UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

DAVID NOSAL,

Defendant.
_____/

No. CR-08-0237 EMC

ORDER DENYING DEFENDANT'S MOTIONS (1) FOR A NEW TRIAL AND (2) FOR ACQUITTAL

(Docket Nos. 397, 436, 437)

I. INTRODUCTION

Pending before the Court is Defendant's motions for acquittal and for a new trial. Docket Nos. 436, 437. In April 2013, Defendant stood trial on three counts under the Computer Fraud and Abuse Act ("CFAA"), two counts under the Economic Espionage Act ("EEA"), and one count of conspiracy. At the close of evidence, Defendant moved for a directed verdict of acquittal under Rule 29 of the Federal Rules of Criminal Procedure. Docket No. 397. The Court took the motion under submission and allowed the case to proceed to verdict. Docket No. 398. On April 24, 2013, the jury returned a verdict of guilty on all counts. Docket No. 408. Defendant now brings a motion for acquittal under Rule 29 and for new trial under Rule 33, asserting insufficiency of evidence and legal errors on several points. Docket Nos. 436, 437. As the arguments in the two motions overlap significantly, the Court will consider them together.

///

///

///

II. FACTUAL AND PROCEDURAL HISTORY

The original indictment in this case was filed on April 10, 2008. Docket No. 1. The second superseding indictment ("SSI") was filed on February 28, 2013. Docket No. 309. The government's allegations in the second superseding indictment were as follows.

Defendant is a former high-level employee of Korn/Ferry International ("KFI"), an executive search firm with offices around the world. SSI ¶¶ 1-2. The company is a leading provider of executive recruitment services, assisting companies to fill executive and other high level positions. SSI ¶ 1. Defendant worked for KFI from approximately April 1996 until October 2004. SSI ¶ 2. When he ceased his employment with the firm, he entered into Separation and General Release Agreement, and an Independent Contractor Agreement with KFI. SSI ¶ 2. In these agreements, he agreed to serve as an independent contractor to KFI from November 1, 2004 through October 15, 2005. SSI ¶ 2. He also agreed not to perform executive search or related services for any other entity during the term of his contract. SSI ¶ 2. In return, he received compensation in the amount of $25,000 per month. SSI ¶ 2. Despite these agreements, Defendant began to set up his own rival executive search firm with the assistance of three other current or former KFI employees: B.C., J.F.L., and M.J. SSI ¶¶ 3-5. J.F.L. was Defendant's assistant while he was a Korn/Ferry employee, and continued to be employed by Korn/Ferry after Defendant's departure. SSI ¶ 4. B.C. was a KFI employee until approximately January 2005. SSI ¶ 3. M.J. was a Korn/Ferry employee until approximately March of 2005. SSI ¶ 5.

The second superseding indictment charges Defendant with three counts of obtaining unauthorized access to a protected computer with intent to defraud and obtaining something of value in violation of the CFAA. SSI ¶ 20-21. The counts are based on three occasions in which J.F.L.'s KFI username and password were used to access KFI's Searcher database. SSI ¶ 20-21. The three incidents took place on April 12, 2005, July 12, 2005, and July 29, 2005. SSI ¶ 21. On each occasion, the person accessing Searcher downloaded information from the database, including source lists of candidates KFI had compiled for previous search assignments. SSI ¶ 21. The government alleges that these searches were performed not by J.F.L., but by B.C. and M.J., neither of whom were KFI employees at the time. SSI ¶ 19.

The second superseding indictment also charges Defendant with unauthorized downloading, copying, and duplicating of trade secrets, as well as unauthorized receipt and possession of trade secrets, all in violation of the EEA. SSI ¶ 22-24. The indictment does not specifically identify the trade secrets Defendant is alleged to have obtained. As discussed below, however, the government later indicated to Defendant that these charges were based on three specific source lists and one set of information drawn from a source list, all of which B.C. obtained from Searcher and emailed to Defendant.

Finally, Defendant was charged with conspiracy to commit the CFAA and EEA violations. SSI ¶¶ 12-19. Additional facts and a discussion of the evidence produced at trial are included as relevant to the discussion below.

III. DISCUSSION

A. Legal Standard

Under Federal Rule of Criminal Procedure 29, a defendant may file a motion for a judgment of acquittal after a jury verdict. A Rule 29 motion is basically a challenge to the sufficiency of evidence. "In ruling on a Rule 29 motion, 'the relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *United States v. Alarcon-Simi*, 300 F.3d 1172, 1176 (9th Cir. 2002) (emphasis in original). "[I]t is not the district court's function to determine witness credibility when ruling on a Rule 29 motion." *Id.*

Under Federal Rule of Criminal Procedure 33, a "court may vacate any judgment and grant a new trial if the interest of justice so requires." Fed. R. Crim. P. 33(a). A motion for a new trial may be granted if an error, "in any reasonable likelihood, [could] have affected the judgment of the jury." *United States v. Butler*, 567 F.2d 885, 891 (9th Cir. 1978).

The Ninth Circuit has also noted that a motion for a new trial may be granted where there is a sufficiency-of-the evidence problem. As suggested by the language of the rule, where sufficiency of the evidence is at issue,

> [a] district court's power to grant a motion for a new trial is much broader than its power to grant a motion for judgment of acquittal. "The district court need not view the evidence in the light most

> favorable to the verdict; it may weigh the evidence and in so doing evaluate for itself the credibility of the witnesses." "If the court concludes that, despite the abstract sufficiency of the evidence to sustain the verdict, the evidence preponderates sufficiently heavily against the verdict that *a serious miscarriage of justice may have occurred*, it may set aside the verdict, grant a new trial, and submit the issues for determination by another jury."

United States v. Alston, 974 F.2d 1206, 1211-12 (9th Cir. 1992) (emphasis added). In short, a motion for a new trial should be granted "only in an exceptional case in which the evidence weighs heavily against the verdict." *United States v. Merriweather*, 777 F.2d 503, 507 (9th Cir. 1985); *see also United States v. Camacho*, 555 F.3d 695, 706 (8th Cir. 2009) (stating that "a new trial motion based on insufficiency of the evidence is to be granted only if the weight of the evidence is heavy enough in favor of acquittal that a guilty verdict may have been a miscarriage of justice[;] [n]ew trial motions based on the weight of the evidence are generally disfavored"); *United States v. Martinez*, 763 F.2d 1297, 1312-13 (11th Cir. 1985) (stating that "[t]he court may not reweigh the evidence and set aside the verdict simply because it feels some other result would be *more reasonable*[;] [t]he evidence must preponderate heavily against the verdict, such that it would be a miscarriage of justice to let the verdict stand") (emphasis added).

B. CFAA Counts

Defendant raises a number of arguments as to why he is entitled to either an acquittal or a new trial on the charges under the Computer Fraud and Abuse Act. The CFAA provides criminal penalties for an individual who:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4). The three CFAA counts are based on three incidents where KFI's Searcher database was accessed using J.F.L.'s password and various information was obtained on April 12, 2005, July 12, 2005, and July 29, 2005, respectively. Docket No. 309 at 10 (second superseding indictment). Defendant argues that he is entitled to acquittal or new trial on the CFAA counts because (1) no person gained unauthorized access to Searcher within the meaning of the CFAA; (2)

the Court's deliberate ignorance instruction was confusing; (3) the government provided insufficient evidence that Defendant had the requisite mental state to commit the CFAA violations because the evidence does not show that he was aware that Searcher was being accessed by someone other than J.F.L.; and (4) there is insufficient evidence of a conspiracy that forms the basis for Defendant's liability on these counts.

1. Unauthorized Access

Defendant argues that he cannot be convicted of the CFAA counts because no person gained "unauthorized access" to Searcher on any of the relevant dates. He advances three basic arguments on this front: (1) that under the Ninth Circuit's *en banc* decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012), there can be no CFAA violation where the access was gained with the permission of the password holder and where there was no circumvention of technological barriers; (2) the evidence introduced at trial established that B.C. and M.J. were authorized to access Searcher on the relevant dates; and (3) since Defendant was authorized to receive certain information from Searcher in the course of his work as an independent contractor, he cannot be convicted of accessing a computer without authorization under the CFAA.

a. Circumvention of Technological Barriers

This Court considered and rejected the first argument in denying Defendant's motion to dismiss the remaining CFAA counts on March 12, 2013. Docket No. 314 at 12. The Court noted that, "[n]owhere does the court's opinion in *Nosal* hold that the government is additionally required to allege that a defendant circumvented technological access barriers in bringing charges under § 1030(a)(4)." *Id.* The Court reaffirms its prior ruling. In any event, the Court noted that the indictment does allege circumvention of a technological barrier because "password protection is one of the most obvious technological access barriers that a business could adopt." *Id.*

b. Permission of the Password Holder

Defendant argues that B.C. and M.J. obtained authorization to KFI's Searcher because J.F.L., who had authority, gave them permission, even though (as discussed below), the evidence establishes B.C. and M.J. did not have KFI's authorization. Defendant's argument is without merit. The Court previously rejected this argument, noting that previous Ninth Circuit precedent had made

clear "that it is the actions of the *employer* who maintains the computer system that determine whether or not a person is acting with authorization," and that *Nosal* had not altered this rule. *Id.* at 13-14 (emphasis added) (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) ("The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer.")). Nothing in the CFAA or cases interpreting it suggests the authorization required under the CFAA can come solely from a password holder even where it contravenes the employer's rule.

At the hearing, Defendant argued that reading the CFAA to proscribe access where the password holder consented to another's use of her password would criminalize the common practice of employees who share passwords with each other in the course of accessing their employer's computer system. In that scenario, however, the co-employees are all authorized to access the computer – even if doing so using a co-worker's password violates the employer's policy. Violating an anti-password swapping policy might violate the employer's rule, but would not entail allowing an unauthorized person access to the employer's computer system in violation of the CFAA. Here, J.F.L. gave her password not to other KFI employees, but to former KFI employees who were *no longer authorized to access KFI's computer system*. The focus, as the *Brekka* court recognized, is on whether an employer authorizes *the person* in question to access the computer. *Brekka*, 581 F.3d at 1133.

c. B.C. and M.J.'s Authorization on the Dates in Question

A reasonable trier of fact could find that B.C. and M.J. were not personally authorized to access Searcher on the relevant dates. The evidence at trial established, as Defendant notes, that B.C. and M.J. were authorized to access Searcher when they worked for KFI, that B.C. worked with Nosal in his capacity as an independent contractor while she was still a KFI employee, and that while he was an independent contractor KFI contemplated that Defendant could ask a KFI employee for information he needed from Searcher for KFI searches he was conducting. 2 RT 407; 3 RT 474-75; 3 RT 573-74. The evidence at trial, however, also included the following:

- KFI maintained a policy that prohibited employees from sharing passwords. Gov. Ex. 1; 3 RT 563. Before logging in, users saw a screen indicating that

they needed "specific authority" to access the KFI computer. Gov. Ex. 5; 3 RT at 565-66.

- Peter Dunn, KFI's general counsel, testified that Defendant's KFI username and password were terminated on December 8, 2004, and that in his opinion, Defendant did not have authorization to access KFI's computer system after that date.[1] 2 RT 421. In November 2004, Defendant asked that he be able to keep his KFI email and voice mail until the end of December, but Dunn denied his request. 2 RT 409-10. At no point thereafter did Defendant ask Dunn to have his KFI username and password reinstated. 2 RT 410.

- Marlene Briski, KFI's Vice President of Information Services, testified that B.C.'s KFI username and password were terminated on January 24, 2005, several days after she stopped working for KFI. 3 RT 573-74. M.J.'s KFI username and password were terminated on March 2, 2005, the day after he stopped working for KFI. 3 RT 574.

- Briski testified that J.F.L. was not authorized to give her KFI computer access credentials to individuals who did not work for KFI. 3 RT 575.

- Dunn testified that Defendant was not authorized to provide access to Searcher to non-KFI employees either during or after his employment with KFI. 3 RT 510-11.

- At no point did Defendant ask Dunn to allow non-KFI employees with whom he was working to have access to KFI's computer system. 2 RT 410. Nor did he tell Dunn that he had KFI employees retrieving information from KFI computers for him, or that B.C. and M.J. had continued to work with Defendant after they left employment with KFI. 2 RT 410-11.

- On April 12, 2005, when B.C. conducted the search that is the basis for the first CFAA count, neither she nor Defendant were KFI employees. 5 RT 959-60. At this point in time, B.C. testified that all EDS[2] searches that Defendant had been working on as an independent contractor for KFI had been completed and transitioned back to KFI. 5 RT 963. B.C. testified that she did not have permission from KFI to access its computer system on this date. 5 RT 976.

- B.C. testified that at the time of the July 12, 2005 search, which forms the basis for the second CFAA count, she did not have a valid KFI username and

---

[1] At Defendant's request, the Court provided a limiting instruction at this juncture, stating:

> Ladies and gentlemen of the jury, you will be instructed at the end of this case on the term "authorization" and "authorized access." So when witnesses state their opinion, that is their opinion. But it is up to you, ultimately, to apply the law.

2 RT 421.

[2] B.C. does not explain what the EDS searches were. Dunn had earlier testified that as an independent contractor, Defendant was charged with completing searches he had begun for four companies: Sinogen, BestBuy, Maxtor, and EDS. 2 RT 419.

> password, and that she did not have permission from KFI to access the company's computers. 5 RT 983.
>
> • M.J. testified that at the time of the July 29, 2005 search, which forms the basis for the third CFAA count, he did not have permission from KFI to access the company's computer system. 5 RT 1140, 1143.

Taken together, this evidence is sufficient to establish that neither Defendant nor B.C. nor M.J. had were authorized to access KFI's computers on the relevant dates. A reasonable jury could well have concluded that all three were not authorized, and that B.C. and M.J.'s activities thus constituted unauthorized access in violation of § 1030(a)(4). Nor can it be said that the weight of evidence weighs so heavily against the verdict that a serious miscarriage of justice may have occurred, requiring a new trial. There was substantial, indeed, uncontradicted, evidence that neither B.C. nor M.J. had KFI's authorization to access the Searcher database at the time of the events in question. The Court therefore denies both the Rule 29 motion for acquittal and the Rule 33 motion for a new trial on this issue.

d. Nosal's Authorization

Defendant's final argument is that he was authorized to receive certain information from Searcher in the course of his work as an independent contractor, and therefore he cannot be convicted of accessing Searcher without authorization under the CFAA, regardless of who actually accessed the database on his behalf. Docket No. 436 at 14; Docket No. 448 at 4-7. Defendant cites to no authority to support this proposition, other than cases generally discussing the rule of lenity. The text of the statute, however, is concerned not with permission to access *information*, but rather with permission to access a protected *computer*. The provision of the CFAA under which Defendant is charged provides penalties for anyone who:

> knowingly and with intent to defraud, *accesses a protected computer without authorization*, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C.A. § 1030(a)(4) (emphasis added). The statute further defines the term "exceeds 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.A. § 1030(e)(6) (emphasis added). Cases discussing this provision similarly focus on rights to access a *computer*, not rights to the *information* stored thereon. *See, e.g., Brekka*, 581 F.3d at 1133 (9th Cir. 2009) ("It is the employer's decision to allow or to terminate an employee's authorization *to access a computer* that determines whether the employee is with or 'without authorization.'") (emphasis added). Defendant's argument that since he was authorized to obtain certain information, he cannot be deemed to have violated the CFAA, is thus not supported by the plain text of the statute, and he points to no case so interpreting the CFAA. Nor does Defendant's interpretation of the CFAA make logical sense. Just because a person is authorized generally to receive information from a database does not mean that person can deputize any other person, including one without authorization, to access the computer in clear violation of an employer's rule. The ends do not justify the means.

In any event, in this case, the evidence suggests that Defendant did *not* actually have unqualified access to all of the information on KFI's system. The information Defendant was authorized to receive was limited to information relevant to the searches he was completing for KFI as an independent contractor; however, the information he received was for searches Defendant was conducting for his own business.

2. Deliberate Ignorance Instruction

Defendant contends that he is entitled to a new trial on the CFAA counts because this Court's instruction on deliberate ignorance would have allowed the jury to convict him on the CFAA counts even if they found that J.F.L., who was authorized to access Searcher, had been the one who accessed Searcher. Docket No. 437 at 7-8. The Court's instruction on this front was as follows:

> With respect to Counts 2 through 6 of the indictment (and not Count 1), you may find that the defendant acted knowingly if you find beyond a reasonable doubt that the defendant:
>
> 1. was aware of a high probability that, [B.C., M.J., or J.F.L.] had gained unauthorized access to a computer used in interstate or foreign commerce or communication, or misappropriated trade secrets, downloaded, copied, or duplicated trade secrets without authorization, or received or possessed stolen trade secrets without authorization, and

> 2. deliberately avoided learning the truth.
>
> You may not find such knowledge, however, if you find that the defendant actually believed that these individuals had not gained unauthorized access to a computer used in interstate or foreign commerce or communication, or had not misappropriated trade secrets, downloaded, copied, or duplicated trade secrets without authorization, or received or possessed stolen trade secrets without authorization, or if you find that the defendant was simply careless. This instruction applies to the terms "knew," "know," or "knowingly," not to the term "firmly believed."

Docket No. 401 at 49. Defendant argues that including the name of J.F.L. who was a KFI employee at all relevant times and was authorized to access the KFI computers, erroneously permitted the jury to convict Defendant even if they found that J.F.L. (not B.C. or M.J.) had been the one who accessed Searcher on the occasions that were the subject of the CFAA counts.

As an initial matter, this is the first time that Defendant has raised this objection. Though Defendant previously objected to this instruction generally, he did not specifically object to the inclusion of J.F.L.'s name in the instruction. Docket No. 334 at 3; 7 RT 1530-33. During a discussion regarding this instruction after the close of the government's case, Defendant objected to a previous version of this instruction, which had not named any individuals, and referred to Defendant's "co-conspirators." 7 RT 1530-33. The government proposed omitting the word "co-conspirators," and instead "substituting the actual names of the three people in question." 7 RT 1532-33. Defendant *assented* to this alteration to the instruction. *Id.* Though J.F.L.'s name was not explicitly mentioned, the government specified that it did not intend to include Michael Louie's name in the instruction, and named B.C. and M.J. as two out of the three who would be named in the instruction. *Id.* It was thus quite clear in context that J.F.L. would be the third person named in the instruction. The Court then issued a version of the jury instructions that included J.F.L.'s name in the deliberate ignorance instruction. Docket No. 400. The following day, Defendant raised additional concerns with the deliberate ignorance instruction, but did not object to the inclusion of J.F.L's name. 8 RT at 1543-46. Hence, Defendant waived any objection to including J.F.L.'s name. Fed. R. Crim. P 30(d) ("A party who objects to any portion of the instructions or to a failure to give a requested instruction must inform the court of the specific objection and the grounds for the objection before the jury retires to deliberate.").

Further, in the context of the entire instruction, the inclusion of J.F.L.'s name in the instruction was not an error. As the instruction applies to both the CFAA and EEA counts, including J.F.L.'s name was appropriate because the government alleged that she had participated in the theft of trade secrets (*i.e.*, the EEA counts). Additionally, the instruction makes sufficiently clear to the jury that they could not convict Defendant on the CFAA counts if they concluded that J.F.L. had been the one to access Searcher. Specifically, it allows a finding of deliberate ignorance only where Defendant was aware of a high probability that one of the named individuals obtained "*unauthorized* access." The Court's instructions elsewhere defined authorized access under the CFAA:

> Whether a person is authorized to access the computers in this case depends on the actions taken by Korn/Ferry to grant or deny permission to that person to use the computer. A person uses a computer "without authorization" when the person has not received permission from Korn/Ferry to use the computer for any purpose (such as when a hacker accesses the computer without any permission), or when Korn/Ferry has rescinded permission to use the computer and the person uses the computer anyway.

Docket No. 401 at 36. In light of this instruction, and the fact that the undisputed evidence showed that J.F.L. was an employee with KFI computer access credentials at all relevant times, there is little risk that inclusion of J.F.L.'s name in the deliberate ignorance instruction confused the jury on the CFAA counts. No new trial in "the interest of justice" is warranted. Fed. R. Crim. P. 33(a). The Court therefore denies Defendant's Rule 33 motion on this issue.[3]

3. Defendant's Knowledge of Downloads

Defendant also contends that he is entitled to an acquittal or new trial because there is insufficient evidence that he was aware that the downloads from Searcher were being conducted by B.C. and M.J., rather than J.F.L., who was authorized to access KFI's computer system. Docket No. 10-11, 15-16. The government, however, presented a significant amount of evidence suggesting that Defendant was aware, or at least maintained deliberate ignorance, of the fact that B.C. and M.J. were accessing Searcher without authorization from KFI. The evidence at trial included:

[3] Defendant does not appear to raise this issue in his Rule 29 motion. In any case, the issues Defendant raises here would not constitute error under the Rule 29 standard either.

- In the spring of 2004, J.F.L. and B.C. had conversations about the possibility of Defendant leaving KFI. 6 RT 1284-85. B.C. encouraged Defendant to leave KFI, telling him that they could take KFI information with them when they left. *Id.* Defendant's reaction was to say "don't talk about this in front of me. I don't want to hear it. Talk about it amongst yourselves." 6 RT 1285. Defendant did *not* tell them *not* to take KFI data. *Id.*

- At a later date, but before Defendant left KFI, J.F.L., who had been tasked with making copies of candidate resumes, asked Defendant where to save them. 6 RT 1286. Defendant told her to figure it out on her own, but told her to purchase any media she used for storage using his personal credit card rather than his KFI business card. *Id.*

- During the time he worked at KFI, Defendant relied on B.C. to retrieve information for him from Searcher on a daily basis. 5 RT 921.

- B.C. testified that though J.F.L. was Defendant's executive assistant while he worked for KFI and she had a basic familiarity with Searcher, she typically did not pull old source lists for him; B.C. would do that for him. 5 RT 921-22.

- J.F.L. testified that she had never pulled an old source list or run a custom report for source lists, and that she did not know how to do either of these things. 6 RT 1279-80, 1337.

- Prior to the April 12, 2005 search, Defendant had discussions with B.C. about how to obtain the information necessary for a search for a client he was trying to attract. B.C. testified that Defendant "was very instructive about where to have – what searches that he had done or what searches from the source list that could be retrieved." 5 RT 958-60. She further testified that Defendant "asked – he asked me to use searches that Korn/Ferry had done in their database, to find candidates for him that he could quickly call." 5 RT 959. She testified that Defendant had told her to "Get what you need. Get what I need." 5 RT 971. J.F.L. was involved in some of these conversations. 5 RT 960. B.C. testified that she subsequently accessed Searcher with J.F.L.'s password and then emailed the information she retrieved to Defendant. 5 RT 959-64.

- On the day of the July 12, 2005 search, B.C. was working in the Nosal Partner's office, and Defendant had been yelling at B.C., telling her that he needed a contact number for a candidate. 5 RT 985, 988. B.C. obtained the number for him from Searcher. 5 RT 988.

- B.C. and Defendant had a romantic as well as professional relationship. 5 RT 925-26. During the course of their romantic relationship, which ended in the spring of 2005, Defendant and B.C. spoke every day. 5 RT 926. She discussed with him the things she was doing in her work life, including keeping him up-to-date on searches she was working on for him, telling him which source lists she was looking at, and brainstorming source lists to use in new searches. 5 RT 925-26.

- B.C. testified that there was no doubt in her mind that Defendant knew that she was accessing Searcher after she left KFI, and that he knew she was doing so with J.F.L.'s password. 5 RT 1080-81.

- After the civil litigation between Defendant and KFI commenced, Defendant never spoke to B.C. or expressed anger at her about the fact that she had accessed KFI's computer system after she was no longer a KFI employee. 5 RT 1000.

- M.J. testified that though Defendant had never directed him to take source lists from Searcher, it was his understanding based on conversations he had with Defendant, B.C., and others that one of his tasks for the business Defendant was starting was to bring data from KFI. 5 RT at 1104-05.

- In July of 2005, Defendant, M.J., B.C. and others participated in a training by a software company from which Nosal Partners had purchased a database. 5 RT 1135-36. At this training, M.J. mentioned that he had source lists from Searcher for import into the new database. 5 RT 1137. Defendant denied to the software company representative that they had the data from Searcher. 6 RT 1176, 1271. Defendant winked at M.J. during this interaction. 6 RT 1176. J.F.L. testified that when M.J. said this, she and Defendant looked at each other "a bit startled that [M.J.] would blurt out something like that." 6 RT 1339.

- M.J. testified that Defendant had this reaction to "various situations over time," and that "he knew we had it but he didn't want to kind of acknowledge it." 6 RT 1175-76.

- Defendant expressed surprise at the amount of data M.J. had, but did not tell him to get rid of the data. 5 RT 1137-38. He told M.J. that he did not want to know about the information M.J. had brought from KFI. 6 RT 1216.

- M.J. testified that there was no doubt in his mind that Defendant was aware that data he had obtained for Nosal Partners was obtained from the Searcher database. 6 RT 1229-30.

The above evidence, taken together, was sufficient to support a finding that Defendant knew that B.C. and M.J. had accessed Searcher without authorization, that he had remained deliberately indifferent to this fact, and/or that he conspired to commit the CFAA violations with which he was charged. The jury heard evidence that Defendant gave B.C. specific directions about information that he wanted from Searcher, and that he was aware that M.J. had a large amount of data taken from Searcher. Importantly, J.F.L., Defendant's longtime executive assistant, did *not* know how to run the types of searches that were the basis for the CFAA counts here. Further, when Defendant had worked for KFI, it had been *B.C.*, and *not J.F.L.*, who would run these types of searches for him. The jury could reasonably have inferred that Defendant, who had worked with J.F.L. closely, would have been aware that she could not have been running the searches in question, and that the work would have to be done by M.J. and B.C. There was evidence that Defendant specifically directed his requests to B.C. and that there was an implicit understanding that M.J. would obtain information

from Searcher for Defendant's new business, and that Defendant knew that B.C, and M.J. did not have authorization to access KFI computers after they ended their employment with KFI.

The jury further heard evidence that at different points in time Defendant had specifically instructed J.F.L, B.C., and M.J. that he did not want to know about data they might take from KFI. J.F.L testified to conversations she and B.C. had with Defendant where he had told them to figure such issues out for themselves, and that he did not want to hear about it. M.J. testified that Defendant had indicated to him that he did not want to know about the data M.J. had taken from Searcher, but that M.J. understood from his interactions with Defendant that it was expected that he would obtain information from Searcher. Both B.C. and M.J. testified that they were certain that Defendant knew that they had accessed Searcher during the relevant period.

Given this evidence, a reasonable jury could have concluded that the government had proved beyond a reasonable doubt that Defendant knew of, was deliberately indifferent to, and/or had conspired to commit the CFAA violations by having B.C. and M.J. access Searcher without KFI's authorization.

The interests of justice do not require a new trial on these grounds. Nor is there insufficient evidence warranting relief under Rule 29. The Court therefore denies both of Defendant's motions on this issue.

4. Evidence of Conspiracy

Defendant argues that there was not sufficient evidence of a conspiracy to convict him of the CFAA violations based on co-conspirator liability. However, the evidence discussed in the previous section is sufficient to support a finding that he entered into a conspiracy to gain unauthorized access to the Searcher database.

Defendant also argues, without much explanation, that in order to establish co-conspirator liability based on conspiracy to violate the CFAA, the government was required to establish that Defendant, B.C., and M.J. entered into a conspiracy *after* B.C. and M.J. stopped working for KFI. Docket No. 436 at 10. This argument seems based on the premise that since B.C. and M.J. could access Searcher with authorization during their employ with KFI, it was not possible to conspire to violate the CFAA until they were no longer employees. The fact that a CFAA violation was not

possible at the time the conspiracy formed, however, does not mean that Defendant, B.C., and M.J. could not have entered a conspiracy in 2004 to commit CFAA violations at some future point when it was anticipated that B.C. and M.J. would no longer employed by KFI (being employed or working independently with Defendant's new business instead). Moreover, they could have entered a conspiracy at that point in time to KFI's steal trade secrets from Searcher to facilitate the establishment of Defendant's new business. The conspiracy would have encompassed not only violation of the EEA (discussed below), but all reasonably foreseeable crimes committed in furtherance of the conspiracy. *United States v. Chong*, 419 F.3d 1076, 1081 (9th Cir. 2005) (citing *Pinkerton v. United States*, 328 U.S. 640 (1946)). Gaining access to those trade secrets through unauthorized means in violation of the CFAA could well have been found to be acts foreseeably contemplated and hence within the scope of the conspiracy to steal trade secrets. In fact, the jury heard evidence from which it could infer that the parties had entered a conspiracy in mid-2004 to commit violations of the CFAA, the EEA, or both. *See, e.g.*, 6 RT 1284-86 (discussions between Defendant, B.C., and J.F.L. about leaving KFI and taking KFI data; Defendant instructed J.F.L. to use his personal credit card to buy discs for use in copying KFI data).

In any case, the jury also heard ample evidence from which they could infer that the parties had entered a conspiracy to commit the CFAA violations after B.C. and M.J. no longer worked at KFI. *See, e.g.*, 5 RT 958-71 (Defendant's directions to B.C. related to the April 12, 2005 search); 5 RT 925-26 (Defendant and B.C. had close personal as well as professional relationship and discussed work daily); 5 RT at 1104-05; 6 RT 1175-76 (M.J. understood that Defendant wanted him to bring KFI information to the new business; Defendant indicated he did not want to know the details); 5 RT 1080-81; 6 RT 1229-30 (B.C. and M.J. stated they had no doubt that Defendant was aware of their activities in accessing Searcher).

As the Court finds that there was adequate evidence to support the jury's verdict on the conspiracy count, whether based on activities before or after Defendant, B.C., and M.J. left KFI, Defendant's motions on this issue are denied.

C. EEA Counts

The jury returned a verdict of guilty on two counts under the Economic Espionage Act, for unauthorized downloading, copying, and duplicating of trade secrets without authorization; and for receipt and possession of stolen trade secrets. Docket No. 408. In relevant part, this statute reads:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly –
>
> (1) . . .
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) . . .
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a).

Prior to trial, the government had indicated that these counts were not based on the contention that Searcher itself was a trade secret; instead, the government asserted that certain source lists that had been obtained from Searcher were the alleged trade secrets the formed the basis for these counts. *See* Docket No. 335-1 (November 29, 2012 letter identifying the source lists the government contends were trade secrets, including those that were downloaded using B.C., M.J.'s and J.F.L.'s login credentials at various points in 2004 and 2005). Ultimately, with the government's approval, the Court's instructions at the close of trial specifically identify four potential trade secrets: the three source lists contained in the government's Exhibit 58, or (for the Count Six only) the information regarding CFOs contained in the government's Exhibit 60. Docket No. 401 at 38-39.

Defendant raises four arguments for why he is entitled to an acquittal or new trial on the EEA counts: (1) the Court erred in instructing the jury that it could find Defendant guilty of conspiracy to commit the EEA violations even if there was in fact no trade secret; (2) there was insufficient evidence that the source lists in question were trade secrets; (3) there was insufficient evidence that Defendant and his co-conspirators knew or believed that the source lists were trade secrets; and (4) there is insufficient evidence that Defendant and his co-conspirators knew or believed that taking the source lists would cause KFI economic harm.

1. *Hsu* and Requirement of Actual Trade Secret

Defendant argues that he is entitled to a new trial on all counts because this Court instructed the jury that it could find Defendant guilty of conspiracy to misappropriate, receive, possess, and transmit trade secrets even if the source lists were not trade secrets so long as Defendant "firmly believed" that they were. Docket No. 437 at 12-17. Since a finding of conspiracy on this theory could be the basis of Defendant's conviction on all other counts on a theory of co-conspirator liability, Defendant argues that error on this front requires a new trial on all counts. *See* Docket No. 401 at 33 (*Pinkerton* instruction).

The Court instructed the jury as follows with regards to count one of the indictment and the allegation that Defendant was part of a conspiracy to commit EEA violations:[4]

> In Count One of the indictment, the defendant is charged with conspiracy to misappropriate, receive, possess, and transmit trade secrets. As with the charges for attempt, in order to prove the defendant's guilt beyond a reasonable doubt on the conspiracy charges, the government need not prove the existence of actual trade secrets and that Defendant knew that the information in question was a trade secret. However, the government must prove that Defendant firmly believed that certain information constituted trade secrets.

Docket No. 401 at 46. This instruction was based on *United States v. Hsu*, 155 F.3d 189, 193 (3d Cir. 1998) and Ninth Circuit cases finding that legal impossibility is not a defense to the attempt or conspiracy charges. *See United States v. Fiander*, 547 F.3d 1036, 1042 (9th Cir. 2008) ("we have

[4] The conspiracy charge also charged Defendant with conspiracy to violate the CFAA. Defendant's objections to that portion of the conspiracy charge are discussed in the section on the CFAA charges above.

held that a conspiracy conviction may be sustained even where the goal of the conspiracy is impossible"); *United States v. Quijada*, 588 F.2d 1253, 1255 (9th Cir. 1978) (holding that impossibility is not a defense to attempt, and that "generally a defendant should be treated in accordance with the facts as he supposed them to be").

"Legal impossibility exists when the intended acts would not constitute a crime under the applicable law." *United States v. McCormick*, 72 F.3d 1404, 1408 (9th Cir. 1995) (distinguishing factual impossibility, which "refers to those situations in which, unknown to the defendant, the consummation of the intended criminal act is physically impossible") (internal citations omitted). In *Hsu*, the defendants were charged with attempt to steal trade secrets and conspiracy to steal trade secrets, and requested discovery that would enable them to prove that the documents they had attempted to obtain did not contain trade secrets. *Id.* at 193. The court ruled, however, that the documents were not relevant to the defendant's defense because legal impossibility is not a defense to either attempt or conspiracy. *Id.* at 203. Here, as in *Hsu*, Defendant argues that he should be able to raise the defense of legal impossibility because the information in question was not a trade secret.[5]

Though the Ninth Circuit has not explicitly addressed the defense of legal impossibility in a trade secrets case, other circuits have followed *Hsu* in holding that proof of an actual trade secret is not necessary in order to support a conviction for of conspiracy to steal trade secrets. *See United States v. Wen Chyu Liu*, 716 F.3d 159, 170 (5th Cir. 2013) ("the relevant inquiry in a conspiracy case, such as this one, is whether the defendant entered into an agreement to steal, copy, or receive information that he believed to be a trade secret"); *United States v. Yang*, 281 F.3d 534, 544 (6th Cir.

---

[5] As the court in *Hsu* noted, this defense could also arguably be classified as one of factual impossibility. 155 F.3d at 199. The court there observed that "the distinction between factual and legal impossibility is essentially a matter of semantics, for every case of legal impossibility can reasonably be characterized as a factual impossibility." *Id.* The Ninth Circuit has also expressed skepticism about drawing a firm distinction between the legal impossibility and factual impossibility. *United States v. Quijada*, 588 F.2d 1253, 1255 (9th Cir. 1978) ("Specifically, we eschew any effort to distinguish so-called Legal impossibility from Factual impossibility or to establish any general principles capable of solving most, if not all, instances in which the defense is raised. We can only say that generally a defendant should be treated in accordance with the facts as he supposed them to be."). In any case, it matters little whether Defendant's argument is characterized as raising legal or factual impossibility as a defense, because the Ninth Circuit has also recognized that "[f]actual impossibility is not a defense to an inchoate offense" such as conspiracy. *United States v. Fleming*, 215 F.3d 930, 936 (9th Cir. 2000).

2002) ("The fact that the information they conspired to obtain was not what they believed it to be does not matter because the objective of the Yangs' agreement was to steal trade secrets, and they took an overt step toward achieving that objective."); *United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000) (rejecting challenge to theft of trade secrets conviction on the ground that the defendant actually received no trade secrets); *see also Fiander*, 547 F.3d at 1042 (citing *Yang* with approval). This Court earlier rejected Defendant's argument that the reasoning in *Hsu* is not applicable here, and that the government was thus required to prove the existence of an actual trade secret in order to secure a conviction on the conspiracy charge. Docket No. 354 at 47-48; Docket No. 402.

This ruling allowing for a conviction of conspiracy even if the conduct did not constitute a substantive violation of the underlying law is consistent with the Supreme Court's recognition that conspiracies themselves are a distinct evil, independent of whether or not their ends are ever achieved. The Court has recognized that "[i]t is elementary that a conspiracy may exist and be punished whether or not the substantive crime ensues, for the conspiracy is a distinct evil, dangerous to the public, and so punishable in itself." *Salinas v. United States*, 522 U.S. 52, 65 (1997). "The conspiracy poses a threat to the public over and above the threat of the substantive crime's commission-both because the combination in crime makes more likely the commission of other crimes' and because it decreases the probability that the individuals involved will depart from their path of criminality." *United States v. Jimenez Recio*, 537 U.S. 270, 275 (2003) (internal citations omitted). Even if the source lists had not been trade secrets – and thus the object of the conspiracy had been impossible – Defendant and his co-conspirators could have still acted culpably in conspiring to steal what they firmly believed to be trade secrets.[6]

---

[6] The Court's instruction that Defendant could be convicted on the conspiracy charge based on his "firm belief" that the source lists in question were trade secrets is further supported by the legislative history of the EEA. A statement made by the EEA's bill managers discussed safeguards in the bill that would prevent an overly expansive application of the EEA. The statement indicated that one of these safeguards:

> is provided by the bill's use of the term ''knowingly.'' For a person to be prosecuted, the person must know *or have a firm belief* that the information he or she is taking is in fact proprietary. Under theft statutes dealing with tangible property, normally, the thief knows that the object he has stolen is indeed a piece of property that he has no lawful right to convert for his personal use. The same principle

In addition to the fact that Defendant offers no new argument that would justify re-visiting the Court's prior ruling, any instructional error here would be harmless as a practical matter. The possibility that the jury could have found Defendant guilty of conspiracy based merely on his "firm belief" that the source lists were trade secrets is obviated by the fact that the jury found Defendant guilty of the substantive EEA counts. The Court had instructed the jury that in order to find Defendant guilty on Count Five (an EEA count), the jury had to find that at least one of the source lists identified in the government's Exhibit 58 is in fact a trade secret; the Court also instructed to the jury that in order to find Defendant guilty on Count Six (another EEA count), the jury had to find that at least one of the Exhibit 58 source lists or the information regarding CFOs contained in the government's Exhibit 60 was in fact a trade secret. Docket No. 401 at 38-39. The instructions on both counts indicated that the jury also had to find that Defendant knew (not just firmly believed) that the source list or information was a trade secret. *Id.* Since the jury convicted Defendant on Counts Five and Six, they necessarily found that at least one of the source lists B.C. sent to Defendant in Exhibit 58 was a trade secret, and that Defendant was aware of this fact. This verdict makes it logically impossible that the jury convicted Defendant of conspiracy on a finding that he conspired to misappropriate, receive, possess, and transmit information that he believed to be a trade secret but that was in fact not a trade secret. Defendant suffered no prejudice as a result of the alleged instructional error.

Defendant also argues that the Court's instruction pursuant to *Hsu* amounts to an impermissible constructive amendment to the indictment. Docket No. 437 at 14-17. This Court

---

> applies to this measure – for someone to be convicted under this statute he must be aware *or substantially certain* that he is misappropriating a trade secret (although a defense should succeed if it is proven that he actually believed that the information was not proprietary after taking reasonable steps to warrant such belief). A person who takes a trade secret because of ignorance, mistake or accident cannot be prosecuted under the Act.

142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996) (managers' statement for H.R. 3723, the Economic Espionage Bill) (emphasis added). This suggests a legislative intent which contemplated that a firm belief could be sufficient to support a conviction for violation of the EEA. Allowing conviction for conspiracy to violate the EEA based on mere firm belief, therefore, does not appear to be inconsistent with the Congressional intent as indicated by the passage quoted herein.

previously rejected the Defendant's argument that the challenged conspiracy instruction effected a constructive amendment of the indictment because it allowed the government to secure a conviction based on the theory that he firmly believed the source lists were trade secrets, even if they were not. Docket No. 402. In his Rule 33 motion, Defendant raises a new constructive amendment argument for the first time, arguing that the conspiracy instruction allowed the jury to convict Defendant on the conspiracy charge based on a finding that Searcher was a trade secret. He bases this argument on the fact that the Court did not specifically instruct the jury that they could not base a conspiracy conviction on a finding that Defendant and his co-conspirators conspired to steal Searcher, which they firmly believed to be a trade secret.

Viewed in the context of the other jury instructions, Defendant's argument is unconvincing. The Court's instruction on the elements of conspiracy required the jury to find that "beginning on a date unknown, and continuing to no later than August 2, 2005, there was an agreement between two or more persons to commit at least one crime as charged in the indictment" in order to convict Defendant on the conspiracy charge. Docket No. 401 at 30. As noted above, the substantive EEA charges specifically identified the source lists and CFO information in government Exhibits 58 and 60 as the alleged trade secrets. Docket No. 401 at 38-39. It did not include Searcher.

In light of these other instructions, the Court finds that the jury was not permitted by the instruction to base a conviction on a finding that Searcher was a trade secret. In any event, given that the conviction on the substantive EEA counts means that the jury necessarily found at least one of the source lists in government's Exhibit 58 to be a trade secret, it is improbable if not logically impossible that the jury convicted Defendant of conspiracy solely on the theory that he and his co-conspirators firmly believed Searcher to be a trade secret. The Court therefore denies Defendant's motions on the above grounds.

2. Evidence Source Lists Were Trade Secrets

Defendant argues that he is entitled to an acquittal or new trial on the EEA counts because the government failed to introduce sufficient evidence that the source lists in Exhibit 58 or the CFO information in Exhibit 60 were, in fact, trade secrets. Specifically, he argues that the government failed to prove that the information in question was not drawn entirely from publically available

sources, and that the source lists had not been publically disclosed.[7] The EEA defines trade secret as follows:

> the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if –
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public;

18 U.S.C. § 1839(3). The Court's instruction on the definition of trade secrets closely tracked this language. Docket No. 401 at 42.[8] Though Defendant offers various cases discussing the definition of trade secrets, he does not contest the accuracy of the Court's instructions on the definition of trade secrets in the instant motions, only the sufficiency of evidence on this issue. Docket No. 436 at 18-35; Docket No. 448 at 15.

---

[7] Defendant also argues that there was insufficient evidence regarding the content of the pre-April 2005 downloads, such that there can be no finding that the information downloaded on those occasions cannot be the basis for the EEA convictions. As the substantive EEA counts specified that the trade secrets in question were the source lists in the government's Exhibit 58 and the source-list derived information in the government's Exhibit 60, this argument only applies to the conspiracy count to the degree that it is based on allegations of conspiracy to violate the EEA rather than CFAA. As discussed in the previous section, however, given the jury's verdict on the substantive EEA claims, they necessarily would have found that at least some of the information in Exhibits 58 and 60 constituted a trade secret, so it is highly improbable that the conspiracy conviction is based solely on other alleged trade secrets.

[8] The Court additionally provided the following instruction on trade secrets:

> As members of the jury, it is your responsibility to determine whether something constitutes a trade secret under the test I have just given you. Just because a witness referred to certain information or documents as trade secrets does not mean that they are necessarily trade secrets within the meaning of the statute. Similarly, just because a document refers to information as a trade secret, confidential, or proprietary, does not necessarily make that information a trade secret if it does not otherwise meet the test I have just described to you.

Docket No. 401 at 43.

a. Creation of Source Lists

It is true that the evidence at trial suggested that much of the information in Searcher was drawn from publically available sources, and that it was often not possible to determine the origin of any particular information contained in a source list. 2 RT 315-21; 4 RT 815-16; 5 RT 1020-21. Further, there was evidence that when individuals in the executive search industry changed firms, they would at times bring information from their old firm with them to their new firm. 2 RT 318-19, 5 RT 1020-21.

The following evidence was also introduced at trial, however, that would support a finding that the source lists derived from Searcher were compilations of both public and non-public information that had been arranged in ways that provided more information and value than a mere recitation of the publically available information:

- Caroline Nahas, KFI's Southern California Managing Director, testified that source lists were "derived from years of accumulated work that came from private information that individuals shared with us." 2 RT 317. She additionally testified that "Searcher is compiled of information that we have built for decades of – since, you know, I believe, 1995. And it's a very valuable tool to us. And it's like the foundation of our work. It's not the only thing, but it is the foundation that we use on every single search." 2 RT 340-41.

- B.C. testified that she would put information into Searcher from a variety of sources, including the internet, Hoovers, ZoomInfo, OneSource, corporate directories, newspapers, and company websites. Once this information was entered into Searcher, it was unnecessary to return to the original sources. 5 RT 1071-73.

- The source lists often included personal contact information for executives that would not have been publically available. 2 RT 322-23; 5 RT 919-20. This information was highly valuable in conducting searches because it enabled the person conducting the search to more easily and privately contact potential candidates. 4 RT 899; 6 RT 1327.

- The source lists contained in the government's Exhibit 58 contain a number of cell, home, and direct telephone numbers for candidates. Gov. Ex. 58.

- KFI employees would often return to an old source list when working on a new assignment because the old lists were helpful to see work that had previously been done and to identify names that would be appropriate for the new search. 2 RT 296-98; 5 RT 1095.

- Nahas testified that KFI employees would draw on old source lists in building a new source list, but would also supplement with additional research to fill gaps in the list. Larger initial source lists, which could have 600 people or more, would then be whittled down by the employees working on the search

> who would make determinations of who would be the best fit for the position, and who would also call the individuals directly to gauge interest. 2 RT 299-300.

Additionally, the jury could have inferred that the information contained in the source lists was not entirely public based on the fact that Defendant and his co-conspirators went to significant trouble to retrieve this information from Searcher. If the information was all publically available, it would make little sense for them to go to such an effort to obtain the information from Searcher.

The above evidence amply supports a finding that the information in Searcher was a compilation that included not just information from public sources, but also information drawn from private sources, and that KFI employees had expended considerable time and judgment in collecting, entering, analyzing, and distilling this information. This is especially true of the source lists compiled from the information in Searcher. KFI employees created source lists in response to searches for individual clients; they contained the list of candidates thought to be the best fit for a specific position with a specific employer. These lists were not merely the result of a mechanical search function, but reflected the judgment and work product of KFI employees experienced in the field of recruiting; the lists were the result of a selective process tailored to the particular circumstances of the search. As such, they had value in future similar searches far beyond an unvetted collection of publically available information. The Court therefore rejects Defendant's argument that the source lists cannot be trade secrets because the government failed to prove that they contained nothing but publically available information.

b. Disclosure to Third Parties

Defendant also argues that the government failed to meet its burden of establishing that the information and source lists in question were trade secrets because the government failed to introduce sufficient evidence to demonstrate that these alleged trade secrets had not been disclosed to any third parties, such as former KFI clients. In support of his argument, Defendant points to *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984). In that case, the Court held that trade secrets could constitute property protected by the Takings Clause of the Fifth Amendment. *Id.* at 1003-04. In discussing the nature of property rights in trade secrets, the Court noted that

> Because of the intangible nature of a trade secret, the extent of the property right therein is defined by the extent to which the owner of the secret protects his interest from disclosure to others. Information that is public knowledge or that is generally known in an industry cannot be a trade secret. If an individual discloses his trade secret to others who are under no obligation to protect the confidentiality of the information, or otherwise publicly discloses the secret, his property right is extinguished.

Id. at 1002.

Defendant correctly points out that the evidence at trial indicated that KFI would sometimes disclose source lists to clients or potential clients, and that KFI would engage in consulting services for clients in which KFI would disclose certain information from Searcher to the client. 2 RT 447-48; 4 RT 807; 5 RT 1020-22. The government also, however, introduced evidence that would support a conclusion that such disclosure was a relatively rare occurrence and that the alleged trade secrets at issue in this case had not been disclosed to third parties, or had been disclosed only subject to a confidentiality agreement.

- Nahas testified that clients were generally given information from source lists, but not given the lists themselves. 2 RT 299-301, 312-313.
- Dunn testified that when KFI provided information from Searcher to clients, the practice was to designate the information as confidential and for the client's use only. 2 RT 448-49.
- With regards to the specific source lists in question, Briski testified that they had not been posted on the internet or otherwise released by KFI, and that she was unaware of anyone outside KFI who had come into possession of the source lists. 4 RT 865-67.
- B.C. testified that to her knowledge, Searcher was the only place to obtain the information contained in the three source lists contained in the government's Exhibit 58. 5 RT 977-78. From this, the jury could infer that the lists had not been disclosed to any outside entity; if the lists had been given to KFI clients, B.C. could have obtained the lists by asking the clients for them.
- With respect to the information in the government's Exhibit 60, the jury heard evidence that the source list from which the names were copied came from an open search engagement which had begun only twelve days prior to B.C.'s email sending the names to Defendant. 4 RT 765-771. Given the short amount of time this list had been in existence, the jury could have reasonably inferred that it had not been disclosed to any entity outside KFI at the time B.C. obtained the information.

On this record, a reasonable jury could have found that the trade secret status of the source lists at issue was not destroyed by any disclosure to third parties.

c. Reasonable Steps to Protect Searcher

The government introduced significant amounts of evidence tending to show more generally that KFI took reasonable steps to protect Searcher and the source lists drawn from Searcher from public disclosure:

- Nahas testified that to her knowledge, KFI did not permit source lists to be sent outside of the company. 2 RT 298. She also testified that non-KFI employees were not permitted to access Searcher or source lists drawn from Searcher. 2 RT 304.
- Searcher could not be accessed unless the user signed onto KFI's computer system with a KFI username and password, but once in the KFI computer system, no additional password was needed to access Searcher. 5 RT 1023-24.
- M.J. testified that prior to leaving KFI, there was never a time when he provided a source list to a KFI competitor. 5 RT 1095.
- Nahas testified that she never sent a source list to a KFI competitor. 2 RT 346.
- In 2005, the Searcher database was housed on servers at a data center in Burbank, California. Access to the center was restricted to two to three KFI employees and access was controlled by biometric identification. The facility has 24/7 guards and monitoring. 3 RT 583-84.
- Searcher is protected by a firewall and anti-virus software. 3 RT 584-85.
- Briski testified that there are "triggers" built into Searcher that allows KFI to later review the downloading activity of users. 3 RT 615-17. Prior to the incidents that form the basis for the allegations in this case, KFI had never detected incidents where employees downloaded large amounts of data immediately prior to the end of their employment on a scale that M.J., B.C., and Louie did. 3 RT 648-49. This incident prompted KFI to build additional "triggers" into Searcher to better monitor downloads from Searcher. *Id.*
- When users ran a custom report in Searcher, a dialog box would appear that stated in relevant part: "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." Gov. Ex. 2 at 7. When the user exported lists from Searcher to excel, the words "Korn/Ferry Proprietary & Confidential" would appear at the top of the document. Gov. Ex. 2 at 12. *See also* 3 RT 614-15 (Briski's testimony concerning these dialog boxes).

To be sure, there is evidence in the record that KFI did not take every conceivable step to protect Searcher and the source lists:

- There was nothing in the KFI system that prevented users from emailing source lists to people or printing out source lists. 5 RT 1026-27.

- Source lists were not encrypted or protected with separate passwords. 5 RT 1026.
- KFI employees would print out source lists, and take the lists home with them. KFI did not have a procedure in place to prevent employees from taking source lists home. 5 RT 1019-20.
- KFI employees would email source lists to people outside of KFI, including clients. 5 RT 1020.

The statute, however, requires only that the owner of trade secrets take "reasonable" steps to protect the trade secrets, not every conceivable step. *See United States v. Hanjuan Jin*, 833 F. Supp. 2d 977, 1008 (N.D. Ill. 2012) ("Thus, while a trade secret owner need not take 'every conceivable step to protect the property from misappropriation,' H.R. Rep. No. 104–788, at 7, 1996 U.S.C.C.A.N. 4021, 4026, the owner must employ precautionary measures that are reasonable under the circumstances.").

d. Conclusion

The evidence at trial is sufficient to support the jury's verdict. The jury heard evidence that the information in the source lists came from a variety of public and non-public sources, and that KFI had expended considerable time and effort to analyze, distill, and arrange that information in a useful manner for specific positions. The jury also heard evidence that KFI took a number of steps to maintain the secrecy of the information in Searcher and the source lists drawn from Searcher. Finally, there was significant evidence from which it could be inferred that the source lists in question had not been previously disclosed to any entity outside of KFI. The government thus introduced sufficient evidence to support a finding that the source lists were compilations of information that were not generally known or readily ascertainable by the public through proper means. As discussed in Section III.C.3 and III.C.4 below, the government also introduced sufficient evidence to support a finding that the source lists derived economic value from the fact that they were secret because they gave KFI an edge over competitors and allowed them to conduct searches for clients more efficiently, quickly finding candidates who were the best fit. The jury thus could have reasonably found that the government had established beyond a reasonable doubt that the source lists were trade secrets within the meaning of the EEA. *See* 18 U.S.C. § 1839(3).

On this record, Defendant has not established that he is entitled to a judgment of acquittal or a new trial. His motions on this issue are therefore denied.

3. Evidence Conspirators Knew or Believed Source Lists Were Trade Secrets

Defendant argues that he is entitled to an acquittal or new trial because the government failed to introduce sufficient evidence that he and his co-conspirators knew that the source lists that were the subject of the EEA counts were trade secrets. He argues that the government introduced no information regarding the co-conspirator's knowledge that is specific to the alleged trade secrets.

Defendant, however, is incorrect on this point. The government introduced evidence showing both that the co-conspirators were generally aware that KFI considered information obtained from Searcher to be confidential, and that they were aware that the specific source lists and information alleged to be trade secrets in this case were, in fact, trade secrets.

- Defendant, M.J., B.C., and J.F.L. all signed documents titled "Agreement to Protect Confidential Information" during the course of their employment with KFI. Gov. Ex. 7, 12, 14, 16. This agreement defined confidential information to include client lists, client prospects, business development information, source lists, executive lists, and candidate lists, profiles, and reports. *Id.* The agreement stated that the employee agreed to keep the confidential information private and use it only in connection with their work for KFI. *Id.*; 5 RT 1093-94.

- As a Managing Director at KFI, Defendant had sent offer letters to M.J. and J.F.L. that specified, among other terms, that the employee agreed to keep confidential candidate lists, personal histories or resumes, employment information, business information, customer lists, business secrets, and the firm's list of clients and placement candidates. Gov. Ex. 15, 17.

- Dunn testified that KFI would not have hired Defendant had he not signed the confidentiality agreement, and that Defendant at no point indicated that he disagreed with the agreement. 2 RT 357-60.

- B.C. testified that she understood it to be a violation of this confidentiality agreement to email source lists to competitors, and that she felt her actions in taking information from Searcher for Nosal Partners were wrong because the information belonged to KFI. 5 RT 1076-78.

- The source lists in the government's Exhibit 58 have the words "Korn/Ferry Proprietary & Confidential" at the top of each document. Gov. Ex. 58. After B.C. sent these lists to Defendant, he never mentioned or expressed surprise at the fact that the documents contained this heading. 5 RT 976-77.

- B.C. states that to her knowledge, Searcher was the only place to obtain the information contained in the three source lists contained in the government's Exhibit 58. 5 RT 977-78.

- The CFO information contained in the government's Exhibit 60 does not contain this header because it is merely a list of names and contact information pasted into the body of an email. Gov. Ex. 60. However, B.C. testified that she obtained this information from a KFI source list. 5 RT 964-66.

- Briski testified that the information from the Government's Exhibit 60 was copied and pasted from a then-open KFI search for a company called Sirna Therapeutics. 4 RT 767-69. She came to this conclusion because the names were identical, as were certain typographical irregularities, such as some names being in all capital letters. *Id.*

- The government introduced a copy of the list B.C. sent Defendant in Exhibit 60 that had Defendant's handwriting on it, circling some candidates, crossing out others, adding names, and indicating that he had left a message for some of the candidates. 5 RT 968; Gov. Ex. 63. B.C. later sent an email to a Nosal Partners client, with Defendant's knowledge and consent, suggesting one of the candidates from this list. Gov. Ex. 64; 5 RT 968-70.

There was also evidence presented of the co-conspirator's efforts to keep their activities secret, from which the jury could have inferred that they knew the information they were obtaining was a trade secret:

- For at least some searches she ran, B.C. affirmatively checked a box that prevented Searcher from saving a custom report title, which was otherwise the default setting. 3 RT 614, 630-31.

- M.J. states that he took information from Searcher starting in mid-2004 – including candidate resumes, source lists, and experience lists – with the intention of bringing this information to Defendant's new business. 5 RT 1107-08. He stated that he did not tell anyone at KFI that he was taking this information, and that he did not want anyone to know. 5 RT 1109-10. He testified that Defendant set the tone for this atmosphere of secrecy in the first conversation he had with M.J. about the new business, telling M.J. to keep the plans for the new business secret. 5 RT 1110.

- J.F.L. testified that in conversations about taking information from KFI, Defendant had told her and B.C. to work out the details between themselves because he did not want to know about it. 6 RT 1284-86. He did not tell them not to take any KFI information. *Id.*

- On December 15, 2004, Defendant sent J.F.L. an email at her KFI email address indicating that he had secured a client for the new business. Gov. Ex. 50. The email also directed M.J. to take the lead on coordinating with the vendor for the new business' database. J.F.L. responded to him saying: "David, you sent this to me at my KF email. PLEASE be careful." *Id.*

- On April 27, 2005, J.F.L. emailed two documents to B.C. that contained position specifications she had obtained from KFI's computer system. 6 RT 1329-30. She named these two files "Chocolate Chip Cookie Recipes" and "Invitation to Marcy's Bridal Shower." *Id.*; Gov. Ex. 71. J.F.L. testified that

she sent these documents to B.C. at B.C.'s request, and that she gave the documents these names to disguise their true contents. 6 RT 1330.

- In June 2005, an individual using J.F.L.'s access credentials ran a search for human resources candidates meeting certain criteria. 3 RT 644-68; Gov. Ex. 31. This individual named the resulting custom report "choc chip." 3 RT 666. The person then created another custom report titled "CCC" and clicked a box to prevent the custom report from being saved. 3 RT 667. This information was downloaded to an Excel document with the title "choc chip cookie recipes." 3 RT 668. The resulting information was burned to a CD that was titled "choc chip cookies." 3 RT 669. After the information was burned to the CD, the user deleted the data from the Excel document saved on the computer, and instead saved a version of the document with the words "four cups of sugar, two cubes of butter" inserted. 3 RT 669.

Though Defendant presented an alternative explanation for this secretive behavior – that he and his co-conspirators were merely trying to avoid tipping off KFI that he was starting his own business in violation of what he contends was an illegal non-compete covenant – the jury could reasonably have concluded that these actions indicated the co-conspirators knew their actions to be criminal. Indeed, Defendant's argument that the non-compete covenant was illegal and unenforceable (discussed below) would seem to undermine the need for secrecy if that were the only reason: if Defendant was certain that the non-compete covenant was unenforceable, what need would he have to hide his activities?

The jury could have inferred that Defendant and his co-conspirators were aware of the trade secret status of the information in question since, at the time in question, they were all current or former KFI employees. Given Defendant's senior position and length of service with KFI, the jury could reasonably inferred his awareness that source lists and similar information drawn from Searcher were valuable trade secrets belonging to KFI. Similarly, B.C., M.J., and J.F.L. had all worked for KFI, and had used Searcher as part of their employment there. The jury could have inferred that they knew of Searcher's value through the use they had made of it, and were aware of the steps KFI took to keep the material secret because they had been exposed to various policies and restrictions on use during the course of their employment.

Indeed, the government produced evidence at trial that Defendant sought to use the source lists and to gain immediate financial benefit by obtaining them directly from KFI's computers rather

than employing his own work effort to derive his own lists. This evidence underscores the likelihood that he knew what he was obtaining was a trade secret.

Looking at this evidence as a whole, a reasonable jury could have concluded that the government had proved beyond a reasonable doubt that Defendant and his co-conspirators knew that the alleged trade secrets were in fact trade secrets. The Court therefore denies Defendant's motions on this ground.

4. Evidence Conspirators Knew or Believed that Taking Source Lists Would Harm KFI

Defendant argues that he is entitled to acquittal or a new trial because the government failed to introduce sufficient evidence that Defendant and his co-conspirators intended or knew that their actions would injure KFI, as is required by the EEA. 18 U.S.C. § 1832(a). The government did, however, present evidence from which the jury could conclude that Defendant and his co-conspirators knew that taking the source lists in the government's Exhibit 58 or the CFO information in the government's Exhibit 60 would injure KFI. In addition to the evidence discussed above about the value of the information found in Searcher and the derived source lists, the government introduced the following evidence, indicating the value of Searcher, the co-conspirator's awareness of this value, and the fact that KFI could be harmed if information from Searcher fell into the hands of a competitor such as Defendant:

- Nahas testified that the executive search industry is highly competitive. 2 RT 290-92. KFI would put a lot of work and research into attempting to solicit clients. *Id.*
- B.C. similarly testified that in order to solicit clients in a competitive bidding process, it was important to have a lot of information about the company, what it was looking for, and potential candidates. 4 RT 889-91.
- M.J. testified that the executive search industry was competitive, and that information was valuable for soliciting and retaining clients. 6 RT 1200-01.
- Nahas testified that if a KFI competitor had access to one of KFI's source lists on a relevant search, this could give the competitor an advantage because they could obtain information that the would not otherwise have had access to. This would permit them to do a better search and possibly obtain business that they would otherwise have gotten. 2 RT 304-05. She described source lists as "the foundation and the springboard and the running start for an assignment." 2 RT 301.
- B.C. testified that KFI ordinarily wouldn't share information with Searcher with competitors because KFI competed with them for business. 5 RT 916-

> 17. Though she had given information from Searcher to friends outside KFI, she did not recall telling her bosses at KFI that she had done so. *Id.*

- M.J. testified that as a KFI employee, he would frequently return to old source lists, because they were helpful in conducting new searches. 5 RT 1095.

- B.C. testified that she would frequently look to source lists from previous similar searches when beginning a new search. 4 RT 893, 897-98. She testified that it was incredibly important to have the contact information contained in Searcher and the source lists, particularly private cell phone and email information for executives, because executives were more likely to respond and to be able to talk to the KFI employee privately. 4 RT 898-99

- B.C. testified that during her time working with Nosal at KFI, he would at times direct her to look at a source list from a prior search because he was interested in "leveraging names from prior searches in order to help expedite a current search that he was working on or a search that he wanted – that he was pitching for." 5 RT 920-21. She additionally testified that clients generally wanted searches conducted in an expedient manner. 4 RT 886. Conducting searches quickly made clients happy, and "opens the door to more searches." 5 RT 954.

- The Confidentiality Agreements Defendant and his co-conspirators signed described Searcher and the information contained therein as "extremely valuable assets" that were "accorded the legal protection applicable to a company's trade secrets." Gov. Ex. 7, 12, 14, 16.

Additionally, the fact that Defendant and his co-conspirators were starting a business that would *compete* with KFI supports an inference that they knew or intended that their actions would injure KFI. The above evidence suggests that Defendant and his co-conspirators were aware of the value of the information contained in Searcher, and sought it because of the advantage it would give them in conducting searches for the new business. Defendant presumably desired the new business to succeed, and given that the business was a direct competitor of KFI's, this could well result in securing clients who might otherwise have gone to KFI for their executive search needs. The Supreme Court has recognized that the owner of a trade secret is harmed when the trade secret is disclosed to competitors:

> Once the data that constitute a trade secret are disclosed to others, or others are allowed to use those data, the holder of the trade secret has lost his property interest in the data. . . . The economic value of that property right lies in the competitive advantage over others that [the trade secret owner] enjoys by virtue of its exclusive access to the data, and disclosure or use by others of the data would destroy that competitive edge.

Ruckelshaus, 467 U.S. at 1011-12; *see also id.* at 1011 n.15 ("We emphasize that the value of a trade secret lies in the competitive advantage it gives its owner over competitors."). While it is not clear that *Ruckelshaus*, which did not consider criminal charges for the theft or misappropriation of trade secrets, establishes that this prong of § 1832 is necessarily met when the defendant works for a competitor, the jury may properly have considered these circumstances as probative to the question of whether Defendant and his co-conspirators knew or intended that their actions would harm KFI.

The government additionally argues that even absent *knowledge* that an offense will injure the owner of the trade secrets, a jury can convict if the government proves beyond a reasonable doubt that the defendant *intended* to injure the owner. *See* 18 U.S.C. § 1832(a). At trial, the government introduced evidence that Defendant was angry with KFI because he had not secured a promotion he desired. 5 RT 928, 950-51. It further introduced evidence suggesting that he harbored resentment against KFI and wanted to make a statement around his departure. 5 RT 1067 (Defendant ghost wrote B.C.'s departure email from KFI "because he was interested in creating kind of a fireball effect from his departure"). From this, a jury could have inferred that Defendant intended to harm KFI.

Taken together, this evidence is sufficient for a reasonable jury to find that Defendant and his co-conspirators knew or intended that their actions in taking the source lists and related information would harm KFI. The Court therefore denies Defendant's motions on this ground.

D. Exclusion of Evidence and Argument Regarding Non-Compete Clause

Defendant argues that he is entitled to a new trial under Rule 33 on all counts because he was prejudiced by the Court's order precluding him from arguing that a non-compete provision in his independent contractor agreement with KFI was illegal under California law. Docket No. 437 at 19-30. In the pre-trial order, this Court granted in part Defendant's motion in limine on this issue, ruling that either party could introduce argument or evidence of a person's subjective beliefs about the validity of the non-compete provision where it was relevant to explain that individual's actions or for some other purpose. Docket No. 352 at 6-8. The Court precluded either party, however, from introducing evidence or argument as to whether the provision was *actually* legal and enforceable because this was irrelevant to the issues in this case. *Id.* at 7.

Furthermore, the Court prohibited the government from arguing that Defendant's breach of any non-compete agreement was probative to his motive or intent to defraud. Both at the beginning of the trial and at the close of evidence, the Court gave the jury the following instruction:

> You have heard testimony from some witnesses that Mr. Nosal entered into a noncompetition covenant with Korn/Ferry when he ceased to be an employee and became an independent contractor. Whether the agreement was legal and enforceable is not relevant to the issues in this case. To the extent that any of the witnesses offered opinions to whether the defendant's conduct was a breach of any covenant or agreement with Korn/Ferry, that opinion testimony must be disregarded as irrelevant to the issues you are to decide. Additionally, evidence that Mr. Nosal breached or did not breach this covenant is not relevant to the question of whether he is guilty of the crimes charged in this case.

Docket No. 375 at 20; Docket No. 401 at 23.

In the instant motion, Defendant renews his argument that the non-compete provision was unlawful, and that this fact was relevant to his defense. He further argues that even if the Court's ruling on this point was not in error, he was prejudiced by the way the government presented evidence on the non-compete provision because the government to introduced evidence suggesting that Defendant had acted dishonestly in violating the non-compete provision, and Defendant was not permitted to argue that this provision was unlawful. He argues, in the alternative, that the Court should have precluded all mention of the non-compete provision, as the parties' subjective beliefs about its validity were irrelevant to the charges in this case.

1. Relevance of Non-Compete Provision

Defendant offers no new argument that the legality of the non-compete covenant was relevant to any issue in this case. Defendant contends that "the covenant was relevant and exculpatory, as its illegality explained actions on the part of the defendant that otherwise appeared wrongfully deceitful," and that the KFI's efforts "to limit Nosal's establishment of a new search business by means of an illegal agreement under threat of denying him a huge balloon payment owed him was relevant to prove the innocence of his efforts to avoid detection of his non-KFI work." Docket No. 437 at 2, 20. To the degree that the relevance of the covenant was to explain Defendant's actions, however, what would be relevant is not the actual legality or illegality of the covenant, but Defendant's subjective belief regarding its legality or illegality. This is exactly what

the Court permitted in its pre-trial ruling. Defendant identifies no time at trial where he was prevented from presenting evidence about his beliefs regarding the legality of the contract.[9]

Further, as noted above, to the degree that Defendant believed the non-compete covenant to be unlawful and unenforceable, this provides no explanation as to why he felt the need to keep his actions secret (and so behaved). If Defendant had believed that portion of his agreement with KFI to be unenforceable, he would have little need to keep his actions in setting up a competing business secret. If KFI had attempted to stop him or otherwise enforce the covenant, he simply could have taken the matter to court and secured an order recognizing his right to set up his business without forfeiting the payments he was owed under the independent contractor agreement. Hence, Defendant's assertion of the illegality of the covenant, if anything, tends to undermine his claim that he acted secretly not because he knew he was taking trade secrets, but because of the non-compete covenant.

Defendant argues in the alternative that given the ruling excluding evidence of the non-compete provision's legality or illegality, this Court erred in allowing the government to present evidence and argument about the non-compete covenant at all. He argues: "Having ruled instead that the noncompetition covenants were flatly irrelevant to Nosal's guilt of the charges, the Court provided no persuasive rationale why evidence of those provisions or the parties' beliefs concerning the matter was relevant to the jury's consideration of the charges." Docket No. 437 at 31.

As this Court previously found, information about the non-compete covenant, and KFI's belief that Defendant was in violation of the covenant, is relevant to explain why KFI began its investigation into the activities of Defendant and his co-conspirators. Docket No. 352 at 6-8. In this case, Defendant has argued that KFI had initiated its investigation and cooperated with the

---

[9] Defendant also renews his argument that the non-compete covenant was illegal under California law, and additionally brings the new argument that his agreements with KFI were illegal because they erroneously classified him as an independent contractor rather than an employee. Docket No. 437 at 27-30. As he offers no reason why the legality of the non-compete covenant is relevant to the issues in this case, however, these arguments are irrelevant. Further, the newly raised argument seems to actually undercut Defendant's position that the non-compete covenant was illegal, as there are cases suggesting that an employer may restrict a current employee's ability to compete. *See Fowler v. Varian Associates, Inc.*, 196 Cal. App. 3d 34, 41, 241 Cal. Rptr. 539 (Ct. App. 1987) ("During the term of employment, an employer is entitled to its employees' undivided loyalty.") (internal citation omitted).

prosecution out of improper motive, such as a desire to avoid paying him funds he was owed under the independent contractor agreement. *See, e.g.*, Docket No. 313 at 4 ("The reason [that KFI did not confront Defendant about B.C. and M.J.'s access to Searcher] became apparent some months later, when KF refused to pay Nosal the more than a million dollars it owed him for past work on the ground that he had violated an agreement not to perform independent searches while working as a KF contractor."). Defendant's cross-examination of some of the government's witnesses attempted to question their motives and thus impeach their credibility on this front. 2 RT 334-36 (cross-examination of Nahas included questions about KFI's financial interest in parallel civil litigation); 2 RT 496-98 (cross-examination of Dunn included questions about KFI's desire to have the federal government initiate criminal proceedings against Defendant and his co-conspirators before the balloon payment under the independent contractor agreement came due, and questions about the civil litigation). Further, in his closing argument, Defendant argued that this case was not actually about violations of the CFAA or the EEA, but that it was

> just an effort by Korn/Ferry to eliminate David Nosal as a competitor; and it's an effort by Korn/Ferry to avoid paying him the money that they owed, and to try to, by whatever means possible, win their $27 million lawsuit against Mr. Nosal.

8 RT 1665. In this context, the Court found it appropriate to allow the government to introduce evidence of the non-compete covenant and the Sandra Horn email to counter the argument that KFI had initiated its investigation into Defendant out of animus or improper motive. Nothing Defendant points to in his Rule 33 motion convinces the Court that this ruling was an error.

Defendant cites various cases in support of his argument that allowing evidence on various individuals' beliefs about the non-compete covenant was an error, but these cases are not on point. Docket No. 448 at 37-38. The cases and treatises he cites concern the appropriateness of allowing otherwise inadmissible hearsay evidence to show state of mind or to provide context for admissible evidence. *See* 2 McCormick On Evid. § 249 (7th ed.); Hearsay Handbook 4th § 2:10; *United States v. Dean*, 980 F.2d 1286, 1288 (9th Cir. 1992) (finding hearsay statement that was relevant to show why an officer was present at a certain location were not admissible where the officer's reason for being at that location were not relevant to any issue in the case); *United States v. Makhlouta*, 790

F.2d 1400, 1402 (9th Cir. 1986) (hearsay statement offered to show FBI agent's state of mind should have been excluded where agent's state of mind was not relevant to defense of entrapment); *United States v. Walker*, 673 F.3d 649, 657 (7th Cir. 2012). None of these cases address the use of evidence to provide context as discussed above.

Defendant does not object to the evidence about the non-compete covenant on the hearsay grounds (with perhaps the exception of evidence about the "Sandra Horn" email). Hence, the authorization he cites are inapposite. Further, to the extent that Defendant does raise hearsay objections, the Ninth Circuit has noted that hearsay evidence about a tip that lead to an investigation may be admissible to explain the origin and course of an investigation. *United States v. Noriega-Lopez*, 47 F.3d 1177 (9th Cir. 1995) ("Here, the testimony about the tip was not hearsay to the extent that it showed how the investigation began and why the agents went to certain locations."); *United States v. Cawley*, 630 F.2d 1345, 1350 (9th Cir. 1980) ("However, with a proper instruction, the court may admit such evidence of tips as was admitted here to explain why an officer conducted an investigation as he did.").

As Defendant offers no convincing argument that this Court's rulings on the admissibility of evidence and argument regarding the non-compete covenant was in error, this Court rejects Defendant's motion for a new trial on these grounds.

2. Prejudice from Evidence Presented and Excluded at Trial

Even if this Court's rulings on the admissibility of evidence and argument regarding the non-compete covenant was not an error, Defendant argues that he was unfairly prejudiced by the way the government actually presented such evidence and argument at trial. He points to several points in the trial that he contends were prejudicial:

- The testimony of KFI general counsel Peter Dunn, in which he discussed the terms of the non-compete covenant, 2 RT 387-90, and stated that KFI had not paid Defendant the full amount of money identified in the independent contractor agreement because KFI believed that Defendant had breached the agreement, 2 RT 443-444.[10] On cross-examination, Defendant elicited from Dunn the fact that Defendant contended in the civil suit between the parties that the non-compete covenant was "void and illegal." 2 RT 465. The Court

[10] Dunn did not identify the actions Defendant took that KFI believed to be a breach of the agreement on direct examination.

permitted this testimony over the government's objection. The Court sustained, however, the government's objection to Defendant's question when counsel asked Dunn whether non-compete covenants were not illegal in some states. 2 RT 465-66.[11]

- The introduction of an email from a "Sandra Horn," in which she stated that Defendant was conducting searches for KFI clients, and suggesting that KFI could "save a few dollars on your agreement with him," or that they may wish to sue, but stating that if KFI did not do anything to stop him, they would "look like chumps." Gov. Ex. 20. Defendant also objects to Dunn's testimony regarding same. 2 RT 421-30. Dunn testified that after getting the email from Horn, he began an investigation to determine whether Defendant was breaching the non-compete covenant. 2 RT 426-27.

- The testimony of B.C. that Defendant had a non-solicitation [sic] agreement with KFI, and that he did not comply with this agreement, 5 RT 940-41, that Defendant had her set up an executive search business in her name through which he worked, *id.*, and that Defendant used an alias during some interactions with clients, which B.C. understood to be because he did not want people to know he was conducting search work in breach of his agreement with KFI. 5 RT at 952-53. Defendant did not object to these portions of B.C.'s testimony at trial.

- The testimony of M.J., in which he testified to his understanding of the terms of the non-compete covenant. 5 RT 1099. Defendant did not object to this testimony at trial.

- The rebuttal portion of the government's closing argument, which suggested that the only explanation for Defendant's secretive behavior was that he was engaging in criminal activity. 8 RT 1689-90.

In addition to the limiting instruction identified above, the Court took the following steps to limit any potential prejudice from this evidence:

- During Dunn's testimony regarding the terms of the non-compete covenant, at Defendant's request, the Court made the following statement to the jury: "I've already instructed the jury that a provision, which I think we referred to as a noncompetition clause, the validity or enforceability of that is not an issue in this case for you to decide." 2 RT at 389. Defendant did not renew his objection after the Court gave this statement.

- When the government introduced the Sandra Horn email during Dunn's testimony, the Court admonished the jury as follows at Defendant's request: "Ladies and gentlemen, I'm going to admit Exhibit Number 20 into evidence. But I need to explain to you that this exhibit is admitted for the purpose of

---

[11] Defendant also objects to the portion of Dunn's testimony in which he stated that KFI had secured a preliminary injunction in a civil case against Defendant. Docket N. 437 at 24. According to Dunn's testimony, however, this preliminary injunction was aimed at preventing Defendant from disseminating certain information belonging to KFI, but did not restrain him from competing against KFI. 2 RT 439-440. It is thus unclear how this testimony would prejudice Defendant relative to the issue of the non-compete covenant.

> giving you some understanding as to the witness's knowledge and, perhaps, intent, but not to prove the truth of the matters that are stated in this email." 2 RT 423.

Taken together with evidence Defendant elicited on cross examination and this Court's limiting instructions, it cannot be said that the government's evidence and argument related to the non-compete covenant was so unfairly prejudicial as to require a new trial. The Court therefore denies Defendant's Rule 33 motion on this ground.

IV. CONCLUSION

For the foregoing reasons, this Court finds that Defendant has established neither that he is entitled to a judgment of acquittal under Rule 29, nor that a new trial is required in the interests of justice pursuant to Rule 33. Defendant's motion for a new trial and motion for acquittal are **DENIED.** The Rule 29 motion Defendant made at the close of evidence in this case is likewise **DENIED.**

This order disposes of Docket Nos. 397, 436, and 437.

IT IS SO ORDERED.

Dated: August 15, 2013

EDWARD M. CHEN
United States District Judge