

Nos. 14-10037 & 14-10275

IN THE UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID NOSAL,

Defendant-Appellant.

---

**BRIEF FOR THE UNITED STATES AS APPELLEE**

APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
DISTRICT COURT NO. 08-CR-00237 EMC

---

**MELINDA HAAG**  
United States Attorney

**BARBARA J. VALLIERE**  
Assistant United States Attorney  
Chief, Appellate Division

**KYLE F. WALDINGER**  
**MATTHEW A. PARRELLA**  
Assistant United States Attorneys  
450 Golden Gate Avenue, 11th Floor  
San Francisco, CA 94102

**LESLIE R. CALDWELL**  
Assistant Attorney General

**SUNG-HEE SUH**  
Deputy Assistant Attorney General

**JENNY C. ELLICKSON**  
Trial Attorney  
Criminal Division, Appellate Section  
U.S. Department of Justice  
950 Pennsylvania Ave. NW, Rm. 1264  
Washington, DC 20530  
Telephone: (202) 305-1674

**Attorneys for Plaintiff-Appellee**  
**UNITED STATES OF AMERICA**

**TABLE OF CONTENTS**

TABLE OF AUTHORITIES ..... vi

JURISDICTION, TIMELINESS, AND BAIL STATUS.....1

ISSUES PRESENTED.....2

STATEMENT OF THE CASE.....2

    A. Overview .....3

    B. Korn/Ferry .....4

        1. Korn/Ferry’s executive-search work .....4

        2. Searcher .....6

        3. Korn/Ferry’s computer system .....8

        4. Additional Korn/Ferry confidentiality measures.....9

    C. The Conspiracy.....10

        1. Nosal decides to leave Korn/Ferry .....10

        2. Nosal decides to start a competing business.....11

        3. Nosal does executive-search work through  
            Christian & Associates .....13

        4. Nosal sets up Nosal Partners .....15

    D. Christian and Jacobson Access Korn/Ferry’s Computers and  
        Take Information.....15

        1. April 12, 2005 .....16

        2. July 12, 2005.....19

- 3. July 29, 2005.....20
- SUMMARY OF ARGUMENT .....20
- ARGUMENT .....24
- I. SUFFICIENT EVIDENCE SUPPORTED NOSAL’S  
CONVICTIONS.....24
- A. Standard Of Review .....24
- B. Nosal Is Guilty Of Computer Fraud .....24
- 1. Procedural background .....25
- 2. The evidence established that Christian and  
Jacobson accessed Korn/Ferry’s computers “without  
authorization” .....26
- a. Christian and Jacobson acted “without  
authorization” when they accessed Korn/Ferry  
computers after Korn/Ferry terminated their  
access privileges .....27
- b. Froehlich-L’Heureaux did not and could not  
unilaterally override Korn/Ferry’s decision to  
terminate Christian’s and Jacobson’s authority  
to access its computers .....29
- c. Section 1030 does not require the government  
to prove “the circumvention of technological  
access barriers,” and in any event,  
the government made this showing .....32
- d. Nosal did not have authorization to access  
Korn/Ferry computers during the relevant  
period.....34

- 3. Nosal was liable for Christian’s and Jacobson’s conduct both under *Pinkerton* and as an aider and abettor .....35
- C. Nosal Is Guilty Of The Trade-Secrets Offenses Charged In Counts Five And Six .....38
  - 1. The relevant source lists were trade secrets .....39
    - a. Korn/Ferry took reasonable measures to keep the source lists secret.....40
    - b. The source lists derived economic value from not being generally known to, and not being readily ascertainable through proper means by, the public .....43
  - 2. Nosal and Christian knew that the source lists were trade secrets .....46
  - 3. Nosal and Christian knew or intended that their conduct would injure Korn/Ferry .....47
- II. THE DISTRICT COURT DID NOT ERR OR PLAINLY ERR IN FORMULATING THE JURY INSTRUCTIONS .....48
  - A. Standard Of Review .....48
  - B. The “Without Authorization” Jury Instruction Was Correct.....49
    - 1. Background.....49
    - 2. The district court properly modeled its “without authorization” instruction on *Brekka*.....50
  - C. The Aiding-And-Abetting And Deliberate-Ignorance Instructions Were Correct .....52
    - 1. Background.....52

- 2. The district court’s instructions were consistent with *Rosemond*, and in any event, Nosal cannot satisfy the plain-error standard.....54
- 3. The district court did not plainly err in including Froehlich-L’Heureaux’s name in the deliberate-ignorance instruction .....57
- D. The Trade-Secrets Conspiracy Instruction Was Correct .....59
  - 1. Background.....59
  - 2. The district court properly instructed the jury that it could find Nosal guilty of trade-secrets conspiracy even if the government did not prove the existence of a trade secret.....60
  - 3. The trade-secrets conspiracy instruction did not constructively amend the indictment.....62
- III. THE DISTRICT COURT’S EVIDENTIARY RULINGS ABOUT THE NONCOMPETE PROVISIONS WERE PROPER.....64
  - A. Background .....64
  - B. Standard Of Review .....67
  - C. The District Court’s Evidentiary Rulings Were Proper.....68
- IV. THE DISTRICT COURT’S RESTITUTION ORDER WAS PROPER.....70
  - A. Background .....70
  - B. Standard Of Review .....72
  - C. The District Court Properly Concluded That A Restitution Award May Be Greater Than The Loss Calculation Under USSG § 2B1.1.....72

D. The District Court Properly Ordered Nosal To Reimburse  
Korn/Ferry For Some Of Its Attorneys' Fees .....74

CONCLUSION.....76

STATEMENT OF RELATED CASES .....77

CERTIFICATE OF COMPLIANCE.....78

CERTIFICATE OF SERVICE .....79

ADDENDUM .....80

**TABLE OF AUTHORITIES**

FEDERAL CASES

*LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) ..... *passim*

*Nationwide Mut. Ins. Co. v. Mortensen*, 606 F.3d 22 (2d Cir. 2010).....45

*Penalty Kick Management Ltd. v. Coca Cola Co.*, 318 F.3d 1284  
(11th Cir. 2003).....45

*Pinkerton v. United States*, 328 U.S. 640 (1946)..... 20, 25, 35, 57, 59

*Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042  
(10th Cir. 1994).....45

*Rosemond v. United States*, 134 S. Ct. 1240 (2014)..... 36, 54

*Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) .....34

*United States v. Anderson*, 741 F.3d 938 (9th Cir. 2013)..... 49, 50, 56, 58

*United States v. Awad*, 551 F.3d 930 (9th Cir. 2009).....48

*United States v. Bingham*, 653 F.3d 983 (9th Cir. 2011).....35

*United States v. Del Toro-Barboza*, 673 F.3d 1136 (9th Cir. 2012) .....55

*United States v. Everett*, 692 F.2d 596 (9th Cir. 1982) .....61

*United States v. Fiander*, 547 F.3d 1036 (9th Cir. 2008) .....60

*United States v. Garcia*, 768 F.3d 822 (9th Cir. 2014).....48

*United States v. Gordon*, 393 F.3d 1044 (9th Cir. 2004)..... 73, 74, 75

*United States v. Heredia*, 483 F.3d 913 (9th Cir. 2007) (en banc).....56

*United States v. Howley*, 707 F.3d 575 (6th Cir. 2013).....40

*United States v. Hsiung*, No. 12-10492, 2015 WL 400550  
(9th Cir. Jan. 30, 2015) .....36

*United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998)..... 61, 62

*United States v. Kahre*, 737 F.3d 554 (9th Cir. 2013) .....68

*United States v. Kessi*, 868 F.2d 1097 (9th Cir. 1989) ..... 55, 57

*United States v. Liu*, 716 F.3d 159 (5th Cir. 2013).....62

*United States v. Luis*, 765 F.3d 1061 (9th Cir. 2014) .....72

*United States v. Lukashov*, 694 F.3d 1107 (9th Cir. 2012).....67

*United States v. Mancuso*, 718 F.3d 780 (9th Cir. 2013) .....49

*United States v. Marcus*, 560 U.S. 258 (2010) .....57

*United States v. Martin*, 228 F.3d 1 (1st Cir. 2000) ..... 61, 62

*United States v. Miller*, 471 U.S. 130 (1985) .....63

*United States v. Nevils*, 598 F.3d 1158 (9th Cir. 2010) (en banc).....24

*United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc)..... 25, 28, 31, 33

*United States v. Padilla*, 639 F.3d 892 (9th Cir. 2011) ..... 68, 69

*United States v. Rodriguez*, 360 F.3d 949 (9th Cir. 2004).....61

*United States v. Stoddard*, 150 F.3d 1140 (9th Cir. 1998) ..... 73, 74

*United States v. Thum*, 749 F.3d 1143 (9th Cir. 2014).....36

*United States v. Torres-Flores*, 502 F.3d 885 (9th Cir. 2007) .....47

*United States v. Ward*, 747 F.3d 1184 (9th Cir. 2014) .....63

*United States v. Wilbur*, 674 F.3d 1160 (9th Cir. 2012)..... 62, 63



*United States v. Wright*, 625 F.3d 583 (9th Cir. 2010).....24

*United States v. Yang*, 281 F.3d 534 (6th Cir. 2002)..... 61, 62

FEDERAL STATUTES, RULES, AND GUIDELINES

18 U.S.C. § 2.....2, 3

18 U.S.C. § 371.....2, 59

18 U.S.C. § 1030..... *passim*

18 U.S.C. § 1832..... *passim*

18 U.S.C. § 1839(3) ..... 39, 40, 43, 45

18 U.S.C. § 3231 .....1

18 U.S.C. § 3663.....74

18 U.S.C. § 3663A..... 72, 74, 75

18 U.S.C. § 3742(a) .....2

28 U.S.C. § 1291 .....2

Fed. R. Evid. 402 .....69

Fed. R. Evid. 403 ..... 64, 69

Fed. R. Evid. 404(b).....64

USSG § 2B1.1..... 23, 70, 72, 73

OTHER AUTHORITIES

H.R. Rep. No. 104-788, at 7 (1996), *reprinted in*  
 1996 U.S.C.C.A.N. 4021, 4026 ..... 40, 47

Nos. 14-10037 & 14-10275

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID NOSAL,

Defendant-Appellant.

---

**BRIEF FOR THE UNITED STATES AS APPELLEE**

---

Following a jury trial, defendant-appellant David Nosal was convicted of conspiracy, computer fraud, and trade-secrets offenses based on his participation in a conspiracy to download trade secrets and other proprietary information from the computers of his former employer. Nosal now appeals his convictions, challenging the sufficiency of the evidence, the jury instructions, and certain evidentiary rulings. Nosal also asks the Court to vacate the district court's restitution order. This Court should affirm.

**JURISDICTION, TIMELINESS, AND BAIL STATUS**

The district court had jurisdiction under 18 U.S.C. § 3231. On January 14, 2014, Nosal filed a timely notice of appeal from the judgment announced on

January 8, 2014, and entered January 21, 2014. Clerk's Record ("CR"):502; Excerpts of Record ("ER"):176-85. On June 5, 2014, Nosal filed a timely notice of appeal of the amended judgment entered May 30, 2014. ER:167-75. This Court has jurisdiction pursuant to 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a). Nosal is on bail pending appeal. CR:523.

### **ISSUES PRESENTED**

- I. Whether sufficient evidence supported Nosal's convictions for computer fraud and trade-secrets offenses.
- II. Whether the district court erred or plainly erred in formulating the jury instructions.
- III. Whether the district court acted within its discretion in admitting and excluding certain evidence relating to Nosal's noncompete agreement with his former employer.
- IV. Whether the restitution order was proper.

### **STATEMENT OF THE CASE**

Following a two-week jury trial in the United States District Court for the Northern District of California, Nosal was convicted on all counts of a second superseding indictment charging him with conspiracy, in violation of 18 U.S.C. § 371 (Count One); computer fraud, in violation of 18 U.S.C. §§ 1030(a)(4) and 2 (Counts Two through Four); unauthorized downloading, copying, and duplicating

of trade secrets, in violation of 18 U.S.C. §§ 1832(a)(2), 1832(a)(4), and 2 (Count Five); and unauthorized receipt and possession of stolen trade secrets, in violation of 18 U.S.C. §§ 1832(a)(3), 1832(a)(4), and 2 (Count Six). ER:1167-78; CR:406. The district court sentenced Nosal to 12 months and one day in prison, three years of supervised release, a \$60,000 fine, and a \$600 special assessment. ER:180-84. In an amended judgment, the district court ordered Nosal to pay \$827,983.25 in restitution to Korn/Ferry International. ER:169-75.

#### **A. Overview**

In 2004, Nosal was a regional director at Korn/Ferry International (“Korn/Ferry”), the largest executive-search firm in the world. Korn/Ferry’s primary business is identifying, assessing, and recommending potential candidates for top-level executive positions with Korn/Ferry’s corporate clients. When conducting an executive search for a particular client, Korn/Ferry develops a “source list” of potential candidates who meet that client’s needs. Korn/Ferry stores these source lists in Searcher, a proprietary database on Korn/Ferry’s password-protected computer system.

In mid-2004, Nosal resolved to leave Korn/Ferry and start a competing executive-search business. He recruited several Korn/Ferry employees to join him in this endeavor, including Becky Christian, Mark Jacobson, and Jacqueline Froehlich-L’Heureaux, and instructed them to take materials from Korn/Ferry’s

computer systems to help his new business. By April 2005, Nosal, Christian, and Jacobson had each left their jobs at Korn/Ferry and had begun conducting their own executive-search work with assistance from Froehlich-L'Heureaux, who was still employed by Korn/Ferry. On April 12 and July 12, 2005, Christian used Froehlich-L'Heureaux's Korn/Ferry password to log into Korn/Ferry's computer system and obtain source lists and information that were relevant to Nosal's executive-search work. Later, on July 29, 2005, Jacobson used Froehlich-L'Heureaux's Korn/Ferry computer account to obtain more source lists from Searcher.

**B. Korn/Ferry**

Korn/Ferry is an executive-search firm that performs headhunting services for its clients. ER:842-43. Korn/Ferry's clients are organizations and companies that hire Korn/Ferry to identify, assess, and recommend senior executives for top-level positions, such as chief executive officers, chief financial officers, and chief marketing officers. ER:842, 845. Korn/Ferry has approximately 600 partners and 3000 employees, and its annual revenue is approximately \$800 million. ER:843. It is the largest executive-search firm in the world. ER:843, 845.

*1. Korn/Ferry's executive-search work*

When a client company hires Korn/Ferry, a Korn/Ferry team creates a "source list" of potential candidates for the client's open position. ER:851, 854.

The source list includes each candidate's name, title, company, email address, and telephone numbers, which may include the candidate's work, home, and cell-phone numbers. ER:879-80. Much of the personal contact information in the source lists is not public, and it is "incredibly important" to Korn/Ferry's work because it increases Korn/Ferry's chances of contacting the executive. ER:316-17, 682, 880. For example, an executive is more likely to answer his cell phone than his work phone, and a cell phone provides a more private means of communicating with an executive who may not want his current employer to know that he is considering a new job. ER:682-83.

To generate a source list for a new executive-search assignment, a Korn/Ferry team searches through past Korn/Ferry source lists for similar executive positions in related industries. ER:681-82, 855-56, 870-71. The Korn/Ferry team then reviews the candidates from the past source lists and makes judgments about whom to add to the new source list. ER:855-56, 870-71. The team may also augment that information by asking Korn/Ferry's research department to collect data about executives at particular companies. ER:871. By the end of this process, the new source list may contain 200 or more potential executive candidates. ER:857-58.

Once the Korn/Ferry team has assembled a source list for a particular engagement, the team spends a "significant amount of time" calling potential

candidates from the list to determine whether they are qualified and interested in the job. ER:317-18, 858. Korn/Ferry then presents a smaller group of candidates' resumes to the client, along with any assessments that Korn/Ferry has generated based on meeting the candidates. ER:858. Korn/Ferry rarely sends the source list itself to the client. ER:858-59. Korn/Ferry considers its source lists confidential and does not allow its employees to send them outside the company. ER:856. If a Korn/Ferry competitor obtained a source list, the source list would give the competitor a potential advantage over Korn/Ferry. ER:862-63.

Because executive search is a competitive industry, a potential client will sometimes ask several firms to "pitch" a particular executive-search assignment before the client decides which firm to hire. ER:848-49. A Korn/Ferry team prepares for a pitch by reviewing source lists for similar assignments that Korn/Ferry has completed in the past and by researching the client and its industry. ER:677, 849. At the pitch meeting, the Korn/Ferry team might provide the potential client with sample candidates to show the client the types of people Korn/Ferry envisions for the position, emphasizing that information about sample candidates is confidential. ER:850.

## 2. *Searcher*

In 1995, Korn/Ferry created Searcher, a proprietary computer program and database of past source lists and potential executive candidates. ER:710-11, 851-

52. Searcher was on Korn/Ferry's internal computer network, and only Korn/Ferry employees were authorized to access it. ER:852-53, 862. The computers that stored Searcher's North American database were located at a guarded data center in Burbank, California, to which only two or three Korn/Ferry employees had physical access. ER:716.

Searcher contained the source lists that Korn/Ferry had compiled since 1995, some pre-1995 source lists, and other documents. ER:719-20, 859-62, 898-99. As of 2004 and 2005, Searcher also contained information about approximately one million executives, and Korn/Ferry employees used Searcher on a daily basis. ER:709, 721. Korn/Ferry employees could use Searcher to create "custom reports" containing only the fields of information that the employees wanted to see. ER:731-32. When a computer user accessed Searcher's custom-report feature, a pop-up window displayed a message that stated in part, "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." ER:743; SER:250.

Searcher was Korn/Ferry's "nerve center" and "core asset," and Korn/Ferry spent \$5 million to \$15 million per year to maintain and improve Searcher. ER:852, 909. When Korn/Ferry provided clients with information that came from Searcher, Korn/Ferry designated the information as confidential and for the client's use only. ER:1007.



3. *Korn/Ferry's computer system*

During the relevant period, Korn/Ferry had a computer system that gave Korn/Ferry employees access to Searcher and other Korn/Ferry resources. ER:689-90. Korn/Ferry deployed firewalls and anti-virus software to protect its computer system, and a computer user could gain access to the system only by entering an authorized username and password. ER:700, 717-18. Every time a computer user attempted to log into Korn/Ferry's computer system, a pop-up window titled "Korn/Ferry Legal Notification" appeared on the screen. ER:698-99; Supplemental Excerpts of Record ("SER"):260, 263. This window displayed a message that stated in part, "This computer system and the information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry information system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution." ER:698-99; SER:260, 263.

Korn/Ferry issued its employees unique usernames for the computer system, and the employees created corresponding passwords, which Korn/Ferry required them to change every 60 days. SER:232; ER:700. Korn/Ferry prohibited its employees from sharing their passwords or computer accounts with anyone. SER:232-33, 235, 237. When an employee left Korn/Ferry's employment, Korn/Ferry terminated that employee's computer-user credentials. ER:703-04.

4. *Additional Korn/Ferry confidentiality measures*

Korn/Ferry required all employees and contractors to sign confidentiality agreements promising to protect Korn/Ferry's confidential information, including Korn/Ferry source lists. ER:934-35; SER:274-75. In these agreements, Korn/Ferry employees and contractors pledged: (1) to keep source lists private and use them only in connection with their Korn/Ferry work; (2) not to disclose, use, or copy source lists except as required by their Korn/Ferry work; (3) to prevent others outside Korn/Ferry from improperly gaining access to source lists; (4) to immediately notify Korn/Ferry if they suspected that anyone was inappropriately using or disclosing source lists; and (5) to return all source lists to Korn/Ferry upon leaving their employment. SER:274. The agreement further informed Korn/Ferry's employees and contractors that the company's "information databases and company records are extremely valuable assets" that "are accorded the legal protection applicable to a company's trade secrets." SER:274.

Korn/Ferry also required its employees to sign a Code of Business Conduct. ER:936-39; SER:264-73. This Code instructed employees to "refrain from disclosing information on proprietary hardware and software programs developed to facilitate servicing K/FI clients." SER:269. The Code further provided that employees should "[a]ssure the safekeeping" of Korn/Ferry documents and files and "refrain from removing said documents or files upon termination of

employment.” SER:269.

### **C. The Conspiracy**

#### *1. Nosal decides to leave Korn/Ferry*

Nosal began working at Korn/Ferry in 1996, and by 2004, he was a regional director at the firm and oversaw its activities in San Francisco, Chicago, and Seattle. ER:844-45, 910. He wanted to be promoted to President of North America for Korn/Ferry, but in early to mid-2004, Korn/Ferry hired an outside candidate instead. ER:330-31. Nosal was “furious” about being passed over and “very angry” at Korn/Ferry management for leading him to believe that he would get the position. ER:330-33.

In mid-2004, Nosal announced that he wanted to leave Korn/Ferry. ER:941. He and Korn/Ferry negotiated a separation agreement and an independent-contractor agreement, which collectively provided that he would work as an independent contractor for Korn/Ferry from October 31, 2004, until October 15, 2005, in exchange for a \$25,000 monthly stipend and a bonus. ER:943-44, 1121-22. The agreements provided that, as an independent contractor, Nosal would work to complete his outstanding Korn/Ferry assignments. ER:948, 1135. Paragraph 7 of each agreement (the “noncompete provisions”) provided that, for the duration of his independent-contractor term, Nosal would not engage in search activities that competed with Korn/Ferry. ER:1123-24, 1136-37. When Nosal

later discussed these agreements, he said that Korn/Ferry was paying him “a lot of money” to “stay out of the market.” ER:353.

2. *Nosal decides to start a competing business*

When Nosal decided to leave Korn/Ferry, he had been romantically involved with Becky Christian, then a Korn/Ferry partner, since approximately 2000, and they spoke daily. ER:325-28, 669. Christian kept Nosal up-to-date on her work activities, and Nosal and Christian brainstormed about which source lists to review for their executive-search projects. ER:327-28. Nosal also relied on Christian to obtain information for him from Korn/Ferry’s computer system on a daily basis. ER:323. By contrast, Nosal’s executive assistant Jacqueline Froehlich-L’Heureaux, who had worked for Nosal since 1998, did not know how to use Searcher to generate custom reports or retrieve source lists, and she never performed these tasks for Nosal or anyone else. SER:98-102.

After Nosal decided to leave Korn/Ferry, he began to talk about starting his own business. ER:332. His confidants included Christian, Froehlich-L’Heureaux, and Korn/Ferry senior associate Mark Jacobson.<sup>1</sup> ER:333-34, 492. Nosal held

---

<sup>1</sup> Nosal, Christian, Froehlich-L’Heureaux, and Jacobson had each signed Korn/Ferry’s confidentiality agreement and Code of Business Conduct. ER:913-39; SER:274-75. When Korn/Ferry hired Froehlich-L’Heureaux, Nosal sent her an offer letter instructing her to review and acknowledge both documents and informing her that her employment was contingent on her abiding with their provisions. ER:926-28; SER:278-80. Christian, Froehlich-L’Heureaux, and Jacobson all testified against Nosal at trial.

meetings in his Korn/Ferry office with Christian, Froehlich-L'Heureaux, and Jacobson, during which he directed them to obtain source lists and other information from Korn/Ferry's computers to help his new business. ER:333-35, 494-96.

During one of these meetings, Christian made a comment to Froehlich-L'Heureaux and Nosal about taking information from Korn/Ferry, and Nosal responded, "Don't talk about this in front of me. I don't want to hear it. Talk about it among yourselves." ER:298. When the topic arose again a few weeks later, Nosal again told Christian and Froehlich-L'Heureaux that they should "figure it out" themselves because he did not want to be part of the discussion. ER:298. However, when Froehlich-L'Heureaux later asked Nosal and Christian what she should do with candidate resumes that she had been copying off of Korn/Ferry's computers, Nosal gave her his credit card and told her, "Figure it out. Do whatever you think is best." ER:299. Froehlich-L'Heureaux then used his credit card to purchase zip drives for her and Christian. ER:300.

In October 2004, Nosal left his employment with Korn/Ferry and began his year-long term as an independent contractor. ER:1120-21. In December 2004, Nosal purchased Encore, a commercial database system from the software vendor Cluen that was similar to Searcher but contained no information. ER:339, 755. He emailed Christian, Jacobson, Froehlich-L'Heureaux, and others about the Encore

contract, telling them, “By god I think I am going to pee in my pants. We ARE in business!!!!” SER:286.

After he left his job at Korn/Ferry, Nosal pressured Christian to leave Korn/Ferry as well, which Christian did in January 2005. ER:338, 706. Before she left, however, Nosal asked her to take various source lists from Korn/Ferry’s computer system because he wanted to use them to populate his own executive-search database. ER:338-39. Accordingly, in late 2004 and early 2005, Christian generated numerous source-list custom reports that contained information about approximately 3500 executives. ER:762-67; SER:284-85. Nosal later asked Christian to give him these materials for his new database (*i.e.*, the Encore database he had purchased from Cluen). ER:351-52. Before Jacobson left his job at Korn/Ferry in early March 2005, he also took source lists and other items from Korn/Ferry’s computer system to help build Nosal’s new business. SER:62-63.

3. *Nosal does executive-search work through Christian & Associates*

At Nosal’s instruction, Christian set up a limited-liability company named Christian & Associates. ER:343. Nosal and Christian agreed that he would receive 80 percent of the fees that Christian & Associates earned, and Christian would receive 20 percent. ER:343. Christian billed the clients with Froehlich-L’Heureaux’s help and then wrote checks to Nosal for his share of the fees. ER:343-47. When Nosal interviewed potential executive candidates for his

Christian & Associates clients, he used the name “David Nelson” because he did not want people to know that he was conducting search work in violation of his agreements with Korn/Ferry. ER:354-55. Because Froehlich-L’Heureaux was still working at Korn/Ferry, Nosal asked her to use the name “Shelly Sparks” when she dealt with clients and candidates for Christian & Associates. ER:355; SER:110.

With Christian’s help, Nosal conducted “a significant amount” of executive-search work through Christian & Associates during the first half of 2005. ER:344. In performing this work, Nosal and Christian sometimes worked out of Christian’s apartment, and they used the materials Christian had taken from Korn/Ferry.

ER:328, 351. In addition, Christian sometimes called Froehlich-L’Heureaux and asked her to retrieve phone numbers from Searcher. SER:116. On one occasion, Nosal was on the call when Christian made this request, and he told Froehlich-L’Heureaux, “What are we going to do when you leave Korn/Ferry?” SER:117.

On April 12 and July 12, 2005, Christian used Froehlich-L’Heureaux’s Korn/Ferry password to access Korn/Ferry’s computer system and obtain additional source lists and information from Korn/Ferry. *See* Statement of Facts D.1-2, *infra*. Nosal knew that Christian was using Froehlich-L’Heureaux’s password to get these materials. ER:484.

4. *Nosal sets up Nosal Partners*

In mid-2005, Nosal rented and began furnishing office space in San Francisco for his own business, which he planned to call Nosal Partners. ER:352, 500. Nosal, Jacobson, and others also began discussing how to import information into the database Nosal had purchased from Cluen. SER:90-91. In July 2005, a Cluen representative came to Nosal's offices to conduct a four-day training session with Nosal, Christian, Jacobson, Froehlich-L'Heureaux, and others about how to set up the database. ER:384; SER:78-79. When they were talking to the Cluen representative during the training, Jacobson mentioned that he had source lists from Searcher. SER:79-80. Nosal, who was present, seemed surprised at the amount of data Jacobson had, and he raised his hands and said, "We don't have that," winking at Jacobson. SER:93-94. According to Jacobson, this response was "fairly common" for Nosal, and Jacobson understood it to mean that Nosal knew they had the data but did not want to acknowledge it. SER:93-94.

**D. Christian and Jacobson Access Korn/Ferry's Computers and Take Information**

During their Korn/Ferry employment, Nosal, Christian, Jacobson, and Froehlich-L'Heureaux each had usernames and passwords that provided them access to Korn/Ferry's computer system. ER:705-08. Korn/Ferry terminated Nosal's login credentials on December 8, 2004, approximately six weeks after he began his independent-contractor term with Korn/Ferry. ER:705. Although Nosal



asked for permission to keep his Korn/Ferry email account and voicemail until the end of 2004, Korn/Ferry denied his request. ER:968-69. Korn/Ferry terminated Christian's login credentials on January 24, 2005, three days after she left Korn/Ferry's employment. ER:706-07. Korn/Ferry terminated Jacobson's login credentials on March 2, 2005, the day after he left Korn/Ferry's employment. ER:707. Until August 2005, Froehlich-L'Heureaux had a username and password that allowed her to access Korn/Ferry's computer system. ER:707-08. Under Korn/Ferry's policies, Froehlich-L'Heureaux was not authorized to allow non-Korn/Ferry employees to use these login credentials. ER:708.

*1. April 12, 2005*

On April 12, 2005, Nosal and Christian were conducting a search for World Heart, a Christian & Associates client in the medical-device industry. ER:356-61. Neither Nosal nor Christian had much familiarity with the medical-device field, and Christian told Nosal that she did not want to do the World Heart search, which she expected would be very difficult. ER:360-61. As a result, Nosal conducted the search largely on his own, but he asked Christian to assist him by using Korn/Ferry source lists to find potential executive candidates. ER:361. Nosal was "very instructive" about which Korn/Ferry source lists might be useful. ER:360.

Following these discussions with Nosal, Christian asked Froehlich-L'Heureaux for her Korn/Ferry computer login credentials, which Froehlich-

L'Heureaux provided. ER:362-65. Christian then used Froehlich-L'Heureaux's credentials to access Korn/Ferry's computer system and ran a query in Searcher for financial executives in Northern California who worked in the medical-devices or life-sciences fields. ER:365. This query uncovered a source list that Korn/Ferry had created for a then-ongoing assignment. ER:365-66, 550-51.

Christian cut-and-pasted information from this source list into an email and sent it to Nosal with the subject line "Medical folks." ER:366, 548-51. The email contained the names, titles, and phone numbers for executives who could be appropriate for the World Heart search. ER:366. A few minutes later, Christian sent Nosal a second email containing a similar list of candidates with the subject line, "Use this one instead." ER:367; SER:318. Nosal printed out the second email, made handwritten notes on it, and circled the name of one executive whom he and Christian subsequently presented to World Heart as a possible candidate. ER:369-70; SER:318. The FBI later discovered this annotated document in Christian's apartment. ER:369; SER:318.

On April 12, 2005, Nosal and Christian were also attempting to win the business of UTStarcom, which was looking for a chief financial officer. ER:358-60. To prepare for that possible search, Nosal told Christian that he needed source lists from Korn/Ferry's past "hardware semiconductor-type telecom searches." ER:362. Nosal instructed Christian to retrieve information about these searches

from Korn/Ferry's computer system, telling her, "Get what you need. Get what I need." ER:362, 373. Thereafter, Christian used Froehlich-L'Heureaux's Korn/Ferry login credentials to access Searcher and generate custom reports from three source lists. ER:373-75, 781. These custom reports included executives' names, current positions, and, where available, cell-phone, work, and home numbers. ER:379; SER:291-317.

On the same day, Christian emailed Nosal a Microsoft Excel workbook that contained these three source-list custom reports, which were each labeled "Korn/Ferry Proprietary & Confidential." ER:373-76, 541-43; SER:288-317. In the body of the email, Christian wrote, "Each tab represents different searches. 1 is Ca Micro Devices, 2 is Perkin Elmer first CFO search, 3 is Perkin Elmer 2nd CFO search." ER:373-74; SER:288 (capitalization corrected). Nosal and Christian later presented UTStarcom with a candidate list that included some of the executives identified in these custom reports. ER:381-82.

None of the source lists that Christian obtained from Searcher on April 12, 2005, was available to the public at the time. ER:647-50. Nosal and Christian planned to bill World Heart and UTStarcom \$66,000 and \$175,000, respectively, for their search work. ER:382-84.

2. *July 12, 2005*

On July 12, 2005, Nosal and Christian were working on an executive-search assignment for PG&E, which wanted to hire a new vice president of corporate development or mergers and acquisitions. ER:384-87. A “very frustrated” Nosal asked Christian to get a cell-phone number for executive candidate Fran Barton. ER:390. Froehlich-L’Heureaux was also at Nosal’s offices for the Cluen training, and Christian asked her for her Korn/Ferry login credentials, which Froehlich-L’Heureaux provided. ER:312, 387.

Christian used Froehlich-L’Heureaux’s password to log into Searcher from the computer in Nosal’s personal office and then ran several searches for executives in the utilities industry who specialized in mergers and acquisitions. ER:387-89, 816-23. As a result of these searches, Christian generated a custom report containing the names of 65 executives, which she later provided to Nosal. ER:388-89, 823-24. Christian then queried Searcher for information on Barton and two other executives and for information on past work Korn/Ferry had done to fill mergers-and-acquisitions positions in the utilities industry. ER:390-91, 826-29. Nosal and Jacobson later called Barton, and before the call, Nosal instructed Jacobson to introduce him to Barton as “David Nelson.” SER:65-68.

3. *July 29, 2005*

On July 29, 2005, Jacobson and Froehlich-L'Heureaux were at Nosal's offices, and Jacobson asked Froehlich-L'Heureaux to log into Korn/Ferry's computer system. ER:500-02. After Froehlich-L'Heureaux did so, she left the room, and Jacobson used Searcher to generate and download 25 custom reports containing information about 3490 executives, including their personal phone numbers. ER:501-02, 526-29; SER:81-82.

**SUMMARY OF ARGUMENT**

This Court should affirm Nosal's convictions and judgment because Nosal has failed to identify any error, much less error that would require reversal.

1. Sufficient evidence supported the jury's verdict. With respect to the computer-fraud offenses, Christian and Jacobson accessed Korn/Ferry's computers "without authorization" when they used Froehlich-L'Heureaux's login credentials to obtain information from Korn/Ferry's computer system after Korn/Ferry had revoked their own login credentials. Although Nosal disagrees, his position is inconsistent with the plain language of 18 U.S.C. § 1030, this Court's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), and the trial evidence. Nosal does not dispute that the evidence allowed the jury to find him liable for Christian's and Jacobson's conduct under *Pinkerton v. United States*, 328 U.S. 640 (1946), and the evidence also established that he aided and abetted their

offenses.

With respect to the trade-secrets offenses, the evidence established that the relevant Korn/Ferry source lists were trade secrets. Korn/Ferry took reasonable measures to protect the secrecy of its source lists, and the source lists derived independent economic value from not being generally known to, or readily ascertainable through proper means by, the public. The evidence also showed that Christian and Nosal both knew that the relevant source lists were trade secrets and knew or intended that they would injure Korn/Ferry when they downloaded the lists from Korn/Ferry's computers to further Nosal's competing business.

2. The district court's instruction on the meaning of "without authorization" properly described this Court's holding in *Brekka*, which addressed the scope of this term. The court also properly declined to instruct that a person accesses a computer without authorization only if he "circumvents technological access barriers" because this proposed instruction misstates the law. Furthermore, any error was harmless because Christian and Jacobson did circumvent technological access barriers: they used Froehlich-L'Heureaux's password to log into Korn/Ferry's computers, thereby bypassing the password-protection that Korn/Ferry used to exclude outsiders from its computers.

The district court's aiding-and-abetting instruction properly advised the jury that it could convict Nosal as an aider and abettor only if the government proved

that Nosal acted knowingly and intentionally before the crime was completed. The deliberate-ignorance instruction did not undercut this advance-knowledge requirement, nor did it allow the jury to convict Nosal as an aider and abettor based on conduct that was merely reckless. Read as a whole, the instructions also did not allow the jury to convict Nosal of aiding and abetting the computer-fraud counts if it found that Nosal believed that Froehlich-L'Heureaux, rather than Christian or Jacobson, accessed Korn/Ferry's computers. Nosal therefore cannot prevail on his plain-error challenges to the deliberate-ignorance instruction, and in any event, the alleged errors did not affect his substantial rights because they could not have affected the jury's verdict.

The district court also correctly instructed the jury that it could find Nosal guilty of conspiring to commit a trade-secrets offense even if the government did not prove that the information he conspired to obtain and possess was, in fact, a trade secret. At least three circuits have so held, and this instruction is consistent with the general principle that a conspiracy conviction may be sustained even where the goal of the conspiracy is impossible. Furthermore, this instruction did not constructively amend the indictment because the indictment's allegation that Nosal and his co-conspirators took "trade secrets" was irrelevant to Nosal's culpability for conspiracy.

3. The district court properly exercised its discretion in admitting and excluding evidence about Nosal's noncompete agreement. The court allowed both parties to introduce evidence about a person's subjective beliefs about the validity of this agreement, which enabled Nosal to present evidence that he believed that Korn/Ferry had subjected him to an illegal contract. The court also properly barred the parties from introducing evidence and argument about whether the noncompete provisions were legal, a question that was both irrelevant and likely to confuse the jury. Furthermore, the district court instructed the jury to disregard any testimony about Nosal breaching his Korn/Ferry agreements.

4. The district court properly ordered Nosal to pay Korn/Ferry \$827,983.25 in restitution, even though this amount exceeded Nosal's loss amount under USSG § 2B1.1. Under the Sentencing Guidelines, Nosal's loss calculation must exclude costs that Korn/Ferry incurred as a result of assisting the government in this criminal investigation and prosecution. However, the Mandatory Victim Restitution Act requires that Nosal reimburse Korn/Ferry for such costs, and the restitution order properly reflected this requirement. Furthermore, Nosal has identified no basis for concluding that the district court abused its discretion or clearly erred in concluding that approximately 62 percent of Korn/Ferry's reported attorneys' fees were reasonable and necessary to the criminal investigation and prosecution.



## ARGUMENT

### I. SUFFICIENT EVIDENCE SUPPORTED NOSAL'S CONVICTIONS

#### A. Standard Of Review

The Court reviews de novo challenges to the sufficiency of the evidence, including challenges that involve questions of statutory interpretation. *United States v. Wright*, 625 F.3d 583, 590 (9th Cir. 2010). A claim of insufficient evidence fails if, “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. Nevils*, 598 F.3d 1158, 1163-64 (9th Cir. 2010) (en banc) (emphasis in original).

#### B. Nosal Is Guilty Of Computer Fraud

Counts Two through Four of the second superseding indictment charged that Nosal fraudulently accessed Korn/Ferry computers “without authorization” and thereby furthered the intended fraud and obtained something of value, in violation of 18 U.S.C. § 1030(a)(4). ER:1176. These charges stemmed from the incidents on April 12, July 12, and July 29, 2005, when Christian and Jacobson used Froehlich-L'Heureaux's login credentials to access Korn/Ferry's computer system after Korn/Ferry had revoked their own login credentials. *See* ER:1176; Statement of Facts D, *supra*. Under the plain language of Section 1030 and this Court's decision in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), these

undisputed facts are sufficient to establish that Christian and Jacobson accessed Korn/Ferry's computer system "without authorization." *See* Part I.B.2, *infra*. Furthermore, Nosal was liable for Christian's and Jacobson's conduct both under *Pinkerton v. United States*, 328 U.S. 640 (1946), and on an aiding-and-abetting theory. *See* Part I.B.3, *infra*.

1. *Procedural background*

In 2008, a superseding indictment charged Nosal with various offenses, including eight violations of 18 U.S.C. § 1030(a)(4). CR:42. Five of these counts alleged that Christian and Froehlich-L'Heureaux had exceeded their authorized access to Korn/Ferry's computers while employed at Korn/Ferry. ER:153-55. The three remaining counts alleged that Christian and Jacobson had accessed Korn/Ferry's computers without authorization after they left Korn/Ferry's employment. ER:153-55. On Nosal's motion, the district court dismissed the five "exceeds authorized access" counts before trial. ER:155. The government appealed, and in an en banc opinion, this Court affirmed the dismissal of those five counts. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).

The case returned to the district court for trial on the three "without authorization" Section 1030(a)(4) charges, now Counts Two through Four of the

second superseding indictment.<sup>2</sup> ER:1176. Before trial, the district court denied Nosal's motion to dismiss these counts. ER:150-65. In so doing, the district court held that Section 1030(a)(4) does not require the government to prove "the circumvention of technological access barriers" but that, in any event, the indictment sufficiently alleged such circumvention. ER:160-62. The court also rejected Nosal's claim that, as a matter of law, Christian and Jacobson did not access Korn/Ferry's computers "without authorization" because Froehlich-L'Heureaux had willingly shared her password with them. ER:162-63.

2. *The evidence established that Christian and Jacobson accessed Korn/Ferry's computers "without authorization"*

To prove that Christian and Jacobson violated Section 1030(a)(4), the government had to show that they: (1) accessed a protected computer, (2) "without authorization" or "exceed[ing] authorized access," (3) knowingly and with intent to defraud, and thereby (4) furthered the intended fraud and obtained something of value. *Id.*; *Brekka*, 581 F.3d at 1132 (describing elements of civil action based on Section 1030(a)(4) violation). Nosal does not dispute the sufficiency of the evidence as to the first, third, and fourth elements. With respect to the second element, the evidence established that Christian and Jacobson accessed Korn/Ferry's computers "without authorization" under Section 1030 and this

---

<sup>2</sup> The original district judge assigned to the case, the Honorable Marilyn Hall Patel, retired during the interlocutory appeal. The case was reassigned to the Honorable Edward M. Chen.

Court's decision in *Brekka*.

- a. *Christian and Jacobson acted "without authorization" when they accessed Korn/Ferry computers after Korn/Ferry terminated their access privileges*

Section 1030 does not define "without authorization," but in *Brekka*, this Court held that a person accesses a computer "without authorization" in two situations: (1) "when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission)," or (2) "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." 581 F.3d at 1135.

Counts Two through Four present the second situation because Christian and Jacobson accessed Korn/Ferry's computers after Korn/Ferry terminated their access privileges. *See* ER:706-07. Accordingly, the jury correctly concluded that Christian and Jacobson accessed Korn/Ferry's computers "without authorization."

Nosal does not address *Brekka*'s holding that a defendant accesses a computer without authorization "when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." 581 F.3d at 1135. Instead, Nosal challenges the applicability of the other "without authorization" scenario described in *Brekka*, which applies "when the person has not received permission to use the computer for any purpose." *Id.* Specifically, Nosal argues that Christian and Jacobson did not act "without authorization"

because they had Froehlich-L'Heureaux's permission to access Korn/Ferry's computers. *See* Appellant's Opening Brief ("AOB"):14-15, 18-19. But because *Brekka's* definition of "without authorization" is framed in the alternative, the government was not required to prove that Christian and Jacobson never had permission to use Korn/Ferry's computers. *See* 581 F.3d at 1135. Rather, the government can and did prove that Christian and Jacobson acted "without authorization" by demonstrating that they accessed Korn/Ferry's computers after Korn/Ferry had terminated their access privileges. *See id.*

In fact, Nosal largely ignores *Brekka* and instead suggests that the en banc opinion in this case supports his claim that he and his co-conspirators did not act without authorization. But the proper interpretation of "without authorization" was not before the en banc Court. Instead, the en banc opinion focused on the scope of the "exceeds authorized access" element of Section 1030, which was not at issue at trial. *See generally Nosal*, 676 F.3d at 856-64. Furthermore, the en banc opinion did not overrule or disturb *Brekka's* holdings about the "without authorization" element. Indeed, the en banc opinion announced that this Court "continue[s] to follow in the path blazed by *Brekka*." *Id.* at 863. Accordingly, *Brekka* remains the law in this circuit, and it establishes that Christian and Jacobson accessed Korn/Ferry's computers "without authorization."

- b. *Froehlich-L'Heureaux did not and could not unilaterally override Korn/Ferry's decision to terminate Christian's and Jacobson's authority to access its computers*

After Korn/Ferry revoked Christian's and Jacobson's computer-access privileges, Froehlich-L'Heureaux allowed both Christian and Jacobson to use her login credentials to obtain information from Korn/Ferry's computer system. But Froehlich-L'Heureaux did not and could not "authorize" Christian and Jacobson to access Korn/Ferry's computer within the meaning of Section 1030 because Korn/Ferry had not empowered her to grant them such permission. Indeed, Korn/Ferry expressly prohibited its employees from sharing their Korn/Ferry passwords or computer accounts with anyone. SER:232-33, 235, 237.

Accordingly, the jury reasonably concluded that Froehlich-L'Heureaux did not reverse Korn/Ferry's revocation of Christian's and Jacobson's access privileges when she shared her password with them.

Nosal does not dispute that Korn/Ferry prohibited Froehlich-L'Heureaux from sharing her login credentials. Instead, Nosal asks this Court to hold that, as a matter of law, a person with a password to a particular computer – here, Froehlich-L'Heureaux – may "authorize" others to access that computer simply by sharing her password with them. *See* AOB:19-23. This argument is inconsistent with *Brekka*, which holds that the actions of the employer, not the actions of an authorized employee user, determine authorization.

In *Brekka*, Brekka’s former employer contended that Brekka’s authorization to use its computer ended during his employment when he resolved to use the computer contrary to the employer’s interest. *See id.* at 1133. The employer presumed that the unilateral actions of an authorized employee user – there, Brekka – could determine whether a person had authorization to access the employer’s computers. *See id.* But the Court disagreed and instead held that the plain language of Section 1030 “indicates that ‘authorization’ depends on actions taken by the employer.” *Id.* at 1135. The Court explained that “[i]t is the employer’s decision to allow or to terminate an employee’s authorization to access a computer that determines whether the employee is with or ‘without authorization.’” *Id.* at 1133.

In other words, *Brekka* establishes that in the employer-employee context, only the employer has the power to authorize someone to access its computers within the meaning of Section 1030.<sup>3</sup> Accordingly, once Korn/Ferry terminated access for Christian and Jacobson, they could not regain authorization through Froehlich-L’Heureaux’s surreptitious sharing of her password. This conclusion is consistent with the plain language of Section 1030, which expressly contemplates that a person who uses someone else’s password to access a computer may act

---

<sup>3</sup> *Brekka* leaves open the possibility that the employer could exercise this power indirectly by expressly allowing others, such as its agents or authorized computer users, to authorize additional persons to access its computers. As discussed earlier, however, Korn/Ferry did not give Froehlich-L’Heureaux that power.

“without authorization” for purposes of Section 1030. *See* 18 U.S.C. § 1030(a)(6) (making it a crime to traffic in “any password or similar information through which a computer may be accessed without authorization”).

This Court did not hold otherwise in its en banc opinion. Although the en banc Court expressed concern that a broader interpretation of “exceeds authorized access” could result in criminal liability for Facebook users who allow their loved ones to access their Facebook accounts, *Nosal*, 676 F.3d at 861, it did not hold that, as a matter of law, a person is “authorized” to access a computer as long as an authorized user of that computer shares her password with him.<sup>4</sup> Indeed, such a holding would allow a hacker to escape liability under Section 1030 simply by using an authorized user’s login credentials to gain access to the target computer. Furthermore, as previously discussed, the en banc Court reaffirmed *Brekka* and did not disturb its holding that, in the employment context, “[i]t 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.’” 581 F.3d at 1133.

Finally, although *Nosal* suggests that upholding the jury’s verdict in this case would criminalize common behavior such as sharing a Facebook password

---

<sup>4</sup> Likewise, under physical-trespass principles, Froehlich-L’Heureaux lacked the authority to consent to others’ access of Korn/Ferry computers because she was neither in possession of the computers nor acting as Korn/Ferry’s agent when she shared her password. *See* AOB:22.



with a friend, *see* AOB 19, 24, Nosal’s examples are materially different from his own conduct. None involves an employee who gives outsiders access to her employer’s computers, and none involves a person who accesses his former employer’s computers after the employer had rescinded his access privileges. *See id.* Accordingly, in the unlikely event that the government attempted to prosecute one of Nosal’s hypothetical cases, the hypothetical defendant could argue that the password holder gave him “permission to use the computer.”<sup>5</sup> *Brekka*, 581 F.3d at 1135. Although *Brekka* largely forecloses this argument in the employer-employee context, it leaves open the possibility that other categories of computer users, such as those with personal online accounts, could authorize friends and family to access the relevant computers for purposes of Section 1030. In an appropriate case, the Court could consider those arguments, but *Brekka* has already answered the legal questions presented by Nosal’s own case.

*c. Section 1030 does not require the government to prove “the circumvention of technological access barriers,” and in any event, the government made this showing*

Nosal also contends that he is not guilty on Counts Two through Four because the government failed to prove that Christian and Jacobson “circumvented technological access barriers” when they accessed Korn/Ferry’s computers.

---

<sup>5</sup> In Nosal’s hypothetical cases, the hypothetical defendants likely did not act “knowingly and with intent to defraud” when they accessed their loved ones’ online accounts, as required by 18 U.S.C § 1030(a)(4).

AOB:21. But “the circumvention of technological access barriers” is not an element of any Section 1030 offense, including Section 1030(a)(4). *See* 18 U.S.C. § 1030(a); *Brekka*, 581 F.3d at 1132 (listing elements required to bring a successful civil action based on a Section 1030(a)(4) violation). Nosal identifies no statutory language to support his contrary position.

Nor did the en banc Court hold that Section 1030 requires the government to prove “the circumvention of technological access barriers.” This phrase appears in the en banc opinion only once, when the Court explains that Section 1030 is “a statute whose general purpose is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets.”<sup>6</sup> *Nosal*, 676 F.3d at 863. This statement does not amount to a holding that “the circumvention of technological access barriers” is a required element of all Section 1030 offenses. Indeed, such a holding would be contrary to the plain language of Section 1030, particularly because some Section 1030 offenses do not require the defendant to access a computer at all. *See* 18 U.S.C. §§ 1030(a)(5)(A), (6), (7).

But even if Section 1030(a)(4) did require proof that Christian and Jacobson “circumvented technological access barriers,” the trial evidence established that

---

<sup>6</sup> The en banc Court provided other “hacking” definitions that do not allude to the circumvention of technological access barriers. *See Nosal*, 676 F.3d at 856-57 (“hacking” means “access[ing] unauthorized data or files”); *id.* at 858 (“outside hackers” are “individuals who have no authorized access to the computer at all” and “inside hackers” are “individuals whose initial access to a computer is authorized but who access unauthorized information or files”).

Christian and Jacobson did exactly that when they accessed Korn/Ferry's computers. Korn/Ferry password-protected its computers, thereby creating a technological access barrier intended to prevent non-Korn/Ferry employees from logging into its computers.<sup>7</sup> ER:696-704. Christian and Jacobson circumvented this barrier when they used Froehlich-L'Heureaux's login credentials without Korn/Ferry's permission to access Korn/Ferry's computers. *Cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir. 2004) (describing a person who "use[s] someone else's password to break into a mail server" as a "hacker").

*d. Nosal did not have authorization to access Korn/Ferry computers during the relevant period*

Nosal does not contend that he had authorization to access Korn/Ferry's computers after December 8, 2004, the date Korn/Ferry revoked his access privileges. ER:980; *see* AOB:25-26. Nonetheless, Nosal argues that the jury should have acquitted him on Counts Two through Four because Korn/Ferry allowed him to ask its employees for information that was relevant to his independent-contractor projects. *See* AOB:25; ER:1032-34. But Nosal does not explain why his ability to request information from Korn/Ferry is relevant to the question of whether *Christian and Jacobson* accessed Korn/Ferry's computers "without authorization." Nor does he claim that Korn/Ferry allowed him to ask

---

<sup>7</sup> Nosal and amicus Electronic Frontier Foundation agree that password-protection may create a technological access barrier. *See* AOB:23; EFF Br:12.

Korn/Ferry employees, much less non-Korn/Ferry employees, to send him information from Searcher that was unrelated to his independent-contractor work.

Nosal's argument also conflates authorization to access a computer with authorization to receive information from that computer. Although Section 1030(a)(4) requires that a person both "access[] a protected computer" and thereby "obtain anything of value," the "without authorization" requirement applies only to the computer access. *Id.*; see also *Brekka*, 581 F.3d at 1133 ("It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'"). Nosal cannot escape liability under Section 1030(a)(4) by arguing that he was authorized to receive certain information from Korn/Ferry computers.

3. *Nosal was liable for Christian's and Jacobson's conduct both under Pinkerton and as an aider and abettor*

The government argued that Nosal was criminally liable for Christian's and Jacobson's conduct under both *Pinkerton* and as an aider and abettor. SER:199-200. Nosal does not dispute that the evidence allowed the jury to find him liable on Counts Two through Four under *Pinkerton*, which "renders all co-conspirators criminally liable for reasonably foreseeable overt acts committed by others in furtherance of the conspiracy." *United States v. Bingham*, 653 F.3d 983, 997 (9th Cir. 2011) (internal brackets omitted). Accordingly, this Court need not decide whether the evidence was also sufficient to support Nosal's conviction on an

aiding-and-abetting theory. *See United States v. Hsiung*, \_\_\_ F.3d \_\_\_, 2015 WL 400550, at \*18 n.10 (9th Cir. Jan. 30, 2015) (“Reversal is not required when the jury returns a general guilty verdict and one of the possible bases of conviction was . . . merely unsupported by sufficient evidence.” (internal quotation marks omitted)).

Nonetheless, the trial evidence sufficiently established that Nosal aided and abetted the conduct at issue in Counts Two through Four. To convict a defendant as an aider and abettor, the jury must find that: (1) the defendant had the specific intent to facilitate the commission of a crime by another; (2) the defendant had the requisite intent of the underlying substantive offense; (3) the defendant assisted or participated in the commission of the underlying substantive offense; and (4) someone committed the underlying substantive offense. *United States v. Thum*, 749 F.3d 1143, 1148-49 (9th Cir. 2014). Last year, the Supreme Court addressed the intent requirement in *Rosemond v. United States*, 134 S. Ct. 1240 (2014), and held that a defendant must have “advance knowledge” that the crime was going to occur. *Id.* at 1243. The Court explained that “advance knowledge” means “knowledge at a time the accomplice can do something with it – most notably, opt to walk away.” *Id.* at 1249-50.

Nosal does not dispute that the government proved most of the elements of aiding-and-abetting liability, including that he knew in advance and intended that

Christian and Jacobson would obtain information from Korn/Ferry's computers. AOB:29-30. The only question is whether the government proved that Nosal had advance knowledge that Christian and Jacobson would access Korn/Ferry's computers without authorization. *See* AOB:29-31. The government presented direct evidence that Nosal had this advance knowledge: Christian herself testified that Nosal knew she was using Froehlich-L'Heureaux's password to get documents from Korn/Ferry. ER:484.

Although Nosal argues that the jury should not have credited this testimony because Christian did not explain how or when she learned this information, Christian was romantically involved with Nosal through spring 2005, spoke to him daily, and kept him apprised of her work activities. ER:325-28. Given this context, the jury could reasonably believe that Nosal knew about Christian's plans to use Froehlich-L'Heureaux's login credentials to access Korn/Ferry computers. Indeed, with respect to the computer access on April 12, 2005, Nosal instructed Christian to retrieve certain information from Korn/Ferry's computer system, telling her, "Get what you need. Get what I need." ER:362, 373. On July 12, 2005, when both Froehlich-L'Heureaux and Christian were in Nosal's offices to attend the Cluen training, Nosal asked Christian, not Froehlich-L'Heureaux, to get Fran Barton's cell-phone number for him. ER:312, 390. Taken together, this evidence establishes that Nosal had advance knowledge that Christian and

Jacobson would use Froehlich-L'Heureaux's login credentials to access Korn/Ferry's computers.

**C. Nosal Is Guilty Of The Trade-Secrets Offenses Charged In Counts Five And Six**

Count Five of the second superseding indictment charged Nosal with downloading, copying, and duplicating trade secrets without authorization, in violation of 18 U.S.C. § 1832(a)(2). ER:1177. Count Six charged Nosal with receiving and possessing Korn/Ferry trade secrets that he knew had been stolen and appropriated without authorization, in violation of 18 U.S.C. § 1832(a)(3). ER:1178. Both counts were based on the events of April 12, 2005, when Christian downloaded three source lists from Searcher and then sent Nosal an email attaching those source lists and a second email containing information copied from a fourth source list. *See* ER:1177-78; Statement of Facts D.1, *supra*.

Sections 1832(a)(2) and (3) impose criminal penalties when: (1) someone knowingly downloads, copies, or duplicates information without authorization, or receives or possesses information that he knows was stolen or appropriated without authorization; (2) the information is a trade secret that is related to or included in a product produced for or placed in interstate or foreign commerce; (3) the person acted with intent to convert a trade secret to the economic benefit of someone other than the owner; and (4) the person intended or knew that the offense would injure

any owner of the trade secret. 18 U.S.C. § 1832(a)(2), (3) (2005).<sup>8</sup>

Nosal does not dispute that the evidence proved some of these elements, but he argues that the government failed to prove that one or more of the April 12 source lists was a trade secret; that he and Christian knew that those lists were trade secrets; and that he and Christian knew or intended that their offenses would injure Korn/Ferry. *See* AOB:41-51. Sufficient evidence supported the jury's verdict as to each of these elements.

*1. The relevant source lists were trade secrets*

For purposes of 18 U.S.C. § 1832(a), the term “trade secret” means “all forms and types of financial, business, scientific, technical, economic, or engineering information,” including compilations, “whether or how stored, compiled, or memorialized,” provided that: (1) “the owner thereof has taken reasonable measures to keep such information secret,” and (2) “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). Nosal does not dispute that the April 12 source lists were business information, and as explained below, the evidence also established the other two requirements of the trade-secrets definition. Accordingly, the jury

---

<sup>8</sup> In 2012, Congress amended the statute to require that the relevant trade secret “relate[] to a product or service used in or intended for use in interstate or foreign commerce.” 18 U.S.C. § 1832(a) (2015).



properly concluded that the April 12 source lists were trade secrets.

*a. Korn/Ferry took reasonable measures to keep the source lists secret*

The jury properly concluded that Korn/Ferry took “reasonable measures” to keep the April 12 source lists secret. 18 U.S.C. § 1839(3). The government did not have to prove that Korn/Ferry took all available measures to protect the secrecy of the source lists, or that the measures Korn/Ferry adopted were foolproof. *See* H.R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026 (“[I]t is not the Committee’s intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.”); *United States v. Howley*, 707 F.3d 575, 579 (6th Cir. 2013) (“The ‘reasonable measures’ requirement does not mean a company must keep its own employees and suppliers in the dark about machines they need to do their work.”). Rather, the government had to prove that the measures Korn/Ferry took were “reasonable under the circumstances.” H.R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026.

The evidence established that Korn/Ferry took the following measures to protect the secrecy of the April 12 source lists. Korn/Ferry stored its source lists on Searcher, which was part of Korn/Ferry’s internal computer system. ER:852-53, 859-62, 898-99. A computer user could access Searcher only by gaining access to Korn/Ferry’s computer system, which required an authorized username

and password. ER:700, 852-53. Korn/Ferry issued its employees unique usernames for the system and required those employees to change their passwords every 60 days. ER:700; SER:232. Korn/Ferry prohibited its employees from sharing their passwords or computer accounts with anyone, and when an employee left Korn/Ferry's employment, Korn/Ferry terminated that employee's login credentials. ER:702-04; SER:232-33, 235, 237. Korn/Ferry also used firewalls and anti-virus software to protect its computer system and stored Searcher's North American database on computers at a guarded data center to which only two or three Korn/Ferry employees had physical access. ER:716-18.

Every time Korn/Ferry employees logged into Korn/Ferry's computer system, a pop-up window notified them that the information stored on Korn/Ferry's computer system was "the property of Korn/Ferry"; that they needed "specific authority" to access any Korn/Ferry information; and that accessing Korn/Ferry information without such authority could "lead to disciplinary action or criminal prosecution." ER:698-99; SER:260, 263. Furthermore, when a computer user accessed Searcher's custom-report feature, a pop-up screen informed them, "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only." ER:743; SER:250.

Korn/Ferry also required its employees and contractors to sign confidentiality agreements, in which the employees agreed to protect source lists

and other confidential information. ER:934-35; SER:274-75. Under these agreements, Korn/Ferry employees pledged: (1) to keep source lists private and use them only in connection with their work at Korn/Ferry; (2) not to disclose, use, or copy source lists except as required by their Korn/Ferry work; (3) to prevent others outside Korn/Ferry from improperly gaining access to source lists; (4) to immediately notify Korn/Ferry if they suspected that anyone was inappropriately using or disclosing source lists; and (5) to return all source lists to Korn/Ferry upon leaving their employment.<sup>9</sup> SER:274. Korn/Ferry also required its employees to sign a Code of Business Conduct that prohibited them from disclosing information on Searcher and Korn/Ferry's other proprietary computer programs; instructed them to "[a]ssure the safekeeping" of Korn/Ferry documents and files; and prohibited them from taking such materials with them at the end of their employment. ER:936-39; SER:269.

Taken together, this evidence sufficiently established that Korn/Ferry took reasonable measures to protect the secrecy of its source lists. Although Nosal suggests additional steps Korn/Ferry could have taken, such as password-protecting individual source lists, the government was not required to prove that

---

<sup>9</sup> The last of these requirements contradicts Nosal's claim that "[e]mployees were free to take all their source lists with them when they left KFI." AOB:48.

Korn/Ferry took all conceivable measures to protect its information.<sup>10</sup> *See* AOB:47-48. Likewise, even if some Korn/Ferry employees did not comply with the terms of their confidentiality agreements, *see* AOB:48, these agreements still constituted a reasonable measure because Korn/Ferry was entitled to rely on its employees to honor their contractual obligations. For all of these reasons, the jury properly concluded that Korn/Ferry took reasonable measures to protect the secrecy of the April 12 source lists.

*b. The source lists derived economic value from not being generally known to, and not being readily ascertainable through proper means by, the public*

The evidence also supported the jury's conclusion that the April 12 source lists derived "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).

First, the trial evidence established that the April 12 source lists were not generally known to the public. Specifically, Korn/Ferry Vice President of Information Services Marlene Briski, who was responsible for the data in Searcher

---

<sup>10</sup> Although Nosal claims that Korn/Ferry disclosed or sold source lists to clients during pitches and "mapping" engagements, the trial evidence he cites does not support this claim. *Compare* AOB:47 (citing ER:590) *with* ER:590 (testimony that Korn/Ferry's "mapping" services involved Korn/Ferry selling "information" to a client, some of which might come from Searcher). Furthermore, when Korn/Ferry provided clients with information that came from Searcher, Korn/Ferry designated the information as confidential and for the client's use only. ER:1007.

in 2005, testified that none of these source lists had become available to the public. ER:647-50, 687. The jury was entitled to credit her testimony and therefore conclude that these source lists were not public. Although Nosal contends that other Korn/Ferry source lists may have been publicly known, he does not dispute Briski's testimony that these particular source lists were not. *See* AOB:47-48. Furthermore, the government was not required to prove that Korn/Ferry withheld these source lists from the clients for whom they were developed, *see* AOB:48, but even if such proof were required, the jury could reasonably conclude that the government made that showing here. Specifically, the evidence established that Korn/Ferry typically did not send source lists to its clients and that, when it did so, it designated them as confidential and for the client's use only. ER:858-59, 1007.

Second, the trial evidence established that the April 12 source lists were not readily ascertainable through proper means by the public. Indeed, Christian testified that she went to Searcher to obtain these source lists because, as far as she knew, the lists were not available anywhere else. ER:379-80. Korn/Ferry's source lists were the fruit of years of work by Korn/Ferry employees, who compiled and culled information from a variety of sources, including previous source lists, to develop lists of promising executive candidates who held particular positions in

particular industries.<sup>11</sup> ER:854-59, 870-71. These lists contained non-public information about the executives, including their cell-phone, home, and direct work numbers. ER:879-80.

This evidence established that source lists were unique compilations of information that could not be readily recreated or ascertained through proper means. Although Nosal argues that some of the information in the source lists was publicly available, he identifies no ready means of compiling this public information into a list of qualified executives that held the same position in the same industry. *See* AOB:44-47. Furthermore, a trade secret can include elements that are in the public domain if the trade secret itself constitutes “an effective, successful and valuable integration of the public domain elements.” *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994) (evaluating claim under Colorado’s Trade Secrets Act); *see also* 18 U.S.C. § 1839(3) (defining “trade secret” to include “compilations”); *Penalty Kick Management Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003) (evaluating claim under Georgia Trade Secrets Act and concluding that “even if all

---

<sup>11</sup> Although Nosal compares the source lists to “customer lists,” *see* AOB:44, this analogy is inapt. The source lists did not contain the names of Korn/Ferry’s clients, but rather compiled information about potential candidates that Korn/Ferry had identified for executive positions that its clients were seeking to fill. ER:854-59. In any event, customer lists may constitute trade secrets if they satisfy the relevant statutory requirements. *See, e.g., Nationwide Mut. Ins. Co. v. Mortensen*, 606 F.3d 22, 28 (2d Cir. 2010) (explaining that customer lists fall within the scope of Connecticut’s trade-secrets statute).

of the information is publicly available, a unique combination of that information, which adds value to the information, also may qualify as a trade secret”).

2. *Nosal and Christian knew that the source lists were trade secrets*

Nosal does not dispute that he and Christian knew about the measures Korn/Ferry took to protect its source lists. *See* AOB:49-50. Because they were familiar with these measures, the jury could also conclude that they knew that the source lists derived independent economic value from being secret. After all, if the source lists were already in the public domain or readily ascertainable, Korn/Ferry would not have gone to such great lengths to prevent their unauthorized use and disclosure. Christian also testified that, as far as she knew, she could obtain the source lists only from Searcher, and not by some other means. ER:379. Because Christian and Nosal worked closely together and regularly discussed source lists, *see* ER:327-28, the jury could reasonably infer that Nosal shared the same view.

In addition, both Nosal and Christian signed confidentiality agreements in which they acknowledged that Korn/Ferry’s source lists were “extremely valuable” confidential information and were “accorded the legal protection applicable to a company’s trade secrets.” ER:319; SER:274-75. These agreements are strong evidence of Nosal’s and Christian’s knowledge because they reveal that Korn/Ferry told both Nosal and Christian that the source lists were trade secrets. Although Nosal now argues that the agreements incorrectly characterized source

lists as trade secrets, *see* AOB:49-50, Nosal never took issue with this characterization when he was at Korn/Ferry. ER:918-19, 940.

Finally, the government was not required to prove that Nosal and Christian were familiar with the legal definition of “trade secret.” As this Court has explained, ignorance of the law is no defense to criminal prosecution, and “knowledge of the law is almost never an element of a crime.” *United States v. Torres-Flores*, 502 F.3d 885, 888 n.4 (9th Cir. 2007). Nosal identifies no court that has held that Section 1832(a) is the rare exception to this general rule, and the statute’s legislative history confirms that it is not. *See* H.R. Rep. No. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030-31 (“It is not necessary that the government prove that the defendant knew his or her actions were illegal.”).

For all of these reasons, sufficient evidence supported the jury’s conclusion that Nosal and Christian knew that the relevant source lists were trade secrets.

3. *Nosal and Christian knew or intended that their conduct would injure Korn/Ferry*

The evidence also established that Nosal and Christian engaged in the conduct charged in Counts Five and Six intending or knowing that these offenses would injure Korn/Ferry. *See* 18 U.S.C. § 1832(a). As discussed in the previous subsection, Nosal and Christian both knew that Korn/Ferry’s source lists were “extremely valuable,” and they were familiar with the steps that Korn/Ferry took to prevent their disclosure. Furthermore, Nosal and Christian took these source lists



to further the work of their competing executive-search business, ER:360-62, a business that they knew would injure Korn/Ferry. Indeed, Nosal repeatedly told Christian that Korn/Ferry was paying him a lot of money to “stay out of the market,” ER:353, which reveals that Nosal and Christian both believed that Korn/Ferry would suffer economic injury if Nosal engaged in competing work. After all, Korn/Ferry would not have paid Nosal to “stay out of the market” if Nosal’s competing work had no adverse effect on Korn/Ferry. Because Nosal and Christian took the relevant source lists to further their competing business, the jury could reasonably conclude that they knew that their efforts would injure Korn/Ferry.<sup>12</sup>

## **II. THE DISTRICT COURT DID NOT ERR OR PLAINLY ERR IN FORMULATING THE JURY INSTRUCTIONS**

### **A. Standard Of Review**

The Court reviews the language and formulation of a jury instruction for an abuse of discretion. *United States v. Garcia*, 768 F.3d 822, 827 (9th Cir. 2014). The Court reviews de novo whether the jury instructions accurately define the elements of a statutory offense. *United States v. Awad*, 551 F.3d 930, 938 (9th Cir. 2009). If a jury instruction misstates an element of a statutory crime, the error is harmless if it is “clear beyond a reasonable doubt that a rational jury would have

---

<sup>12</sup> Given Nosal’s personal animus towards Korn/Ferry, the jury could also conclude that Nosal, at least, intended this result. *See* ER:330-33, 352-53.

found the defendant guilty absent the error.” *Id.* The Court reviews de novo allegations that the jury instructions constructively amended the indictment.

*United States v. Mancuso*, 718 F.3d 780, 790 (9th Cir. 2013).

When a defendant fails to make a timely objection to the jury instructions, the Court’s review is for plain error. *United States v. Anderson*, 741 F.3d 938, 945 (9th Cir. 2013). Plain-error review requires the Court to find (1) an error that is (2) plain and (3) affects substantial rights. *Id.* Even if these conditions are met, this Court may only exercise its discretion to correct the error if it seriously affects the fairness, integrity, or public reputation of judicial proceedings. *Id.*

## **B. The “Without Authorization” Jury Instruction Was Correct**

### *1. Background*

Before trial, the district court proposed an instruction on the meaning of “without authorization” which stated in part, “Whether a person is authorized to access the computers in this case depends on the actions taken by Korn/Ferry to grant or deny access to that person.” SER:17. Nosal objected to this instruction and asked the district court to instruct that “[a] person accesses a computer without authorization when he circumvents technological access barriers.” ER:1083.

At the jury-instructions hearing after the close of evidence, the district court announced that it intended to give a “without authorization” instruction that closely resembled an instruction the government had proposed. SER:154-57; *see also*

SER:26-27. The court read its proposed instruction aloud, and Nosal did not object to its language, except to suggest a minor amendment that the district court adopted. SER:154-57. Nosal did not ask the district court to instruct the jury that “without authorization” requires proof that the defendant circumvented technological access barriers. *See* SER:154-66.

The district court’s final “without authorization” instruction stated:

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 a computer without any permission), or when Korn/Ferry has rescinded permission to use the computer and the person uses the computer anyway.

ER:255-56.

2. *The district court properly modeled its “without authorization” instruction on Brekka*

The district court properly instructed the jury on the meaning of “without authorization” under 18 U.S.C. § 1030.<sup>13</sup> In particular, the district court correctly

---

<sup>13</sup> Given Nosal’s acquiescence to the “without authorization” instruction at the jury-instructions hearing, *see* Part III.B.1, *supra*, Nosal may not have properly preserved an objection to the district court’s final instruction. *See Anderson*, 741 F.3d at 945-46. However, the Court need not decide whether plain-error review applies because Nosal’s claim fails under any standard.

stated that “[w]hether 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.” ER:255-56. This instruction accurately describes *Brekka*’s holding that “authorization” means “permission or power granted by an authority” and, under Section 1030, “depends on actions taken by the employer.”<sup>14</sup> *Brekka*, 581 F.3d at 1135. As discussed in Part I.B, *supra*, *Brekka* remains good law in this circuit, and the Court’s en banc opinion in this case did not disturb its holdings. Accordingly, the district court properly based its “without authorization” instruction on *Brekka*.

The district court also properly declined to instruct the jury that “[a] person accesses a computer without authorization when he circumvents technological access barriers.” ER:1083. This proposed instruction misstates the law because “the circumvention of technological access barriers” is not an element of any Section 1030 offense. *See* Part I.B.2.c, *supra*. Furthermore, any error was harmless because the evidence established that Christian and Jacobson did circumvent technological access barriers. Korn/Ferry employed password-protection to prevent outsiders from accessing its computers, and Christian and Jacobson circumvented that barrier by using Froehlich-L’Heureaux’s password.

---

<sup>14</sup> The rest of the court’s “without authorization” instruction, which Nosal does not specifically criticize, also mirrors *Brekka*. Compare ER:256 *with Brekka*, 581 F.3d at 1135.

See Part I.B.2.c.

**C. The Aiding-And-Abetting And Deliberate-Ignorance Instructions Were Correct**

*1. Background*

Before trial, the government and the district court each proposed jury instructions on aiding-and-abetting liability and deliberate ignorance. SER:7-8, 20-21. The proposed deliberate-ignorance instructions stated in part that the jury could find that Nosal acted knowingly if he: (1) “was aware of a high probability that, for example, co-conspirators” had committed a crime charged in Counts Two through Six, and (2) deliberately avoided learning the truth. SER:7, 21. Nosal objected to the government’s proposed deliberate-ignorance instruction on the ground that “[t]he facts alleged in the indictment do not permit a theory of deliberate ignorance.” SER:12. Nosal did not otherwise object to these proposed instructions. See SER:11-12; ER:1074-89.

At the jury-instructions hearing, Nosal argued that the deliberate-ignorance instruction should not apply to the conspiracy charged in Count One, and the district court revised the instruction to clarify that it applied only to Counts Two through Six. SER:182-83. Nosal then asked the court to remove the instruction’s reference to “co-conspirators,” and the court agreed. SER:183-84. Government counsel suggested replacing “co-conspirators” with the actual names of Nosal’s three co-conspirators, and when the court reiterated, “Put in the names of the three

people instead –,” Nosal’s counsel responded, “Right.” SER:184-85. The next day, Nosal raised an unrelated concern about the deliberate-ignorance instruction, and the court revised the instruction accordingly. SER:195-98. Nosal did not otherwise object to the court’s proposed aiding-and-abetting and deliberate-ignorance instructions. *See generally* SER:124-89.

Thereafter, the district court instructed the jury that to convict Nosal of aiding and abetting a particular crime, it had to find the following elements beyond a reasonable doubt: (1) the crime was committed by someone; (2) Nosal “knowingly and intentionally aided, counseled, commanded, induced, or procured that person to commit each element of the crime”; and (3) Nosal “acted before the crime was completed.” ER:260. The district court further instructed:

It is not enough that the defendant merely associated with the person committing the crime, or unknowingly or unintentionally did things that were helpful to that person, or was present at the scene of the crime. The evidence must show beyond a reasonable doubt the defendant acted with the knowledge and intention of helping that person commit the crime.

ER:260.

The district court also gave the deliberate-ignorance instruction, instructing the jury that it could find that Nosal acted “knowingly” with respect to Counts Two through Six if it found beyond a reasonable doubt that Nosal: (1) “was aware of a high probability that Becky Christian, Mark Jacobson, or Jacqueline Froehlich-

L’Heureaux 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.” ER:263-64.

After the verdict, Nosal moved for a new trial, arguing in part that he was entitled to a new trial on Counts Two through Four because of the inclusion of Froehlich-L’Heureaux’s name in the deliberate-ignorance instruction. ER:39-40. The district court concluded that Nosal had waived this objection and held that, in any event, the inclusion of Froehlich-L’Heureaux’s name in the instruction was not erroneous and did not warrant a new trial. ER:39-41.

2. *The district court’s instructions were consistent with Rosemond, and in any event, Nosal cannot satisfy the plain-error standard*

As discussed in Part I.B.3, *supra*, a defendant is guilty of aiding and abetting a crime only if he knew in advance that the crime was going to occur. *See Rosemond*, 134 S. Ct. at 1249-50. The district court’s instructions properly conveyed this requirement by advising the jury that it could convict Nosal on an aiding-and-abetting theory only if the government proved beyond a reasonable doubt that Nosal “knowingly and intentionally aided, counseled, commanded, induced or procured” someone else to commit the crime, and that Nosal did so

“before the crime was completed.” ER:260. Nosal did not object to these aiding-and-abetting instructions in the district court, nor does he challenge them now. *See* AOB:32-34, 51-52. Instead, Nosal argues that the district court’s deliberate-ignorance instruction allowed the jury to convict him of aiding and abetting a crime without finding that he had advance knowledge of the crime. *See id.* Because Nosal makes this argument for the first time on appeal, this Court’s review is for plain error. *See United States v. Kessi*, 868 F.2d 1097, 1102 (9th Cir. 1989). Nosal cannot satisfy any of the requirements of plain-error review.

To begin with, the deliberate-ignorance instruction did not undercut the aiding-and-abetting instruction’s advance knowledge and intent requirements. The deliberate-ignorance instruction provided the jury with additional guidance on how to determine whether Nosal acted “knowingly,” ER:263-64, but it did not alter the aiding-and-abetting instruction’s requirement that Nosal act knowingly and intentionally “before the crime was completed.” ER:260. Although Nosal suggests that the deliberate-ignorance instruction should have somehow repeated the advance-knowledge requirement for aiding and abetting, *see* AOB:32-33, the district court did not abuse its discretion, much less plainly err, by choosing to include this requirement only in the aiding-and-abetting instruction itself. *See United States v. Del Toro-Barboza*, 673 F.3d 1136, 1147 (9th Cir. 2012) (“So long as the instructions fairly and adequately cover the issues presented, the judge’s



formulation of those instructions or choice of language is a matter of discretion.”).

Nor did the deliberate-ignorance instruction allow the jury to convict Nosal of aiding and abetting a crime based on conduct that was only reckless, rather than knowing and intentional. *See* AOB:33-34. Deliberate ignorance “is categorically different from negligence or recklessness” because “[a] willfully blind defendant is one who took *deliberate* actions to avoid confirming suspicions of criminality.” *United States v. Heredia*, 483 F.3d 913, 918 n.4 (9th Cir. 2007) (en banc) (emphasis in original). This Court therefore allows district courts to instruct juries that a defendant acts “knowingly” when he “does not possess positive knowledge only because he consciously avoided it.” *Id.* at 918. Furthermore, the district court instructed that Nosal would be guilty of aiding and abetting a crime only if he acted with the “intention of helping that person commit the crime.” ER:260. This instruction squarely precluded the jury from convicting Nosal on an aiding-and-abetting theory based on conduct that was merely reckless or otherwise unintentional.

Finally, Nosal cannot show that the deliberate-ignorance instruction affected his substantial rights or seriously affected the fairness, integrity, or public reputation of judicial proceedings. *See Anderson*, 741 F.3d at 945. The government presented substantial evidence that Nosal had advance knowledge of the crimes charged in Counts Two through Six. *See* Parts I.B.3 & I.C, *supra*.

Furthermore, Nosal does not dispute that the trial evidence established that he was liable for Counts Two through Six under *Pinkerton*. *Cf.* Part I.B.3, *supra*.

Accordingly, any error in the deliberate-ignorance instruction did not affect Nosal's substantial rights because there is no "reasonable probability that the error affected the outcome of the trial." *United States v. Marcus*, 560 U.S. 258, 262 (2010).

3. *The district court did not plainly err in including Froehlich-L'Heureaux's name in the deliberate-ignorance instruction*

Nosal also claims that the district court erred by including Froehlich-L'Heureaux's name in the deliberate-ignorance instruction. *See* AOB:34. Specifically, Nosal contends that this aspect of the instruction improperly allowed the jury to convict him on Counts Two through Four if he believed that Froehlich-L'Heureaux, rather than Christian or Jacobson, accessed Korn/Ferry's computers on the dates charged in those counts. *See id.* Because Nosal did not raise this objection before the jury retired to deliberate, this Court's review is for plain error. *See Kessi*, 868 F.2d at 1102. Nosal has not shown error, much less error that was plain and affected his substantial rights.

Read as a whole, the instructions did not allow the jury to convict Nosal of aiding and abetting the Section 1030 offenses charged in Counts Two through Four if it found that Nosal believed that Froehlich-L'Heureaux, rather than Christian or Jacobson, had accessed Korn/Ferry's computers without authorization. The

aiding-and-abetting instructions required the jury to find that “someone” committed the relevant offense and that Nosal “knowingly and intentionally aided, counseled, commanded, induced or procured *that person* to commit each element of the crime.” ER:260 (emphasis added). Because Froehlich-L’Heureaux was an authorized user of Korn/Ferry’s computers during the relevant period, ER:707-08, the instructions did not permit the jury to find that she was the “someone” who committed the crimes charged in Counts Two through Four. *See* ER:255-56 (instructions on Section 1030(a)(4) elements and authorized access); Part II.B, *supra*.

Accordingly, the district court did not err or plainly err in including Froehlich-L’Heureaux’s name in the deliberate-ignorance instruction. Furthermore, even if there were error, it did not affect Nosal’s substantial rights or seriously affect the fairness, integrity, or public reputation of judicial proceedings. *See Anderson*, 741 F.3d at 945. Both Christian and Jacobson testified that they committed the conduct charged in Counts Two through Four, and Froehlich-L’Heureaux confirmed that she allowed both of them to use her Korn/Ferry account to access Korn/Ferry’s computers. ER:312, 314, 362-69, 373-79, 387-91, 500-02; SER:114-15. Furthermore, the evidence established that Froehlich-L’Heureaux was authorized to access Korn/Ferry’s computers until August 2005,

ER:707-08, and the government never argued otherwise.<sup>15</sup> Given this evidence, as well as Nosal's independent liability for Counts Two through Four under *Pinkerton*, there is no reasonable probability that the jury convicted Nosal on these counts because it believed that Froehlich-L'Heureaux had gained unauthorized access to Korn/Ferry's computer systems and that Nosal had aided and abetted her efforts.

#### **D. The Trade-Secrets Conspiracy Instruction Was Correct**

##### *1. Background*

Count One of the second superseding indictment charged Nosal with violating 18 U.S.C. § 371 by conspiring to misappropriate, receive, possess, and transmit trade secrets and to gain unauthorized access to a protected computer. ER:1171. The "Manner and Means of the Conspiracy" section of the indictment further alleged that Nosal and his co-conspirators took "trade secrets" from Korn/Ferry's computer system. ER:1171-72.

Before trial, the district court held that the government "need not prove the existence of an actual trade secret" to prove that Nosal conspired to commit a trade-secrets offense. SER:18. Nosal objected to this ruling. ER:1084-88. Nosal further argued that the district court would constructively amend the indictment by instructing the jury that it could convict him of trade-secrets conspiracy without

---

<sup>15</sup> During opening statements, government counsel told the jury that Froehlich-L'Heureaux "was authorized to access the computer system." SER:44.

finding the existence of actual trade secrets. ER:70. The district court disagreed. ER:71-73.

Thereafter, the district court instructed the jury that, for the trade-secrets conspiracy charged in Count One, “the government need not prove the existence of actual trade secrets and that the defendant knew that the information in question was a trade secret.” ER:261-62. The district court instructed that, as to those conspiracy charges, the government must instead prove that Nosal “firmly believed that certain information constituted trade secrets.” ER:262.

2. *The district court properly instructed the jury that it could find Nosal guilty of trade-secrets conspiracy even if the government did not prove the existence of a trade secret*

The district court correctly instructed the jury that it could find Nosal guilty of conspiring to commit a trade-secrets offense, as charged in Count One, even if the government did not prove that the information Nosal conspired to misappropriate, receive, possess, and transmit was, in fact, a trade secret. ER:261-62. This instruction is consistent with this Court’s precedent on conspiracy and with other circuits’ law on trade-secrets conspiracy.

As this Court has explained, “a conspiracy conviction may be sustained even where the goal of the conspiracy is impossible.” *United States v. Fiander*, 547 F.3d 1036, 1042 (9th Cir. 2008). Based on this principle, this Court has repeatedly upheld conspiracy convictions where a defendant conspired to commit a crime that

was, for reasons unknown to him, impossible to complete. *See, e.g., United States v. Rodriguez*, 360 F.3d 949, 957 (9th Cir. 2004) (upholding a defendant’s conviction for conspiracy to steal non-existent drugs from non-existent narcotics traffickers and noting that “[i]mpossibility is not a defense to the conspiracy charge”); *United States v. Everett*, 692 F.2d 596, 599-601 (9th Cir. 1982) (describing cases that reject the doctrine of legal impossibility as a defense to a conspiracy charge).

Although the Court has yet to apply this principle in a trade-secrets-conspiracy case, at least three other circuits have concluded that a defendant may be guilty of conspiring to commit a trade-secrets offense involving information that was not, in fact, a trade secret, as long as the defendant believed that the information was a trade secret. *See United States v. Yang*, 281 F.3d 534, 544 (6th Cir. 2002) (“The fact that the information they conspired to obtain was not what they believed it to be does not matter.”); *United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000) (“The relevant question to determine whether a conspiracy existed was whether Martin *intended* to violate the statute.”); *United States v. Hsu*,<sup>16</sup> 155 F.3d 189, 204 (3d Cir. 1998) (“[P]roof that the defendants sought to steal actual trade secrets is not an element of the crimes of attempt or conspiracy under

---

<sup>16</sup> Nosal argues that *Hsu*’s holding applies to defendants who are charged only with attempt and conspiracy, but not to defendants charged with attempt, conspiracy, and “actual theft of trade secrets.” AOB:40 (quoting *Hsu*, 155 F.3d at 194). *Hsu*’s holding is not so limited. *See Hsu*, 155 F.3d at 203-04.

[Section 1832.]”); *cf. United States v. Liu*, 716 F.3d 159, 170 (5th Cir. 2013) (citing *Yang*, *Martin*, and *Hsu* for the proposition that “the relevant inquiry in a conspiracy case . . . is whether the defendant entered into an agreement to steal, copy, or receive information that he *believed* to be a trade secret”).

These holdings do not render the statutory definition of “trade secrets” superfluous, as Nosal now claims. *See* AOB:40. To begin with, a jury must always find the existence of a trade secret to convict a defendant of a completed trade-secrets offense under 18 U.S.C. § 1832(a)(1)-(3). Moreover, even when a defendant is charged only with attempting or conspiring to commit a trade-secrets offense, the government must still prove that the defendant believed that the information in question was a trade secret. *See, e.g., Yang*, 281 F.3d at 543-44; *Martin*, 228 F.3d at 13. The district court’s instructions reflected this requirement. *See* ER:261-62.

For all of these reasons, the district court’s instructions on trade-secrets conspiracy correctly described the elements of this offense.

3. *The trade-secrets conspiracy instruction did not constructively amend the indictment*

A constructive amendment of an indictment occurs when the prosecutor or a court alters the charging terms of the indictment, either literally or in effect, after the grand jury has last passed on them. *United States v. Wilbur*, 674 F.3d 1160, 1177-78 (9th Cir. 2012). But this doctrine applies only when the alterations

broaden the indictment. *Id.* at 1178; *see also United States v. Miller*, 471 U.S. 130, 138-40 (1985). Accordingly, when the jury instructions narrow the indictment's charges by requiring the government to prove only some of the conduct alleged in the indictment, there is no impermissible constructive amendment. *See Miller*, 471 U.S. at 138-40; *Wilbur*, 674 F.3d at 1178.

In this case, Nosal's constructive-amendment claim amounts to a complaint that the jury instructions narrowed the indictment. Specifically, Nosal bases his constructive-amendment claim on the indictment's allegations that Nosal and his co-conspirators took "trade secrets" from Korn/Ferry's computer system. *See AOB:37-39*. Nosal argues that, in light of these allegations, the district court should have instructed the jury that it could convict Nosal of trade-secrets conspiracy only if it found that the information Nosal conspired to misappropriate, receive, possess, or transmit was, in fact, a trade secret. *See AOB:38-39*. As discussed in the previous subsection, the district court correctly declined to give this instruction. For the same reasons, the allegations in the indictment that form the basis of Nosal's constructive-amendment claim are simply "superfluously specific language describing alleged conduct irrelevant to the defendant's culpability under the applicable statute." *United States v. Ward*, 747 F.3d 1184, 1191 (9th Cir. 2014). This Court has declined to find a constructive amendment based on this category of allegations, and it should follow the same path here. *See*



*id.* (citing cases).

### **III. THE DISTRICT COURT'S EVIDENTIARY RULINGS ABOUT THE NONCOMPETE PROVISIONS WERE PROPER**

#### **A. Background**

When Nosal decided to leave Korn/Ferry in 2004, he entered into two agreements with Korn/Ferry that contained noncompete provisions. *See* Statement of Facts C.1, *supra*. Before trial, the district court ruled that either party could introduce “evidence of a person’s subjective belief about the validity of the non-compete clause,” provided that the evidence was relevant and otherwise admissible. ER:136. The court excluded evidence and argument about “whether the noncompete clause was actually legal and enforceable.” ER:136. The court reasoned that “[w]hether the agreement is in fact valid is irrelevant to this case and thus lacks probative value,” and it noted that “a trial on actual legality would result in a mini-trial on a collateral issue which could require resolution of facts by the jury,” thereby causing “confusion and inefficiency.” ER:135. The court also expressed concern that “focusing substantial trial time on the validity vel non of the non-compete agreement may unduly emphasize a wrong committed by Defendant and raise concerns under F.R.E. 403 and F.R.E. 404(b).” ER:135. In addition, the court ordered the government not to argue that Nosal’s breach of the agreement was probative of his motive or intent to defraud. ER:136.

At the beginning of trial, the district court told the jury that it would hear testimony that Nosal had entered into two agreements with Korn/Ferry that each included a “noncompetition clause” and that “different individuals held different beliefs about whether this agreement was fair, legal, and enforceable.” SER:40-41.

The court then instructed the jury:

You may consider this testimony only as it helps to explain the actions of those witnesses. Whether or not the agreement was legal and enforceable is not relevant to the issues in this case. Additionally, any evidence of whether Mr. Nosal did or did not comply with the terms of this clause is not relevant to the question of whether he is guilty of the crimes charged in this case.

SER:41. During the government’s case, when Korn/Ferry general counsel Peter Dunn began to testify about the noncompete provisions, the district court again reminded the jury that the validity or enforceability of these provisions was not an issue for the jury to decide. ER:947-48.

Thereafter, Dunn testified that in March 2005, he and others at Korn/Ferry received an email from a person using the name “Sandra Horn” who claimed that Nosal was “conducting searches for Korn/Ferry clients in Silicon Valley.”

ER:981-84. This email stated, “Perhaps you could save a few dollars on your agreement with him; alternatively, you may just want to go ahead and sue.”

SER:263. When the government introduced this email chain, the district court instructed the jury, “[T]his exhibit is admitted for the purpose of 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." ER:982. Dunn then testified that, as a result of this email, he initiated an internal investigation that ultimately uncovered the conspiracy to take information from Korn/Ferry. ER:984-96; *see* ER:752-60 (additional testimony about internal investigation).

Dunn further testified that, as of July 2005, Korn/Ferry believed that Nosal was "in breach" of his agreements with Korn/Ferry. ER:1001-03. On cross-examination, Nosal's counsel asked Dunn whether, in subsequent civil litigation, Nosal had taken the position "that under California law, noncompetition agreements are void and illegal." ER:1024. Dunn confirmed that he had. ER:1024-25. Nosal's counsel then asked Dunn whether noncompetition agreements were illegal in some states, and the district court sustained the government's relevance objection. ER:1025.

Thereafter, Christian testified that Nosal was "not allowed to conduct searches outside of Korn/Ferry once he left" and that he used her as a "conduit" for conducting such search work. ER:342-43. Christian further testified that, during his work with Christian & Associates, Nosal sometimes used the name "David Nelson" because "he didn't want people to know that he was conducting search work, which would breach his contract with Korn/Ferry." ER:354-55.

In its final instructions, the district court instructed the jury as follows:

You have heard testimony from some witnesses that Mr. Nosal entered into a noncompete 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 as 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.

ER:247-48. Thereafter, during the government's rebuttal argument, government counsel asked the jury why Nosal had hidden his identity by using the name "David Nelson." ER:226. Counsel then stated, "The fact that this defendant chose to hide his identity shows his intent. And his intent was to conspire with [Christian], with [Jacobson], and with [Froehlich-L'Heureaux] to . . . steal information from Korn/Ferry to get a jump, a head start on his business." ER:226. Nosal did not object to these statements. ER:226.

## **B. Standard Of Review**

The Court reviews a district court's evidentiary rulings for abuse of discretion and its underlying factual determinations for clear error. *United States v. Lukashov*, 694 F.3d 1107, 1114 (9th Cir. 2012). However, when a defendant fails to object to an evidentiary ruling, the Court's review is for plain error. *United*

*States v. Kahre*, 737 F.3d 554, 577 n.18 (9th Cir. 2013).

**C. The District Court’s Evidentiary Rulings Were Proper**

The district court properly allowed both parties to introduce “evidence of a person’s subjective belief about the validity of the noncompete clause,” provided that the evidence was relevant and otherwise admissible. ER:136. This ruling allowed Nosal to present evidence that he believed that Korn/Ferry had subjected him to an illegal contract. *See* ER:1024-25. Furthermore, the district court ensured that Nosal suffered no unfair prejudice from Dunn’s and Christian’s statements about Nosal breaching his Korn/Ferry agreements because the court instructed the jury to disregard this testimony.<sup>17</sup> ER:247-48. *See United States v. Padilla*, 639 F.3d 892, 897 (9th Cir. 2011) (“[W]e . . . presume that juries follow instructions given to them throughout the course of the trial.”).

The district court also properly exercised its discretion when it barred the parties from introducing evidence and argument about whether the noncompete provisions were legal and enforceable under California law. The legal status of these provisions was irrelevant because none of the criminal statutes charged in this case include exemptions from criminal liability for defendants who entered into illegal contracts with the victims of their crimes. Indeed, Nosal does not explain how the actual legality of the noncompete provisions was probative in any

---

<sup>17</sup> Although Nosal claims that the “Sandra Horn” emails also accused him of breach, *see* AOB:55, the emails are not so specific. *See* SER:281-83.

way. *See* AOB:55-56. Because the legality of the noncompete provisions shed no light on the issues in Nosal's criminal trial, the district court properly prohibited the parties from distracting the jury with this irrelevant and confusing contract-law issue. *See* Fed. R. Evid. 402, 403.

Finally, the district court properly allowed government counsel to argue in rebuttal that Nosal's use of the name "David Nelson" revealed his criminal intent.<sup>18</sup> Despite Nosal's claims, these statements did not violate the court's order precluding the government from arguing that Nosal's breach of the noncompete provisions was probative of his motive or intent to defraud. *See* ER:136. These statements did not even mention Nosal's Korn/Ferry agreements, much less argue that Nosal had breached their noncompete provisions and that the jury should draw inferences from such a breach. Furthermore, even if the government had somehow argued that Nosal's breach was relevant to his criminal intent, the jury would have disregarded that argument because the district court's instructions stated that evidence that Nosal breached the noncompete provisions was irrelevant to his guilt. ER:247-48. *See Padilla*, 639 F.3d at 897.

---

<sup>18</sup> Because Nosal did not object to this argument at the time, the Court reviews this claim for plain error. It fails under any standard.

#### **IV. THE DISTRICT COURT'S RESTITUTION ORDER WAS PROPER**

##### **A. Background**

Before Nosal's sentencing, the law firm O'Melveny & Myers LLP ("O'Melveny") submitted a declaration to the district court which explained that, from July 2005 through July 2013, O'Melveny had represented Korn/Ferry in connection with the criminal investigation and prosecution of Nosal. SER:203. The declaration provided a general description of O'Melveny's work in this criminal case and a monthly breakdown of the resulting attorneys' fees, which then totaled \$939,406.25. SER:204-06. The following month, O'Melveny submitted a supplemental declaration attaching 76 exhibits of billing records, totaling hundreds of pages and containing approximately 2000 entries, that described these fees in more detail.<sup>19</sup> ER:10; SER:208.

At Nosal's sentencing hearing, the district court concluded that, for purposes of USSG § 2B1.1, Korn/Ferry suffered \$46,907.88 in "actual loss" because of Nosal's actions. ER:14. The district court deferred its restitution determination to a later date, and at subsequent hearing, it held that Nosal's restitution amount could exceed his Section 2B1.1 loss calculation. ER:183; SER:210-11. The court further held that the restitution amount should include costs Korn/Ferry incurred in connection with the investigation and prosecution of Nosal's criminal case,

---

<sup>19</sup> Because these records are voluminous and remain under seal, the government has not included them in the SER.

including attorneys' fees, provided that Nosal's conduct was a proximate cause of those losses. SER:211-13. The court and the parties also agreed that the restitution order should not require Nosal to reimburse Korn/Ferry for attorneys' fees incurred in connection with the government's interlocutory appeal in his case. SER:211-12, 214, 216.

In a subsequent order, the district court ordered Nosal to pay \$827,983.25 in restitution to Korn/Ferry. ER:13. This amount represented \$27,400 for costs that Korn/Ferry incurred in responding to Nosal's actions; \$204,825 for the value of the time that Korn/Ferry employees spent participating in the criminal investigation and prosecution; and \$595,758.25 for attorneys' fees that Korn/Ferry incurred in aid of the criminal investigation and prosecution. ER:3-12. With respect to the attorneys' fees, the district court explained that it had "carefully reviewed" O'Melveny's billing records and that "most but not all" of these records were sufficiently detailed to allow the court to confirm that O'Melveny's fees were "reasonable and necessary to the government's investigation and prosecution." ER:10-11. Although the government had asked the district court to order restitution for \$964,929.65 in attorneys' fees, the court reduced this amount to \$595,758.25 because it concluded that 10 percent of the fees were not reasonably necessary and 25 percent were the result of staffing inefficiencies. ER:11-13.



**B. Standard Of Review**

This Court reviews de novo the legality of a restitution order and reviews for clear error the factual findings supporting the order. *United States v. Luis*, 765 F.3d 1061, 1065 (9th Cir. 2014). If the restitution order is within the bounds of the statutory framework, the Court reviews the order for abuse of discretion. *Id.*

**C. The District Court Properly Concluded That A Restitution Award May Be Greater Than The Loss Calculation Under USSG § 2B1.1**

The district court correctly concluded that Nosal's restitution amount could exceed his loss amount under USSG § 2B1.1. Under Section 2B1.1, a loss calculation must exclude "costs incurred by victims primarily to aid the government in[] the prosecution and criminal investigation of an offense." USSG § 2B1.1 cmt. 3(D)(ii). By contrast, under the Mandatory Victim Restitution Act ("MVRA"), 18 U.S.C. § 3663A, a restitution award must reimburse the victim for "expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense." 18 U.S.C. § 3663A(b)(4). In other words, Nosal's Section 2B1.1 loss calculation may not include the \$800,583.25 that Korn/Ferry incurred as a result of its participation in this criminal investigation and prosecution, but Nosal's restitution order must include this amount. The district court correctly recognized these differing requirements, and its restitution order was therefore proper because it required Nosal to reimburse Korn/Ferry for the actual losses it suffered as a result of his

conduct.

Furthermore, the restitution order did not contravene this Court's decision in *United States v. Stoddard*, 150 F.3d 1140 (9th Cir. 1998), as Nosal now claims. In *Stoddard*, the district court ordered the defendant to pay \$116,223 in restitution, an amount that represented the profits the defendant had accrued as a result of his crimes. *Id.* at 1147-48 (Ferguson, J., dissenting). Because the victim's actual losses were only \$30,000, however, this Court vacated the higher restitution order and ordered the district court to reduce the restitution award to \$30,000. *Id.* at 1145-47. In so doing, the Court concluded that "[r]estitution can only be based on actual loss." *Id.* at 1147.

But *Stoddard* did not hold that, for purposes of restitution, "actual loss" excludes expenses that a victim incurs because of its participation in the criminal investigation and prosecution. *See id.* Nor did *Stoddard* suggest that district courts must use USSG § 2B1.1's definition of loss when calculating restitution, rather than complying with the provisions of the MVRA. *See id.* Indeed, this Court has since rejected that notion, explaining that the Sentencing Guidelines and the MVRA serve different purposes and employ different loss-calculation schemes. *See United States v. Gordon*, 393 F.3d 1044, 1052 n.6 (9th Cir. 2004). Furthermore, *Stoddard* did not implicate the MVRA because the criminal conduct in *Stoddard* occurred in 1990 and earlier, before Congress passed either the MVRA

or the Victim and Witness Protection Act provision that most closely resembles 18 U.S.C. § 3663A(b)(4). *Compare Stoddard*, 150 F.3d at 1142-43, and 18 U.S.C. § 3663 (1990) (VWPA), with 18 U.S.C. § 3663(b)(4) (2015).

**D. The District Court Properly Ordered Nosal To Reimburse Korn/Ferry For Some Of Its Attorneys' Fees**

The district court properly ordered Nosal to reimburse Korn/Ferry for approximately 62 percent of the attorneys' fees that Korn/Ferry reported incurring as a result of its participation in this criminal case. As this Court has explained, a private party may be entitled to restitution for attorneys' fees that it incurs "as a direct and foreseeable result of the defendant's wrongful conduct." *Gordon*, 393 F.3d at 1057 (upholding \$1,038,477 restitution award to Cisco for investigation costs, including attorneys' fees). Here, the district court "carefully reviewed" approximately 2000 billing entries from O'Melveny and determined that \$595,758.25 of O'Melveny's fees were "reasonable and necessary to the government's investigation and prosecution." ER:10-12.

Although Nosal argues that the district court should have ordered restitution only for attorneys' fees that Korn/Ferry incurred "in the immediate aftermath" of discovering Nosal's crimes, AOB:62-63, the MVRA includes no such temporal restriction. *See* 18 U.S.C. § 3663A(b)(4). Nor did *Gordon* impose a time restriction on reimbursable costs, as Nosal now suggests. *See* AOB:62-63. In fact, *Gordon* noted that "[t]his circuit has adopted a *broad* view of the restitution

authorization” in Section 3663A(b)(4). 393 F.3d at 1056-57 (emphasis in *Gordon*).

Nosal also provides no evidentiary support for his contention that the district court’s restitution order requires him to pay attorneys’ fees that Korn/Ferry incurred in civil litigation with Nosal. Indeed, this claim is contrary to O’Melveny’s submissions to the district court, which clarify that Korn/Ferry has not sought restitution for the attorneys’ fees resulting from the civil litigation. SER:202-04.

Finally, Nosal has identified no basis for concluding that the district court abused its discretion or clearly erred in concluding that \$595,758.25 of Korn/Ferry’s attorneys’ fees were “reasonable and necessary to the government’s investigation and prosecution.” ER:10-12. Nosal’s only specific complaint is that Korn/Ferry’s restitution request included attorneys’ fees for O’Melveny’s review of the en banc opinion in this case. AOB:63. As discussed above, however, the district court declined to require Nosal to reimburse Korn/Ferry for \$369,171.40 of the attorneys’ fees it reported. In so doing, the court announced that the restitution award would not include “fees relating to attorney review of filings, orders, and press coverage.” ER:11. Furthermore, at the hearing on February 12, 2014, the district court stated that Nosal should not be required to reimburse Korn/Ferry for costs associated with the interlocutory appeal. SER:211-12, 216. Accordingly,

Nosal cannot and does not contend that the district court's restitution order actually requires him to reimburse Korn/Ferry for O'Melveny's review of the en banc opinion. *See* AOB:63.

### CONCLUSION

For the reasons set forth above, this Court should affirm Nosal's convictions and judgment.

Dated: March 2, 2015

MELINDA HAAG  
United States Attorney

BARBARA J. VALLIERE  
Assistant United States Attorney  
Chief, Appellate Division

KYLE F. WALDINGER  
MATTHEW A. PARRELLA  
Assistant United States Attorneys

Respectfully submitted,

LESLIE R. CALDWELL  
Assistant Attorney General

SUNG-HEE SUH  
Deputy Assistant Attorney General

/s/ JENNY C. ELLICKSON  
JENNY C. ELLICKSON  
Attorney, Appellate Section  
Criminal Division  
U.S. Department of Justice  
950 Pennsylvania Ave. NW, Rm. 1264  
Washington, DC 20530  
Tel. (202) 305-1674  
jenny.ellickson@usdoj.gov

Attorneys for Plaintiff-Appellee  
UNITED STATES OF AMERICA

## STATEMENT OF RELATED CASES

The following case previously heard in this Circuit is related within the meaning of Ninth Circuit Rule 28-2.6 because it arose out of the same case in the district court: *United States v. Nosal*, No. 10-10038.

Dated: March 2, 2015

/s/ JENNY C. ELLICKSON  
JENNY C. ELLICKSON  
Attorney, Appellate Section  
Criminal Division  
U.S. Department of Justice

## CERTIFICATE OF COMPLIANCE

I certify that (check appropriate option):

- This brief complies with the enlargement of brief size permitted by Ninth Circuit Rule 28-4. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). This brief is \_\_\_\_\_ words, \_\_\_\_\_ lines of text or \_\_\_\_\_ pages, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), if applicable.
- This brief complies with the enlargement of brief size granted by court order dated \_\_\_\_\_. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6). This brief is \_\_\_\_\_ words, \_\_\_\_\_ lines of text or \_\_\_\_\_ pages, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), if applicable.
- This brief is accompanied by a motion for leave to file an oversize brief pursuant to Circuit Rule 32-2 and is 16,500 words, \_\_\_\_\_ lines of text or \_\_\_\_\_ pages, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), if applicable.
- This brief is accompanied by a motion for leave to file an oversize brief pursuant to Circuit Rule 29-2(c)(2) or (3) and is \_\_\_\_\_ words, \_\_\_\_\_ lines of text or \_\_\_\_\_ pages, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii), if applicable.
- This brief complies with the length limits set forth at Ninth Circuit Rule 32-4. The brief's type size and type face comply with Fed. R. App. P. 32(a)(5) and (6).

Dated: March 2, 2015

/s/ JENNY C. ELLICKSON  
JENNY C. ELLICKSON  
Attorney, Appellate Section  
Criminal Division  
U.S. Department of Justice

## CERTIFICATE OF SERVICE

I, Hui Chen, certify that I am an employee of the Office of the United States Attorney, Northern District of California, a person over 18 years of age and not a party to the within action. I certify that on March 2, 2015, I electronically submitted the

- **Brief for the United States as Appellee**
- **Motion to File an Oversized Brief**
- **Government's Supplemental Excerpts of Record (Volume 1 of 2)**

in the case of *United States v. David Nosal*, Nos. 14-10037 & 14-10275, with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system for the above documents.

I also certify that I served **Volume 2 of the Supplemental Excerpts of Record**, submitted under seal to the Court, and **Motion to Seal**, to the party or parties listed below, by enclosing them in a sealed envelope to be delivered via Federal Express service.

Dennis P. Riordan, Esq.  
Donald M. Horgan, Esq.  
Riordan & Horgan  
523 Octavia Street  
San Francisco, CA 94102

Dated: March 2, 2015

/s/ Hui Chen

Hui Chen, Legal Assistant



# ADDENDUM

TABLE OF CONTENTS

18 U.S.C. § 1030 (2005) .....	82
18 U.S.C. § 1832 (2005) .....	90
18 U.S.C. § 1839 (2005) .....	91

**18 U.S.C.A. § 1030 (2005)**

United States Code Annotated

Title 18. Crimes and Criminal Procedure (Refs & Annos)

Part I. Crimes

Chapter 47. Fraud and False Statements (Refs & Annos)

**§ 1030. Fraud and related activity in connection with computers**

**(a)** Whoever—

**(1)** having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

**(2)** intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

**(A)** information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

**(B)** information from any department or agency of the United States;  
or

**(C)** information from any protected computer if the conduct involved an interstate or foreign communication;

**(3)** intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that

department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

**(4)** 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;

**(5)(A)(i)** knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

**(ii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

**(iii)** intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

**(B)** by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

**(i)** loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

**(ii)** the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

**(iii)** physical injury to any person;

**(iv)** a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [Footnote Omitted]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

**(B)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

**(i)** the offense was committed for purposes of commercial advantage or private financial gain;

**(ii)** the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

**(iii)** the value of the information obtained exceeds \$5,000; and

**(C)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

**(3)(A)** a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

**(B)** a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [Footnote Omitted] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

**(4)(A)** except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

**(B)** a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

**(C)** except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under

subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

**(5)(A)** if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

**(B)** if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

**(d)(1)** The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

**(2)** The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

**(3)** Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

**(e)** As used in this section—

**(1)** the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

**(2)** the term “protected computer” means a computer—

**(A)** exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct

constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term “financial institution” means—

(A) an institution, [Footnote Omitted] with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;



(5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this

section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

**(h)** The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

**18 U.S.C.A. § 1832 (2005)**

United States Code Annotated

Title 18. Crimes and Criminal Procedure (Refs & Annos)

Part I. Crimes

Chapter 90. Protection of Trade Secrets

**§ 1832. Theft of trade secrets**

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed 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) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(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) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000.

**18 U.S.C.A. § 1839 (2005)**

United States Code Annotated

Title 18. Crimes and Criminal Procedure (Refs & Annos)

Part I. Crimes

Chapter 90. Protection of Trade Secrets

**§ 1839. Definitions**

As used in this chapter—

(1) the term “foreign instrumentality” means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) the term “foreign agent” means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) 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; and

(4) the term “owner”, with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.