect it. On the
2 other hand, a person could not be convicted under Section 1832 if he took a trade secret because
3 of “ignorance, mistake, or accident.” *Id.* Nor could he be convicted if “he actually believed that
4 the information was not proprietary after [he took] reasonable steps to warrant such belief.” *Id.*

5 **B. Counts Ten and Eleven are Properly Pleaded.**

6 In addition to the three *mens rea* elements explicitly set out in Section 1832, the
7 defendant argues that this Court should read a *fourth* mental state requirement into the statute,
8 *i.e.*, that the defendant knew his actions to be illegal. However, it is undisputed that Counts Ten
9 and Eleven track the language of Section 1832 and that they duly incorporate all three of the
10 *mens rea* elements set out in the statute. Moreover, it is undisputed that neither the Ninth Circuit
11 nor any district court sitting in the Ninth Circuit has held that knowledge of illegality is an
12 “implied, necessary element[.]” of Section 1832. *See Jackson*, 72 F.3d at 1380.

13 As noted above, Section 1832 sets out a “knowing” *mens rea* requirement. The Supreme
14 Court has held that, “unless the text of the statute dictates a different result, the term ‘knowingly’
15 merely requires proof of knowledge of the facts that constitute the offense.” *Bryan v. United*
16 *States*, 524 U. S. 184, 193 (1998); *see also United States v. Kafka*, 222 F.3d 1129, 1131 (9th Cir.
17 2000) (citing *United States v. Bostic*, 168 F.3d 718 (4th Cir. 1999), for proposition that “the term
18 ‘knowingly’ as applied to section 922(g)(8) offenses does not require a defendant be aware of the
19 illegality of his conduct”). In *Bryan*, the Supreme Court stated that “the term ‘knowingly’ does
20 not necessarily have any reference to a culpable state of mind or to knowledge of the law.”
21 *Bryan*, 511 U.S. at 192. Rather, “the knowledge requisite to knowing violation of a statute is
22 factual knowledge as distinguished from knowledge of the law.” *Id.* at 192–93 (quoting *Boyce*
23 *Motor Lines v. United States*, 342 U.S. 337, 345 (1952) (Jackson, J., dissenting)).

24 Notably, the *Bryan* Court dealt with a statute (Section 922) that included a “willful”
25 element in the subsection at issue, but a “knowing” element in other subsections. Only the
26 provision punishing willful violations required knowledge of illegality. The Court noted that, in
27 order to establish a “willful” violation of a statute, the government must generally “prove that the
28 defendant acted with knowledge that his conduct was unlawful” or that the defendant acted with

1 a “bad purpose.” *Bryan*, 524 U.S. at 191–92 & n.12 (quoting, e.g., *Ratzlaf v. United States*, 510
2 U.S. 137, 137 (1994)); *cf. also id.* at 198–200 (holding that “willfulness” element required only
3 that government prove defendant’s knowledge that the conduct was illegal, not that the
4 government needed to prove the defendant had knowledge of the specific law or that he
5 disregarded a known legal obligation). Based on *Bryan*, it would be a strange result to import a
6 “willfulness” requirement into a statute (Section 1832) that clearly includes no such language and
7 that, instead, sets forth the less-exacting *mens rea* requirement of “knowingly.”

8 The defendant relies on a Sixth Circuit case and Pennsylvania district court case to argue
9 that knowledge of illegality is an element of Section 1832 that must be pleaded and proved. *See*
10 *Def. Mtn.*, at 9–10 (citing *United States v. Krumrei*, 258 F.3d 535 (6th Cir. 2001) and *United*
11 *States v. Hsu*, 40 F. Supp.2d 623 (E.D. Pa. 1999)). However, the cases relied upon by the
12 defendant do not stand for the proposition he advances in his motion because those cases do not
13 announce a rule of pleading. Neither *Krumrei* nor *Hsu* held that an indictment must contain an
14 allegation that the defendant knew that his actions were illegal, nor did they hold that knowledge
15 of illegality is an element of Section 1832. Rather, each court simply upheld the constitutionality
16 of the EEA in the face of void-for-vagueness challenges, and each court did so after finding that
17 the evidence showed that the defendant was aware that the information he stole was proprietary.

18 In *Krumrei*, the defendant argued on appeal that because the “reasonableness” of
19 measures taken to maintain the confidentiality of a trade secret must be decided on a case-by-case
20 basis, the entire statute was too vague to be enforced. *Krumrei*, 258 F.3d at 538; *see also id.*
21 (“[D]efendant alleges that the lack of clarity as to what constitutes ‘reasonable measures’ has the
22 potential to lead to arbitrary and discriminatory enforcement of the EEA.”). In holding that
23 Section 1832 was not unconstitutionally vague as applied to *Krumrei*, the Sixth Circuit found
24 that there was sufficient evidence to show that he “was aware that he was selling confidential
25 information to which he had no claim” and that he knew that the information that he took was
26 proprietary to the company Wilsonart. *Id.* at 539. The court relied on statements made by the
27 defendant at his guilty plea hearing, at which he admitted (1) obtaining trade secret information
28 from his employer that he knew to be proprietary to Wilsonart, (2) forwarding the information to

1 a competitor of Wilsonart, and (3) taking his actions for the purpose of benefitting someone other
2 than the owner of the trade secret. *Id.* Based on these concessions, the court found that Krumrei
3 “cannot claim that the statute is vague when he clearly was aware that his actions fell within the
4 activity proscribed by the statute.” *Id.*

5 In *Hsu*, the defendant moved to dismiss a theft of trade secrets charge brought against him
6 under Section 1832. As in *Krumrei*, the defendant in *Hsu* argued that Section 1832 was void for
7 vagueness because the definition of “trade secret” does not define “‘reasonable measures’ to keep
8 the information secret” or “what is meant by information not being ‘generally known’ or ‘readily
9 ascertainable’ to the public.” *Hsu*, 40 F. Supp.2d at 626. The district court held that Section
10 1832 was not void for vagueness as applied to *Hsu* because, based on evidence before the court,
11 *Hsu* knew that the owner of the alleged trade secrets “had taken many steps to keep its
12 technology to itself,” *id.* at 628, and that the defendant could not acquire the technology by any
13 other means than by getting it from a corrupt employee of the trade secret’s owner, *id.* at 631.

14 Accordingly, neither the *Krumrei* holding nor the *Hsu* holding “determined” that the EEA
15 included a knowledge-of-illegality element. *See* Def. Mtn., at 9:19–21.

16 * * *

17 Section 1832 makes it a crime to steal or otherwise misappropriate trade secrets. It does
18 not regulate unusual financial transactions or obscure fraudulent business dealings. Theft,
19 trafficking in stolen property, and possession of stolen property are common law concepts that
20 every citizen is expected to understand. In this case, the Indictment alleges that the defendant
21 knowingly stole and possessed trade secret information from Korn/Ferry’s computer system that
22 was (1) proprietary to Korn/Ferry, (2) the product of years of work by Korn/Ferry employees,
23 (3) valuable, (4) protected by numerous security measures, (5) subject to confidentiality
24 agreements, and (6) marked “Korn/Ferry Proprietary and Confidential.” Indictment, ¶¶ 6–11. It
25 further alleges that Nosal obtained that information through unauthorized access to Korn/Ferry’s
26 computer system, and that he obtained the information for the purpose of furthering his own
27 economic interests. There is nothing about the nature of these crimes that suggests that Section
28 1832 must be read to include an element of knowledge of illegality. For all of these reasons, this

1 Court should deny the defendant's motion to dismiss Counts Ten and Eleven (and the
2 corresponding portions of the conspiracy charge in Count One).

3 **IV. COUNTS TEN AND ELEVEN ARE NOT MULTIPLICITOUS.**

4 The defendant next argues that Counts Ten and Eleven of the Indictment should be
5 dismissed because they are multiplicitous. In the alternative, the defendant argues that Count
6 Ten is duplicitous. As set forth in more detail below, the defendant's multiplicity argument is
7 without merit, and none of the defendant's arguments requires dismissal now of either count.

8 **A. Legal Standard Regarding Multiplicitous Indictments.**

9 Multiplicity arises when separate counts against a defendant charge the same offense.
10 *United States v. Garlick*, 240 F.3d 789, 793–94 (9th Cir. 2001). “The test for multiplicity is
11 whether each count ‘requires proof of a[n additional] fact which the other does not.’” *Id.* at 794
12 (quoting *Blockburger v. United States*, 284 U.S. 299, 304 (1932) (alteration by *Garlick*)).

13 Contrary to the defendant's suggestion, multiplicity *does not* arise when a defendant is
14 charged with two offenses related to the same underlying conduct. *See* Def. Mtn., at 10 (“The
15 two counts are based on the same instance of conduct . . .”). Congress may authorize
16 cumulative punishments for separate criminal offenses that occur in the same act. *Albernaz v.*
17 *United States*, 450 U.S. 333, 344 (1981). As set forth above, double jeopardy is not implicated,
18 so long as each violation requires proof of an element that the other does not. *Blockburger*, 284
19 U.S. at 304.

20 **B. Counts Ten and Eleven are not Multiplicitous.**

21 The defendant contends that Counts Ten and Eleven are multiplicitous because they “are
22 based on the same instance of conduct” and because “they are charged under subdivisions of
23 Section 1832 that merely set out different means of committing the same offense.” Def. Mtn., at
24 10. The defendant's argument fails for at least two reasons.

25 First, the defendant is wrong when he claims that Counts Ten and Eleven pertain to “the
26 same instance of conduct.” On the contrary, the two charges pertain to entirely different acts that
27 occurred at different times. Count Ten relates to the *theft, copying and downloading* of *one* set of
28 data from Korn/Ferry's computer system on April 12, 2005. *See* Indictment, Count Ten (“three

1 Korn/Ferry source lists” and referencing ¶ 19.b); *id.*, ¶ 19.b (“Each source list had been
2 downloaded from the Searcher database earlier in the day on April 12, 2005 . . .”). The
3 government intends to show at trial that these source lists were downloaded on April 12 by
4 Christian, after she had asked for and received J.F.’s username and password on April 11. *See*
5 *id.*, ¶ 19.a (“On or about April 11, 2005, the defendant Christian sent an e-mail to J.F. stating ‘It
6 is to difficult to explain the searcher run I would need to log in as you.’”).

7 In contrast, Count Eleven relates to the defendant’s *receipt* and *possession* later in the day
8 on April 12 of *two* sets of data. *See* Indictment, Count Eleven (“three Korn/Ferry source lists
9 relating to prior searches for CFOs and information regarding CFOs that was ‘cut and pasted’
10 from a source list in Searcher” and referencing ¶¶ 19.b and 19.g). The Indictment alleges that the
11 defendant came into the possession of the first set of data via an e-mail dated April 12. *See id.*,
12 ¶ 19.b. The Indictment alleges that Nosal came into the possession of the second set of data via
13 two other e-mails on the same day. *See id.*, ¶ 19.g. Thus, the defendant’s argument regarding
14 “the same instance of conduct” ignores the plain language of Counts Ten and Eleven.

15 The fact that there may be overlapping proof with respect to Counts Ten and Eleven does
16 not mean that the counts are multiplicitous. *See United States v. Muhammad*, 120 F.2d 688, (7th
17 Cir. 1997) (noting that, in determining multiplicity, “we focus on the statutory elements of the
18 charged offenses, not the overlap in the proof offered to establish them, because a single act may
19 violate several statutes without rendering those statutes identical”). Here, because each charge
20 requires proof of a fact that the other does not, there is no multiplicity problem.

21 Second, the defendant’s insistence that Congress intended only one penalty for violations
22 of Section 1832’s multiple subsections is belied by the statute’s structure. Because it intended to
23 define a distinct offense for conspiracy in subsection (a)(5), Congress must also have intended to
24 define distinct offenses in subsections (a)(1) through (a)(3). *See United States v. Summit*
25 *Refrigeration Group, Inc.*, 2006 WL 3009111 (E.D. Wisc. Oct. 26, 2006) (“the plain language of
26 18 U.S.C. § 1832 does not . . . suggest that Congress intended that there be just one penalty for
27 violating any one or more of the subsections contained therein”).

28 Even if Counts Ten and Eleven were multiplicitous, the wholesale dismissal of both

1 counts would amount to throwing the baby out with the bath water. The remedy for meritorious
2 multiplicity claims is for the district court to vacate the multiplicitous conviction and sentence.
3 *United States v. Zalapa*, 509 F.3d 1060, 1065 (9th Cir. 2007); *accord Ball v. United States*, 470
4 U.S. 856, 864 (1985); *United States v. Luskin*, 926 F.2d 372, 378 (4th Cir. 1991).⁶ Accordingly,
5 the defendant's motion to dismiss those counts must be denied.

6 **V. THE MAIL FRAUD CHARGES PROPERLY STATE AN OFFENSE.**

7 The defendant's final argument is that the mail fraud charges in the Indictment should be
8 dismissed because "an undisclosed breach of an invalid contractual provision does not constitute
9 fraud." Def. Mtn., at 12. The defendant's argument fails for two reasons.

10 First, the Indictment alleges much more than an "undisclosed breach" of contract, and
11 much more than a breach of what Nosal calls the "non-compete" provisions of his agreement
12 with Korn/Ferry. Rather, as set out in more detail below, it alleges that Nosal devised a scheme
13 to defraud Korn/Ferry through theft of proprietary and confidential information from its
14 computer system, regular misrepresentations about his activities, and use of a fictitious name, all
15 the while accepting \$25,000 monthly payments from Korn/Ferry that were meant to compensate
16 him for making his best efforts to act in Korn/Ferry's best interests.

17 Second, Nosal's argument that he could not have defrauded Korn/Ferry because his
18 independent contractor agreement with Korn/Ferry was invalid under Section 16600 of the
19 California Business and Professions Code fails to consider well-settled law holding that the
20 scope of the federal fraud statutes is not confined by state law.

21 These points are set out in more detail below.

22
23 ⁶To the extent that this Court finds that Count Ten is duplicitous because it charges two
24 offenses in a single count, *see* Def. Mtn., at 11 n.6, dismissal of that count is also not the proper
25 remedy. *See United States v. Ramirez-Martinez*, 273 F.3d 915 (9th Cir. 2001) ("Defendant's
26 remedy is to move to require the prosecution to elect . . . the charge within the count upon which
27 it will rely. Additionally, a duplicitous . . . indictment is remediable by the court's instruction to
28 the jury particularizing the distinct offense charged in each count in the indictment.") (quoting
United States v. Robinson, 651 F.2d 1188, 1194 (6th Cir. 1981)); *see also* 1A Charles A. Wright,
Federal Practice and Procedure: Criminal § 145 at 83–84 (1999) (duplication "is not fatal and
does not require dismissal of the indictment").

1 **A. The Indictment Alleges a Scheme to Defraud under the Mail Fraud Statute.**

2 A conviction under the mail fraud statute requires the government to prove: (1) a scheme
3 to defraud; (2) use of the mails in furtherance of the scheme; and (3) specific intent to defraud.

4 *See United States v. Selby*, — F.3d —, 2009 WL 102711, at *8 (9th Cir. 2009) (wire fraud). The
5 government agrees that a breach of contract might not, in and of itself, constitute a basis for mail
6 fraud charges. However, the Indictment in this case alleges far more than a simple breach of
7 contract by Nosal. Rather, the Indictment alleges that the defendant devised a scheme to defraud
8 Korn/Ferry that consisted of:

- 9 • Nosal's direction to others to steal trade secrets and other things of value
10 from Korn/Ferry's computer system, Indictment, ¶ 28;
- 11 • Nosal's use, direction to others to use, and ratification of others' use of
12 trade secrets and other things of value stolen from Korn/Ferry's computer
13 system for the purpose of assisting Nosal's competing business with
14 Korn/Ferry, *id.*, ¶ 29;
- 15 • Nosal's deprivation of honest services as an independent contractor to
16 Korn/Ferry, by engaging in business on his own behalf, through shell
17 companies, instead of solely for Korn/Ferry, *id.*, ¶¶ 30–31;
- 18 • Affirmative misrepresentations by Nosal on numerous occasions to
19 Korn/Ferry executives that he was complying with his agreement with
20 Korn/Ferry, for the purpose of defrauding Korn/Ferry into continuing to
21 make \$25,000 monthly payments, among other payments, *id.*, ¶ 32;
- 22 • Nosal's failure to notify Korn/Ferry that he was engaging in his own
23 executive search activities (and thus failure to notify Korn/Ferry that he
24 was no longer entitled to \$25,000 monthly stipends), *id.*; and
- 25 • Nosal's concealment from Korn/Ferry that he was engaging in his own
26 executive search activities by, for example, using a fictitious name when
27 he interviewed candidates for executive positions that he was seeking to
28 fill, *id.*, ¶¶ 32–33.

22 The mail fraud charges also incorporate the allegations in ¶¶ 1–11 and ¶¶ 13–19 of the
23 Indictment regarding specific actions taken by Nosal and others to access Korn/Ferry's computer
24 system for the purpose of stealing confidential and proprietary information. The Indictment
25 alleges that, for the purpose of executing and attempting to execute this scheme to defraud, the
26 defendant caused eight (8) \$25,000 checks to be mailed by Korn/Ferry to his home in this
27 District. These mailings are alleged in Counts Twelve through Nineteen.

28 None of the cases cited by the defendant in which the courts found a breach of contract to

1 be insufficient to support mail fraud charges, *see* Def. Mtn., at 13, involved situations involving
2 such extensive schemes to defraud. *See, e.g., Kehr Packages v. Fidelcor, Inc.*, 926 F.2d 1406,
3 1417 (3^d Cir. 1991) (holding that allegation that defendant “unreasonably delayed” approving
4 sale of corporation to plaintiffs, while possibly amounting to breach of contract, “contains no
5 deception that would bring it within the purview of the mail fraud statute”); *McEvoy Travel*
6 *Bureau, Inc. v. Heritage Travel, Inc.*, 904 F.2d 786, 792 (1st Cir. 1990) (holding that allegations
7 of complaint did not sufficiently allege scheme to defraud any entity of money or property).⁷
8 Accordingly, the detailed allegations of this Indictment distinguish this case from the cases relied
9 upon by the defendant.

10 The defendant deftly sidesteps the portions of the Indictment that allege that, as part of
11 the scheme to defraud, Nosal stole proprietary and confidential information from Korn/Ferry and
12 “affirmatively misrepresented on numerous occasions to Korn/Ferry executives that he was
13 complying with the Nosal-Korn/Ferry Agreements.” Indictment, ¶¶ 28–29, 32. This is telling,
14 because such allegations, if true, clearly establish that Nosal’s actions constituted more than a
15 simple breach of contract.

16 Nosal’s argument that the Indictment is insufficient because it fails to allege that he
17 intended to cause economic harm to Korn/Ferry is also without merit. *See* Def. Mtn., at 13–14
18 (citing *Pennington* and *Sun-Diamond Growers*). Neither case cited by the defendant holds that
19 an Indictment must contain such allegations, which allegations are not elements of the mail fraud
20 offense. In any event, the Indictment *does* contain such allegations because it alleges that the
21 defendant engaged in a scheme to defraud Korn/Ferry for the purpose of receiving “monthly
22 independent contractor payments of \$25,000 from Korn/Ferry and so that he remained eligible to
23

24 ⁷Beyond the allegations of the Indictment here (which sufficiently allege the elements of
25 the mail fraud statute), the government intends to prove at trial that, *prior* to entering into his
26 agreement with Korn/Ferry, the defendant began directing others to take materials from
27 Korn/Ferry in preparation for starting a competing business. *See, e.g., Plea Agrm.*, ¶ 2, CR 07-
28 0568 MHP (docket entry 9) (“I also understood [Nosal] to be directing me to take from
Korn/Ferry whatever I thought would be necessary or helpful for [Nosal’s] new company,
including ‘source lists’ to populate the database at [Nosal’s] new company.”).

1 be paid the lump-sum payments” envisioned in the parties’ agreement and because it alleges that
2 he stole valuable information from Korn/Ferry. Indictment, ¶¶ 28–29, 32.

3 In sum, although the mail fraud statute may not reach every business practice that fails to
4 fulfill expectations, every breach of contract, or every breach of fiduciary duty, it *does* reach such
5 breaches where there was a recognizable scheme to defraud and where the defendant has made
6 fraudulent representations or omissions reasonably calculated to deceive. The allegations in the
7 pending Indictment describe such a scheme, and, for that reason, the defendant’s motion should
8 be denied.

9 **B. California Law Does Not, and Cannot, Preclude the Mail Fraud Charges.**

10 The defendant’s argument that the mail fraud counts must be dismissed because
11 California law prohibits “noncompetition” agreements is without merit. *See* Def. Mtn., at 14–15
12 (relying on California Business and Professions Code 16600).

13 As an initial matter, the agreement between Nosal and Korn/Ferry was not a
14 “noncompetition” agreement falling within the prohibitions of Section 16600. (Indeed, even the
15 defendant is careful not to label the entire agreement as a “noncompetition” agreement, but only
16 argues that the agreement contains “non-compete” provisions. Def. Mtn., at 12:23–25.) Rather,
17 it was an agreement in which Nosal agreed to act solely as an independent contractor to
18 Korn/Ferry for a period of one year. In addition, that agreement contained other promises on
19 Nosal’s behalf, including promises to maintain the confidentiality of the information in
20 Korn/Ferry’s computer system. *See* Def. Mtn., Ex. 1, ¶ 18, at 9. In return for *all* of the promises
21 he made, Nosal received the sizable salary of \$25,000 per month, in addition to being eligible to
22 receive lump-sum payments from Korn/Ferry near the end of his term as independent contractor.
23 The defendant has cited no California law that makes such an arrangement requiring a duty of
24 loyalty on the part of a compensated independent contractor void or invalid. The California
25 Supreme Court’s decision in *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (2008), a case
26 heavily relied upon by the defendant, is not to the contrary. The agreement in that case was a
27 pure “noncompetition” agreement that restricted the employee’s ability to work for or solicit
28 particular clients after he left Arthur Andersen’s employment. *See id.* at 942. The agreement in

1 *Edwards* did not involve, as did the agreement here, a continued quasi-employment relationship
2 between the parties.

3 Notably, by its very terms, Nosal's agreement with Korn/Ferry did not run afoul of
4 Section 16600 because it did not restrain him from engaging in a lawful profession, trade, or
5 business. *At any time*, Nosal could have withdrawn from the agreement and conducted his own
6 executive search activities. In doing so, however, he would have become ineligible to receive the
7 \$25,000 monthly payments, or the lump-sum payments, that Korn/Ferry agreed to pay in return
8 for Nosal agreeing to work solely for Korn/Ferry, payments which Korn/Ferry was not otherwise
9 bound to pay him.

10 Even assuming that the independent contractor agreement that Nosal voluntarily entered
11 into with Korn/Ferry was void under California law, that situation would not require dismissal of
12 the mail fraud charges. The Ninth Circuit has held that “state law is irrelevant in determining
13 whether a certain course of conduct is violative of the wire fraud statute.” *United States v.*
14 *Weyhrauch*, 548 F.3d 1237, 1245 (9th Cir. 2008) (quoting *United States v. Louderman*, 576 F.2d
15 1383, 1387 (9th Cir. 1978)); *see also Weyhrauch*, 548 F.3d at 1245 (noting that Ninth Circuit has
16 “never limited the reach of the federal fraud statutes only to conduct that violates state law”)
17 (honest services mail fraud prosecution of public official).⁸ Although these cases consider state
18 law under different circumstances than in this case, they enunciate the general principle that
19 federal mail fraud prosecutions should not be conditioned on the vagaries of state law.

20 Moreover, despite the defendant's arguments regarding “federalism,” “federal action
21 based on a valid constitutional grant of authority is not improper simply because it intrudes on
22 state interests.” *Weyhrauch*, 548 F.3d at 1246. The Supreme Court's decision in *Cleveland v.*
23 *United States*, 531 U.S. 12 (2000) — cited by the defendant — does not hold otherwise. In
24 *Cleveland*, the Court simply held that the state licenses at issue were not “property” falling within
25 the scope of the mail fraud statute. *Id.* at 20.

26
27 ⁸The Ninth Circuit expressed “no opinion” on the role of state law in honest services
28 fraud prosecutions in the private context. *Weyhrauch*, 548 F.3d at 1237 n.5.

