DAVID L. ANDERSON (CABN 149604)
United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

COLIN C. SAMPSON (CABN 249784)
450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
FAX: (415) 436-7234
Colin.Sampson@usdoj.gov

JOHN C. DEMERS
Assistant Attorney General
National Security Division

BENJAMIN J. HAWK (NJBN 030232007)
Trial Attorney, National Security Division
950 Pennsylvania Avenue NW
Washington, DC 20530-0001
Telephone: (202) 307-5176
Benjamin.Hawk@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. AHMAD ABOUAMMO, Defendant.	Case No. CR 19-621 EMC UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS FOR FAILURE TO STATE OFFENSE, ECF. NO. 84 Date: January 6, 2021 Time: 2:30 p.m. Courtroom: 5, 17th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

The government respectfully submits its Opposition to Defendant Ahmad Abouammo's Motion to Dismiss[1] Counts Four through Twenty-Three, asserting that the Superseding Indictment fails to state an offense as to those counts. *See* Dkt. No. 8. The Superseding Indictment alleges facts that satisfy each of the crimes charged related to Defendant's use of his employment at Twitter, Inc. to commit fraud on behalf of the Saudi Arabian government and enrich himself. Rather than accept the allegations in the First Superseding Indictment (Dkt. 53) as true for purposes of the Motion, Defendant repeatedly disputes the allegations. For the reasons that follow, Defendant's Motion should be denied.

I. BACKGROUND FACTS AND PROCEDURAL HISTORY

A. The Charges Against Defendant Abouammo

On November 5, 2019, a Complaint was issued charging Defendant Abouammo and two co-defendants – Ali Alzabarah and Ahmed Almutairi – with acting as agents of a foreign government without notifying the Attorney General, in violation of 18 U.S.C. § 951. Dkt. 1 ("Complaint"). Defendant Abouammo also was charged with falsification of records, in violation of 18 U.S.C. § 1519. *Id.* Defendant Abouammo was arrested on the same day. Warrants have been issued for the arrests of Defendants Alzabarah and Almutairi, who are believed to be in Saudi Arabia.

On November 19, 2019, the Grand Jury returned an Indictment, which charged the same offenses alleged in the Complaint. Dkt. 13. Defendant Abouammo was further charged with falsification of records. *Id*. On April 7, 2020, after the Grand Jury was suspended due to COVID-19, the government filed a Superseding Information, charging the defendants with the same counts from the Indictment, as well as one count of conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and fifteen substantive counts of wire fraud, in violation of 18 U.SC. §§ 1343 and 1346. Dkt. 42 ("Superseding Information"). Defendant Abouammo was also charged with three counts of international money laundering, in violation of 18 U.S.C. § 1956(a)(2)(B)(i). *Id.* On July 28, 2020, after the Grand Jury resumed in limited capacity, it returned a Superseding Indictment, charging the same offenses alleged in the Superseding Information. Dkt. 53 ("Superseding Indictment").

//

[1] The government will cite to the page number on the "ECF" header stamped at the top of each page of Defendant's Motion (hereafter "Def. Mot.").

B. Overview of the Fraud Schemes

As alleged in the Superseding Indictment, between approximately November 2014 and March 2016, the Kingdom of Saudi Arabia and its Royal Family, who hold most of the country's governmental posts, sought to identify the users of certain Twitter accounts that posted information critical of, or embarrassing to, the Saudi government and members of the Royal Family, including "Saudi Royal Family Member-1." *See* Superseding Indictment ¶¶ 8, 22. To carry out this scheme, "Foreign Official-1" and Defendant Almutairi, both of whom were closely associated with and performed work for Saudi Royal Family Member-1, secretly recruited Defendants Abouammo and Alzabarah, both of whom worked for Twitter, to access proprietary and confidential Twitter information. *See id.* ¶¶ 9, 10, 17, 21. Such protected Twitter information included user-provided names and birthdates, device identifiers, relationships, phone numbers, internet protocol ("IP") addresses and session histories, among other things, all of which could have been used by the Saudi government to identify and locate the individuals behind the accounts. *See id.* ¶ 17. During the course of the scheme, while acting beyond their job duties and contrary to Twitter's policies, Defendants Abouammo and Alzabarah used their access privileges as employees and fiduciaries of Twitter, to obtain confidential Twitter-user data for the Saudi government in exchange for gifts, cash payments, and promises of future employment. *See id.* ¶¶ 21, 23-24.

C. Defendants Abouammo and Abzabarah Owed a Fiduciary Duty to Twitter

Twitter, Inc. is headquartered in the Northern District of California and operates a social-networking website. *See id.* ¶ 4. As employees of Twitter, Defendants Abouammo and Alzabarah agreed to abide by Twitter's policies. *See id.* ¶¶ 14-15. As part of their confidentiality agreements they affirmed a relationship of confidence and trust between themselves and Twitter with respect to any information of a confidential or secret nature that Twitter disclosed to them related to its business. *See id.* ¶ 14. Those agreements further required the defendants to keep and hold all proprietary information in strict confidence and trust, including Twitter's customer lists and data, and forbid them from disclosing such information without Twitter's express written consent or using it for any other business or employment. *See id.* ¶ 14. Additionally, Twitter's security policies, which the defendants acknowledged reading and understanding, prohibited them from sharing Twitter's confidential user data with third parties without approval. *See id.* ¶ 15. While the defendants had access to Twitter-user data,

their job duties did not involve a need to access such private information, and doing so was a reportable violation of Twitter's policies. *See id.* ¶ 18.

In addition to agreeing to protect Twitter's proprietary and confidential information, Defendants Abouammo and Alzabarah agreed to abide by Twitter's gift policy. *See id.* ¶ 16. That policy required the defendants to notify their managers and the vice president of human resources of any gifts exceeding $100 in value before returning them. *See id.*

D. Allegations Specific to Defendant Abouammo

In furtherance of the scheme, Foreign Official-1 compensated Defendant Abouammo with valuable gifts and cash payments for his access to confidential Twitter-user data that was of interest to the Saudi government. *See id.* ¶ 26. Specifically, on December 5, 2014, during a meeting in London, England, Foreign Official-1 provided Defendant Abouammo with a luxury watch worth at least $20,000, which Defendant Abouammo concealed from Twitter, contrary to Twitter's gift disclosure policy. *See id.* ¶¶ 26(f), 27(b). One week later, on December 12, 2014, in exchange for the $20,000 watch and the expectation of additional payments from Foreign Official-1, Defendant Abouammo began accessing, without authorization, confidential data for "Twitter User-1," an account that had posted critical information about the Saudi Royal Family, including Saudi Royal Family Member-1. *See id.* ¶ 26(g). Among other account information, Defendant Abouammo accessed the email address and telephone number for Twitter User-1, which the Saudi government could have used to identify and locate the user of that account. *See id.* Defendant Abouammo accessed user data for Twitter User-1 again on January 5, 2015. *See id.* Twelve days later, on January 17, 2015, Foreign Official-1 emailed information concerning Twitter User-1 to Defendant Abouammo with the following brief message: "as we discussed in London." *See id.* ¶ 26(h). Thereafter, between January 27 and February 24, 2015, Defendant Abouammo accessed user data for Twitter User-1 on five more occasions. *See id.* ¶ 26(g).

Further, on February 5, 2015, Foreign Official-1 sent a second email to Defendant Abouammo with information concerning a second Twitter account ("Twitter User-2") that he claimed was impersonating a member of the Saudi Royal Family. *See id.* ¶ 26(i). Within two days, on February 7, 2015, Defendant Abouammo accessed, without authorization, Twitter's confidential data for that account, including the user's email address, which the Saudi government could have used to identify and

locate the user of that account. *See id*. Less than a week later, on February 13, 2015, Foreign Official-1 wired $100,000 to a recently opened bank account in Lebanon in the name of Defendant Abouammo's close relative, which Defendant Abouammo could access online. *See id*. ¶ 26 (j). Around this same time, on February 16, 2015, Defendant Abouammo facilitated an introduction between Defendant Almuitari and Defendant Alzabarah, who thereafter also began accessing confidential Twitter information for Foreign Official-1 and the Saudi government. *See id*. ¶ 26(m), (o). As with the $20,000 luxury watch he received from Foreign Official-1 for accessing Twitter's confidential information, Defendant Abouammo also concealed his receipt of $100,000 from Foreign Official-1. *See id*. ¶ 27(c).

On February 24, 2015, while Defendant Abouammo was employed by Twitter and residing in the Northern District of California, he caused $9,963 of the money he received from Foreign Official-1 to be transferred from the account in Lebanon to his Bank of America account in the United States. *See id*. ¶¶ 2, 12, 26(j). On March 8, 2015, shortly after Defendant Abouammo accessed data for Twitter User-1, he sent the following message to Foreign Official-1: "proactive and reactively we will delete evil my brother." *See id*. ¶ 26(j). Then, on March 12, 2015, while Defendant Abouammo remained employed by Twitter and continued to reside in the Northern District of California, he caused another $9,991 to be transferred from Lebanon to his Bank of America account in the United States. *See id*. ¶¶ 2, 12, 26(j), and 40. Not too long after, Defendant Abouammo caused another $40,000 of the money he received from Foreign Official to be transferred from Lebanon to the same account. Specifically, $10,000 was transferred on June 11, 2015, *see id*. ¶ 42, and $30,000 was transferred on July 2, 2015, *see id*. ¶ 42.

Defendant Abouammo left Twitter on May 22, 2015. *See id*. ¶ 26(k). Shortly after, and at some point before July 9, 2015, Foreign Official-1 wired a second $100,000 to the aforementioned account in Lebanon. *See id.*; Complaint ¶ 46 (specifying that Foreign Official-1 sent Defendant a receipt for this wire transfer on July 9, 2015). Foreign Official-1 then sent a Twitter message to Defendant Abouammo showing the wire receipt and apologizing for the delay in sending the "late" payment. *See id*. ¶¶ 26(j), 38 (Count 11). Based on Foreign Official-1's message and other facts, this second payment of $100,000 related to Defendant Abouammo's access to confidential information while he was employed by Twitter prior to May 22, 2015.

Defendant Abouammo continued to act as an agent of the Saudi government after he left Twitter by engaging employees of the company on the Saudi Arabian government's behalf and by performing other acts at Foreign Official-1's direction. *See id.* ¶ 26(k). On December 31, 2015, Defendant created a sole proprietorship, CYRCL, LLC, and registered it with the State of Washington. *See* Complaint ¶ 49; Superseding Indictment ¶ 46. On January 12, 2016, he opened a business checking account in the United States, and on January 25, 2016, Foreign Official-1 wired a third payment of $100,000 to that account. *See* Complaint ¶ 49; Superseding Indictment ¶ 26(k).

On October 20, 2018, FBI agents conducted a voluntary interview of Defendant about his receipt of the aforementioned luxury watch and his communications with Foreign Official-1 and others. *See* Complaint ¶ 51. Agents informed Defendant that they had come from Palo Alto, California (within the Northern District of California) and were conducting an investigation there. *See id.* During the interview, Defendant Abouammo admitted that he accessed Twitter User-1's nonpublic account information after receiving an email from Foreign Official-1 about the account. *Se id.* ¶ 52(a). He further admitted that he had met with Foreign Official-1 in London and received a watch from him. *See id.* ¶ 52(b). However, he falsely described it as "plasticky" and junky" and claimed it was valued at only $500. *See id.* Additionally, Abouammo appeared to regret showing FBI agents the July 9, 2015 Twitter message from Foreign Official-1, referenced above, regarding a late payment; after doing so, FBI agents observed him delete it. *See id.* ¶ 52(d).

Related to the money he had received from Foreign Official-1, Defendant falsely stated that he only received $100,000 from Foreign Official-1 (when, in fact, he had received at least $300,000) and claimed that it was payment for consulting and media strategy work related to CYRCL, LLC (which, in fact, he did not register until December 31, 2015). *See id.* ¶¶ 52(c), 54; Superseding Indictment ¶ 46. After making that claim, Defendant Abouammo offered to obtain a copy of the consulting contract from a desktop computer in his bedroom and requested that the FBI agents not follow him into the bedroom. *See* Complaint ¶ 54. They complied. *See id.* A few minutes later, he emailed an undated invoice to one of the FBI agents, which was received by the FBI in the Northern District of California. *See id.*; Superseding Indictment ¶ 46. As the evidence at trial will show, Defendant Abouammo fabricated that invoice, which purported to show services rendered in 2015 and 2016, during the interview with the

intent to impede, influence, and obstruct the FBI's investigation in the Northern District. *See id.* ¶ 55; Superseding Indictment ¶ 46. Specifically, the invoice identified Defendant Abouammo's current address in Washington, which he did not purchase until August 2017. *See* Complaint ¶ 55. Further, the metadata properties associated with the file indicate that it was created on October 20, 2018, the date of the FBI interview. *See id.*

II. APPLICABLE LAW

A. Review of a Motion to Dismiss for Failure to State an Offense

An indictment need not explain all factual evidence to be proved at trial. *United States v. Blinder*, 10 F.3d 1468, 1476 (9th Cir.1993). A motion to dismiss "is not the appropriate time to require the Government to present its proof." *United States v. Buckley*, 689 F.2d 893, 900 (9th Cir. 1982).

An indictment "will withstand a motion to dismiss 'if it contains the elements of the charged offense in sufficient detail (1) to enable the defendant to prepare his defense; (2) to ensure him that he is being prosecuted on the basis of the facts presented to the grand jury; (3) to enable him to plead double jeopardy; and (4) to inform the court of the alleged facts so that it can determine the sufficiency of the charge.'" *United States v. Rosi*, 27 F.3d 409, 414 (9th Cir. 1994) (quoting *United States v. Bernhardt*, 840 F.2d 1441, 1445 (9th Cir. 1988)); *United States v. Rodriguez*, 360 F. 3d 949, 958 (9th Cir. 2004) ("Generally, an indictment is sufficient if it sets forth the elements of the charged offense so as to ensure the right of the defendant not to be placed in double jeopardy and to be informed of the offense charged.") (quoting *United States v. Woodruff*, 50 F.3d 673, 676 (9th Cir. 1995). "In the end, the test is not whether the indictment could have been framed in a more satisfactory manner but whether it conforms to minimal constitutional standards." *Rosi*, 27 F.3d at 415 (quotation marks omitted); *see also United States v. Stringer*, 730 F.3d 120, 124 (2d Cir. 2013) ("[A]n indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime.") (quotation marks omitted).

B. Wire Fraud

The elements of Wire fraud are as follows: "(1) the existence of a scheme to defraud; (2) the use of [a] wire . . . to further the scheme; and (3) a specific intent to defraud." *United States v. Lindsey*, 850 F.3d 1009, 1013 (9th Cir. 2017). As discussed below, the "scheme to defraud" element must include

false statements or material omissions.

i. *False Statements or Material Omissions*

A wire fraud scheme may involve materially false statements and half-truths or material omissions. *See United States v. Woods*, 335 F.3d 993 (9th Cir. 2003) (false statements); *United States v. Omer*, 395 F. 3d 1087, 1088 (9th Cir. 2005) (holding that in a case not involving false statements, the scheme to defraud must be material). Moreover, "[a] nondisclosure or concealment may serve as a basis for the fraudulent scheme . . . when there exists an independent duty (either fiduciary or derived from an explicit and independent statutory requirement) and such a duty has been breached." *United States v. Dowling*, 739 F.2d 1445, 1449-50 (9th Cir. 1984), *rev'd on other grounds*, 473 U.S. 207 (1985).

If the government is proceeding on a theory that includes only omissions, the indictment must allege facts giving rise to a duty to disclose. *See United States v. Lonich*, 2016 WL 324039, at *8 (N.D. Cal. Jan. 27, 2016). A formal fiduciary duty is not required, but rather, "a trust relationship, as existed here, is sufficient" to establish a duty to disclose. *United States v. Milovanovic*, 678 F.3d 713, 721 (9th Cir. 2012) (en banc), *cert denied*, 568 U.S. 1126 (2013). This duty may be interpreted broadly and need not be formal, but "extends to a trusting relationship in which one party acts for the benefit of another and induces the trusting party to relax the care and vigilance which it would ordinarily exercise." *Id*. at 724.

"'The existence of a fiduciary duty . . . is a fact-based determination that must ultimately be *determined by a jury* properly instructed on this issue.'" *Id*. at 723 (emphasis added). In *United States v. Shields*, the Ninth Circuit applied the fiduciary standard to wire fraud charges for an investment fraud scheme based on a material omissions theory. 844 F.3d 819, 823 (9th Cir. 2016) ("[T]he relationship creating a duty to disclose may be a formal fiduciary relationship, or an 'informal,' 'trusting relationship in which one party acts for the benefit of another and induces the trusting party to relax the care and vigilance which it would ordinarily exercise.'") (quoting *Milovanovic*, 678 F.3d at 723-24); *see also Chiarella v. United States*, 445 U.S. 222, 230 (1980) (holding, in a securities fraud case, that "a relationship of trust and confidence" is required to create a duty to disclose).

//

//

C. Honest Services Wire Fraud

ii. Elements

Section 1346 provides that a "'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services." The Ninth Circuit's Pattern Criminal Jury Instructions (8.121) set forth the elements of honest services mail[2] fraud as follows:

> (1) The defendant devised or knowingly participated in a scheme or plan to deprive Twitter, Inc. of its right of honest services;
> (2) The scheme or plan consists of a bribe or kickback in exchange for the defendant's services. The exchange may be express or may be implied from all the surrounding circumstances;
> (3) The defendant owed a fiduciary duty[3] to [Twitter, Inc.];
> (4) The defendant acted with the intent to defraud by depriving Twitter, Inc. of its right of honest services;
> (5) The defendant's act was material; that is, it had a natural tendency to influence, or was capable of influencing, an entity's acts; and
> (6) The defendant used, or caused someone to use, the wires to carry out or to attempt to carry out the scheme or plan.

ii. Honest Services Caselaw

Section 1346 applies to private sector fraud. As the Fifth Circuit has explained, "[t]he principal federal bribery statute, [18 U.S.C.] § 201 . . . generally applies only to federal public officials, so § 1346's application to *state and local corruption* and to private sector fraud reaches misconduct that might otherwise go unpunished." *United States v. Christensen*, 828 F. 3d 763, 785 (9th Cir. 2016) (emphasis in original)). In *United States v. Rybicki,* the Second Circuit held:

> Based upon a review of the case law extant at the time that Congress enacted section 1346, we conclude that the statute clearly prohibits a scheme or artifice to use the mails or wires to enable an officer or employee of a private entity (or a person in a relationship that gives rise to a duty of loyalty comparable to that owed by employees to employers)

---

[2] Model Jury Instruction 8.121 (2019) defines honest services fraud, albeit in the nearly identical mail fraud context. The elements for honest services wire fraud would be identical, save "an interstate wire" instead of "the mails" in the sixth element."

[3] The Model Jury Instruction defines "fiduciary duty" to "exist[] whenever one . . . places special trust and confidence in another person–the fiduciary–in reliance that the fiduciary will exercise . . . discretion and expertise with the utmost honesty and forthrightness in the interests of the [person or entity], such that the [person or entity] relaxes the care and vigilance that [he, she, or it] would ordinarily exercise, and the fiduciary knowingly accepts that special trust and confidence and thereafter undertakes to act on behalf of the other [person or entity] based on such reliance."

> purporting to act for and in the interests of his or her employer (or of the person to whom the duty of loyalty is owed) secretly to act in his or her or the defendant's own interests instead, accompanied by a material misrepresentation made or omission of information disclosed to the employer.

354 F. 3d 124, 126-127 (2d Cir. 2003).

The Supreme Court has limited the definition of honest services fraud under 18 U.S.C. § 1346 to include only cases in which the perpetrator received a bribe or kickback from a third party. *See Skilling v. United States*, 561 U.S. 358, 404 (2010); *Black v. United States*, 561 U.S. 465, 471 (2010). The required exchange, or *quid pro quo*, need not be explicit, and may be implied. *See United States v. Garrido*, 713 F. 3d 985, 997 (9th Cir. 2013) ("Section 1346 honest services convictions on a bribery theory . . . require at least an implied *quid pro quo*"); *see also United States v. Andrews*, 681 F.3d 509, 527 (3d Cir. 2012) ("The *quid pro quo* can be implicit") (quotation marks omitted). These concepts are incorporated in Model Jury Instruction 8.121 (2019), described above.

III. ARGUMENT

Counts Five through Nineteen allege that Defendant, his two co-defendants, and others sought to obtain money or property by means of false statements and material omissions, and sought to deprive Twitter of its intangible right of honest services through the same and in exchange for bribes, and aided and abetted such violations. The Superseding Indictment includes 28 paragraphs (one of which includes 21 subparagraphs) of detailed factual allegations, which, if proven, meet the elements of each of these violations.

That Defendant is charged with both participating in a scheme to defraud Twitter of its property (i.e., its proprietary and confidential user information), and its intangible right to Defendant Abouammo's and Defendant Alzabarah's honest services. Those charges are not a mistake, but rather, a recognition that Defendants' conduct both constituted an honest services crime as well as a scheme to obtain proprietary and confidential information in exchange for money. Rather than assume that the conduct alleged in the Superseding Indictment is true, as Defendant now must, Defendant's Motion to Dismiss appears to largely ignore the well-established principle that the factual allegations in the Superseding Indictment must be accepted as true, and Defendant further appears to challenge the weight of the government's evidence, which is the province of the jury. *See United States v. Holmes, et al.*,

5:18-cr-00258-EJD, Dkt. 330 (N.D. Cal. Feb 11, 2020) ("Ironically, the fact that Defendants can pick apart the truth of the events in the indictment indicates that the SI is constitutionally sound—it means Defendants know what they will face at trial."). For the reasons that follow, Counts Four through Nineteen are sound.

A. The Superseding Indictment Properly Alleges the Elements of Wire Fraud

The Superseding Indictment charges Defendant with conspiracy and wire fraud by accessing and providing user data on Twitter users of interest[4] to the Kingdom of Saudi Arabia and Royal Family Member-1, including User-1 and User-2. *See* Superseding Indictment, Dkt. 53, ¶¶ 21-25. Indeed, Defendant was offered a $20,000 watch in London by Foreign Official-1 to access Twitter's proprietary and confidential information about User-1. *See id.* at ¶¶ 26(g) through (j). If the bribe were not clear enough, Defendant continued to access that account and User-2's account in exchange for the $100,000 Foreign Official-1 paid him in February 2015 and another "late" payment of $100,000 in July 2015. *Id.* at ¶ 39 (Count 11). Defendant ignores the allegations that are plainly set forth in the Superseding Indictment, instead arguing the irrelevant and unsupported point that his repeated accesses of Twitter's information in exchange for bribes did not affect the performance of his job duties, discussed further below. *See Holmes*, 5:18-cr-00258-EJD, Dkt. 330 (N.D. Cal. Feb 11, 2020) (rejecting arguments disputing facts alleged in the indictment).

In support of his argument that the government has not properly alleged a scheme in violation of the wire fraud and honest services statutes, Defendant relies heavily on the First Circuit's decisions in *United States v. Czubinski*, 106 F. 3d 1069 (1st Cir. 1997). In that case, after a jury conviction, the defendant's wire and honest services fraud convictions were reversed because the First Circuit found there was no evidence of a bribe or that the defendant (an IRS employee) was doing anything other than accessing taxpayers' information for personal amusement. The First Circuit explained that "either some articulable harm must befall the holder of the information as a result of the defendant's activities, or

[4] The Superseding Indictment identifies two accounts that Defendant accessed, and numerous others accessed by his co-defendant. The number of accounts accessed does not negate the fraudulent nature of Defendant's actions. Moreover, evidence at trial will demonstrate that Defendant similarly accessed numerous other Twitter accounts in violation of his company's data policies, some possibly out of curiosity. Defendant is not charged with a fraud scheme for accessing those accounts, however.

some gainful use must be intended by the person accessing the information, whether or not this use is profitable in the economic sense." *Id.* at 1074. The First Circuit specifically found that it might have upheld the jury convictions of a government employee if there "[h]ad there been sufficient proof that [the defendant] intended either to create dossiers for the sake of advancing personal causes or to disseminate confidential information to third parties," which is strikingly similar to the conduct alleged against Defendant in the Superseding Indictment. Id., 106 F. 3d at 1075. Unlike *Czubinski*, Defendant was paid by a third party to violate his duty of loyalty to Twitter by obtaining user information for users of interest to the Kingdom of Saudi Arabia and providing it to them.

B. Defendant Schemed To Deprive Twitter of Money And Property

Taken as true, the Superseding Indictment alleges that Twitter's proprietary and confidential user data was "valuable property." Superseding Indictment, ¶ 21. Defendant would have the Court find that intangible property must always meet the California definition of "trade secret." *Carpenter*, which Defendant fails to address or distinguish, says otherwise. 484 U.S. at 27 ("Confidential business information has long been recognized as property."). However, the property need not be a trade secret[5] to constitute property for purposes of the federal fraud statutes. The First Circuit in *Czubinski* seemed to concede that even IRS' taxpayer database information constituted property. Nor can Defendant credibly suggest that the Indictment runs afoul of *United States v. Cleveland*, which he cites for the proposition that the "thing obtained must be property in the hands of the victim." 531 U.S. 12, 15 (2000). Defendant's citation of *Carpenter* immediately thereafter to support his argument is self-defeating, as *Carpenter* and other cases treat intangible data as valuable property for purposes of the federal wire and mail fraud statutes without looking to state law definitions. *Id.*; *see also Pasquantino v. United States*, 544 U.S. 349 (2005) (explaining that "[t]here was no suggestion in *Cleveland* that the defendant aimed at depriving the State of any money due under the license," whereas the "petitioners' scheme aimed at depriving Canada of money").

[5] A separate criminal statute, 18 U.S.C. § 1832, specifically protects trade secrets from theft, indicating that the wire and mail fraud statutes include valuable property that falls short of the definition of a trade secret. The government does not concede for purposes of this motion, however, that the user data involved in the scheme to defraud is not also a trade secret of Twitter, Inc. as defined in 18 U.S.C. § 1839.

Finally, Defendant argues – incorrectly- that the type of property involved in the fraud must be defined by state statutes. In analyzing the Motion, the Court must take the factual allegation that a social media company's information about its users' IP addresses and associated email addresses or phone numbers constitute property as true. Whether or not state law defines the data that Defendant agreed to access and share with Foreign Official-1 and others does not render it "property" for purposes of the wire fraud and conspiracy statutes. *See United States v. Inzunza*, 638 F. 3d 1006, 1018 (9th Cir. 2011) ("We also reject Inzunza's contention that a state law violation must be alleged and proved in cases of honest services fraud."). Defendant's factual dispute is both dismissive of the revenue model of social media companies and his former job duties as a Media Partnerships Manager advising notable individuals, journalists, and public officials about how to use Twitter and engage users in order to drive traffic on Twitter's social media platform.

C. Defendant Ignores the Government's Allegations of False Statements and Material Omissions

The essence of honest services fraud involves an undisclosed conflict of interest as a result of bribes or kickbacks, coupled with acts in furtherance of the scheme. Whether an honest services scheme or wire fraud alone, under a material omissions theory, it is the "*materiality of the scheme* or artifice that must be alleged." *United States v. Omer*, 395 F. 3d 1087, 1089 (9th Cir. 2005) (emphasis added). In contrast, where false statements are made as part of a wire fraud scheme, each of the charged material statements must be material. *See United States v. Woods*, 335 F.3d 993, 1000 (9th Cir. 2003). The government is not required to detail the specific false statements made in the indictment. *See United States v. Buckley*, 689 F.2d 893, 899 (9th Cir. 1982).

Unlike *Keuylian*, cited by Defendant, the Superseding Indictment here alleges numerous deceptive acts underlying the scheme to defraud, including the material omission of his receipt of a watch valued at $20,000 on December 5, 2014, and $100,000 on February 13, 2015, and keys those bribes to Defendant Abouammo's accesses of User-1 and User-2's account information and numerous communications close in time with the payor, Foreign Official-1, who specifically requested that information. *See* Superseding Indictment, ¶¶ 26(f), (j); *cf. United States v. Keuylian*, 23 F. Supp. 3d 1126, 1129 (C.D. Cal. 2014) (dismissing indictment because it failed to describe any of the deceptive

acts underlying the alleged scheme to defraud and thus only showed willful breach of contract). Defendant further failed to obtain prior written consent of Twitter before disclosing the user information, as his employment agreement required. *See* Superseding Indictment, ¶ 14.

Defendant does appear to concede that the government alleges at least one (of several) act of concealment: Defendant's use of private means to communicate with foreign individuals seeking business with Twitter. But his argument is not a legal one: Defendant claims that the methods of communication by email, telephone and direct message are "extremely common." Def. Mot., p. 10. This is not a legal bar to charges, but rather an assertion of perceived weakness of the government's case that should be made to the jury and not packaged to the Court in the form of a motion to dismiss. Defendant also appears to want the Court to believe that Twitter monitors the private Twitter messages in the user accounts of its employees, a baseless claim that has no factual support.

With regard to omissions, Defendant makes the bare factual claim that he made no material omissions as part of the alleged fraud scheme. Defendant's not guilty plea does not render the charges insufficient. The Superseding Indictment includes the following allegations:

- Defendant affirmed Twitter's "Playbook" of employment policies. ¶ 15.
- Twitter policies prohibit outside employment "or any other business activity that would create a conflict of interest with the Company." ¶ 14.
- Twitter's "Gift Policy" prohibited "gifts exceeding $100 in value," and required employees to "bring the gift to the attention of both your manager and VP of HR before returning to sender." ¶ 16.
- Twitter Policies described "a relationship of confidence and trust" between themselves and Twitter "with respect to any information of a confidential or secret nature that may be disclosed to [them] by the Company or a third party that relates to the business of the Company." ¶ 14.
- Accessing Twitter user information "was a reportable violation of the Twitter Playbook policies regarding handling and protecting user data." ¶ 18.
- Proprietary information, including customer lists, are not to be disclosed outside of Twitter without prior written permission of the company. ¶ 14.

Just because Defendant had access to user information does not mean that he was allowed to access it, much less at the direction of a foreign official paying him in cash and expensive gifts. Moreover, Defendant did not act alone; the alleged scheme involved other parties who also made false statements and material omissions.

The Indictment clearly lays out that Defendant "fraudulently used [his] position[]s and access to information at Twitter to provide Foreign Official-1 and others related to, and working for, the government of KSA and the Saudi Royal Family with nonpublic information held in the accounts of Twitter users." Superseding Indictment, ¶ 21. Paragraph 23 of the Superseding Indictment further alleges that "ABOUAMMO . . . communicated such nonpublic account information to Foreign Official-1 and others in the government of KSA, contrary to Twitter policies" and Paragraph 24 alleges that, "[i]n exchange for accessing nonpublic account information of Twitter users, outside the scope of their job duties, and for communicating such nonpublic account information to Foreign Official-1, contrary to Twitter's policies, Foreign Official-1 rewarded ABOUAMMO and ALZABARAH including with compensation such as gifts [and] cash payments." *Id.*

The Superseding Indictment further alleges that Defendant materially omitted his receipt of a watch valued at $20,000 or more from Foreign Official-1 in violation of the Twitter gift policy requiring employees to report gifts valued at over $100. Whether Defendant "signed or acknowledged" the Gift Policy, which Defendant appears to dispute, is yet another question of fact or the weight of the evidence to be undertaken by the jury that Defendant seeks to have the Court decide instead. Defendant's unsupported musings about it being "doubtful" that he could be charged where he did not specifically sign the policy at issue is as insufficient to secure a dismissal as it is speculative and illogical. Employers would surely not write corporate policies for their employees to willfully ignore.

In a similar vein, Defendant's factual argument that his omission of his receipt of a watch and cash in exchange for accessing users' information is not material because the Gift Policy did not specify that he would have to divulge the payor of the gift is ridiculous. If Defendant thought that he only had to disclose the gifts and not their source, his omission is all the more material and willful. By willfully failing to disclose the gift (and indeed concealing it in a relative's foreign bank account and falsely describing it when he repatriated it), and further by using his personal Twitter account, telephone number, and email address to communicate with Foreign Official-1, Defendant deprived his supervisors the opportunity to investigate his conflict of interest or prevent the unauthorized access and dissemination of its user's information. This is the essence of fraud.

//

D. The Superseding Indictment Alleges a Fiduciary Duty

The Superseding Indictment properly alleges that Defendant was a fiduciary of Twitter. Indictment, Dkt. 53, ¶ 23 (Alzabarah and Abouammo had "access privileges as employees and fiduciaries of Twitter") and ¶ 28. Mounting an improper factual challenge to this allegation, Defendant wrongly claims that he was not required to disclose his accesses of User-1 or User 2 to his employer and therefore did not violate 18 U.S.C. §§ 1341 or 1346. This again is contradicted by the Superseding Indictment, which alleges that Twitter policies described "a relationship of confidence and trust" between it and Defendant "with respect to any information of a confidential or secret nature that may be disclosed to [them] by the Company," and required Defendant to "keep and hold all such Proprietary Information in strict confidence and trust," including "customer lists and data." Id. at ¶ 14. Defendant agreed that he would "not use or disclose any Proprietary Information without the prior written consent of the Company." Id. This element is properly alleged.

E. The Superseding Indictment Alleges Numerous Wires

The Indictment alleges fifteen specific interstate wires, including accesses of user data from abroad, Twitter direct messages, and telephone calls, in furtherance of Defendants' scheme to defraud Twitter of property and honest services. *See* Superseding Indictment, Dkt. 53, ¶ 38. This alone is sufficient to meet the interstate wire element for both 18 U.S.C. §§ 1343 and 1346. Instead, Defendant argues that the Superseding Indictment fails to allege *which* wires between him and Foreign Official-1 carried a Twitter user's information. The elements of the crimes alleged do not require that the Superseding Indictment specify any particular wire that carried the user data, or even that a wire carried such data,[6] and Defendant's unsupported argument ignores that the government may prove the allegation that Defendant "used [his] positions and access to information at Twitter to provide Foreign Official-1 . . . with nonpublic information held in the accounts of Twitter users" through circumstantial as well as direct evidence. *See* Superseding Indictment, Dkt. 53, at ¶ 21.

//

//

[6] The accesses of Twitters' user information database by Defendants Alzabarah from Almutairi's network in the Kingdom of Saudi Arabia clearly would meet Defendant's challenge, however.

F. The Superseding Indictment Alleges Defendant's Intent to Defraud

Defendant claims that the Superseding Indictment "does not allege that Defendant acted with the specific intent to defraud Twitter." Def. Mot., p. 7. It clearly does. Count Four alleges that Defendant "devised and *intended* to devise a scheme and artifice to defraud Twitter", while Counts Five through Nineteen allege that Defendant, his codefendants, and others "did knowingly, and *with the intent to defraud*, participate in, devise, and intend to devise a scheme and artifice to defraud Twitter." Indictment, Dkt. 53, pp. 14, 15 (emphasis added). Defendant then argues that the Indictment is silent elsewhere as to "Twitter's money," ignoring both Defendant's continuing salary while he concealed his violations of company policy as well as the value of the information to the payor of the bribe, which was worth at least $200,000 and a $20,000 watch to Foreign Official-1. Indeed, nothing further is required, and Defendant fails to suggest what allegations would be required to satisfy the fraud and honest services statute. *See United States v. Utz,* 886 F.2d 1148, 1151 (9th Cir. 1989). (holding it sufficient for "the government [to] charge and the jury [to] find either that the victim was actually deprived of money or property *or* that the defendant intended to defraud the victim of the same.") (emphasis in original); *see also United States v. Wright*. 665 F. 3d 560, 568 (3d Cir. 2012) *(*"[A] bribery theory does not require that each quid, or item of value, be linked to a specific quo, or official act. Rather, a bribe may come in the form of a 'stream of benefits.'" (quoting *United States v. Bryant*, 655 F.3d 232, 240-41 (3d Cir. 2011)).

G. The Government Properly Alleges the Elements of Honest Services Fraud

The Superseding Indictment alleges facts which, if proven, satisfy the elements of wire fraud. A wire fraud scheme may be proven through false statements, material omissions, or both. The government incorporates its arguments above with respect to Defendant's intent to defraud, use of the wires, and status as a fiduciary of Twitter, Inc.

Defendant concedes, in a footnote, that the caselaw requiring a scheme to obtain money and property from the victim (a scheme to deceive *and* cheat) under the wire fraud statute excludes honest services frauds. *See United States v. Miller,* 953 F.3d 1095, 1103 (9th Cir. 2020). Moreover, Defendant is clearly wrong when he claims that "[t]he counts charging honest services fraud do not even allege that Twitter was *actually* deprived of its right to Mr. Abouammo's honest services." Def. Mot., p. 6

(emphasis added). It, of course, does. Counts Five through Nineteen, charging wire fraud, and honest services fraud, and Count Four charging the same as a conspiracy,[7] incorporate Paragraph 28, which provides "[t]he scheme deprived Twitter of . . . *Twitter's intangible right to the honest services* of its employees and fiduciaries, ABOUAMMO and ALAZABARAH." (emphasis added). Moreover, Paragraph 38 of the Superseding Indictment alleges that all three charged Defendants, and others, "did knowingly . . . devise a scheme and artifice to defraud Twitter . . . and to deprive Twitter of its right to the honest and faithful services of its employees and fiduciaries through bribes, and attempt[ed] to do so." Nor is actual damage to Twitter required: the fraud statutes prohibit devising the scheme, not completing it. *See Vinyard*, 266 F.3d at 329. It is unclear what further allegations Defendant believes are required by law such that these counts must be dismissed.

i. The Scheme to Defraud Twitter of its Intangible Right to Honest Services

As alleged in the Superseding Indictment, Defendant was paid by a third party to violate his duty to safeguard Twitter confidential property, specifically, its user data. *See* Superseding Indictment, Dkt. No. 53, ¶¶ 14-15. Defendant, whose job duties included assisting notable individuals with Twitter accounts in the Middle East and North Africa region, began working for officials of the Saudi Arabian government who bribed him to provide them with protected user information that he had access to as an employee of Twitter. *Id.* at ¶ 17. By doing so, Defendant violated his affirmative duties to (1) report violations of the company's data handling policies and (2) disclose to his supervisors gifts from individuals such as Foreign Official-1. *Id.* at ¶¶ 16, 18. Defendant's failure to do so and concealment amount to material omissions underlying his honest services charges. *See United States v. Dowling*, 739 F.2d 1445, 1449-1450 (9th Cir. 1984) (holding a violation of a duty to disclose satisfies the material omission theory of wire fraud). Moreover, Defendant is also liable for the affirmative false statements of his coconspirator, Ali Alzabarah, who lied to Twitter about the purpose of his accesses when challenged. *See* Superseding Indictment, ¶ 26(s). Taking these allegations as true, Defendant's claims that the Superseding Indictment fails to properly allege an honest services violation fails.

[7] The Indictment alleges that Defendant agreed with others to commit wire and honest services fraud and intended to help accomplish it. *See, e.g.,* Superseding Indictment, Dkt. 53, ¶¶ 21-24, 26(g) and (h), 36.

ii. The Bribe or Kickback

Defendant also argues, wrongly, that the Superseding Indictment "does not adequately allege that Mr. Abouammo received a bribe." Def. Mot., Dkt. 83, p. 13. The Superseding Indictment specifically calls the watch and cash payments "bribes," and further details a watch worth at least $20,000 and several payments of $100,000, including one in February 2015, that he received while he was working at Twitter and accessing users' data at Foreign Official-1's direction. Superseding Indictment, Dkt. 53, ¶¶ 26(f), (j), and (k), 36. Defendant's attempt to dispute the alleged facts at this stage fails, and will likely also fail at trial. *See* Def. Mot., p. 16 (citing *United States v. Hawkins*, 777 F. 3d 880, 882 (7th Cir. 2015)). If accessing and providing proprietary, confidential Twitter-user information to foreign government officials was in no way related to his official duties, as Defendant argues, then his receipt of a watch and cash could not have been a gratuity. *See id.*, 777 F.3d at 882 (defining a gratuity as "a payment that does not entail a plan to change how the employee or agent does his job."). Although this is a dispute of fact appropriate for trial, the Superseding Indictment alleges that Defendant violated his job responsibilities and policies in accessing and sharing confidential users' information.

iii. Materiality

The Superseding Indictment sufficiently alleges that the false statements and omissions were material. Defendant's omission of his affirmative duty to disclose to his employer his own violation of the company's data policies and his receipt of the watch and cash from Foreign Official-1 Defendant's receipt of bribes to violate his company's data protection policies was certainly the kind of omission that had the natural tendency to influence his employer. Failing to disclose these violations, Twitter was deprived of the opportunity to investigate whether officials of the government of Saudi Arabia were seeking to co-opt employees in order to obtain personal information (in the possession of Twitter) about its critics and other accounts of interest. *See* Superseding Indictment, at ¶¶ 27 ("material false representations, promises, and omissions"), ¶ 27(c). Moreover, co-defendant Ali Alzabarah's false denials when confronted about the accesses were also material to the fraud scheme. *Id.* at ¶ 27(f). Defendant cites no case requiring that the indictment must use the word "material," but even so, each of Counts Four through Nineteen allege "material" three times. ¶¶ 36, 38. Defendant's attempt to challenge the factual allegations in the Superseding Indictment fail.

H. Defendant's Other Factual Challenges Should Be Made at Trial

i. Confidential Business Information is "Property"

Defendant appears to dispute the value of the user data that he schemed to access and provide to Foreign Official-1. However, in *United States v. Carpenter*, the Supreme Court held that intangible "confidential business information" is property for purposes of the wire fraud statute. 484 U.S. 19, 25 (1987). At issue in *Carpenter* was a scheme by a *Wall Street Journal* reporter to leak the contents of upcoming "Heard on the Street" columns to his associates at a brokerage firm, who would then make trading decisions based on the column's likely impact on the market. *Id.* at 23. The reporter never altered the articles for purposes of boosting the traders' profits, but he did violate the *Journal*'s confidentiality policy by disclosing the columns' contents. *Id.* In affirming the conviction, the Court unanimously rejected the defendants' claim that they took no "money or property" from the *Journal*. *Id.* at 25. The Court explained that "the object of the scheme was to take the *Journal*'s confidential business information—the publication schedule and contents of the 'Heard' column—and its intangible nature does not make it any less 'property' protected by the mail and wire fraud statutes." *Id.* at 25. Even though the *Journal* suffered no monetary loss, it was "sufficient that the *Journal* has been deprived of its right to exclusive use of the information," because "exclusivity is an important aspect of confidential business information," and "[c]onfidential business information has long been recognized as property." *Id.* at 26–27; *see also United States v. Middendorf,* No. 18-CR-36 (JPO), 2018 US Dist. LEXIS 118850, at *7 (S.D.N.Y. July 17, 2018) (quoting *Carpenter,* 484 U.S. at 26-27). *Carpenter*, which was based on a property or "thing of value" theory of wire fraud, predated *Skilling* and Section 1346 and therefore is unaffected by *Skilling*'s limitations on bribe and kickback schemes. *See, e.g.*, *United States v. Hager*, 879 F.3d 550 (5th Cir. 2018) ("We conclude that *Carpenter*'s holding is unaffected by *Skilling* and, accordingly, that confidential business information remains a cognizable property right protected by §§ 1341 and 1343"); *see also United States v. Brugnara*, 856 F. 3d 1158, 1207 (9th Cir. 2017) (quoting *Carpenter* post-*Skilling*).

Nor does Defendant support his argument that the government must allege some economic value to the property stolen. If the government is not required to do so for fraud schemes involving stolen artwork, for example, Defendant provides no basis for the Court to dismiss the fraud counts based on a

failure to provide a valuation for the data of a Twitter user with at least one million followers, and ignores that Foreign Official-1 valued it at several hundred thousand dollars.

ii. Defendant's Claim of a Lack of Harm to Twitter is Irrelevant and Wrong

Defendant's argument that his actions did not harm his employer (a question for trial) is irrelevant to the issue of whether the government has properly alleged criminal offenses. Section 1346 is violated by materiality, not by economic harm to the victim. *See, e.g., Christensen*, 828 F.3d 763 (honest services fraud upheld in scheme to access information from police databases); *United States v. Vinyard*, 266 F.3d 320, 329 (4th Cir. 2001) ("The reasonably foreseeable harm test [under § 1346] neither requires an actual economic loss nor an intent to economically harm the employer . . . . [T]he reasonably foreseeable harm test is met whenever, at the time of the fraud scheme, the employee could foresee that the scheme potentially might be detrimental to the employer's economic well-being."); *United States v. Nayak*, 769 F.3d 978, 981 (7th Cir. 2014) (explaining that honest services cases have largely "focused on the defendant's benefit from the fraud rather than any harm to the victim"); *see also United States v. Tanner*, No. 17 Cr. 61 (LAP), 2018 WL 1737235, at *6 (S.D.N.Y. Feb. 23, 2018) ("The Court agrees with the Government that after *Skilling*, Section 1346 requires a defendant to act in exchange for a bribe or kickback, but whether such actions benefited or harmed the employer who enjoyed a right to the honest services of its employee, is irrelevant." (citing *Nayak*, 769 F.3d at 981–82)); *United States v. Sorich*, 523 F.3d 702, 707 (5th Cir. 1941); *and United States v. Renzi*, 2012 U.S. Dist. LEXIS 39595 (Mar. 22, 2012, D. AZ) (same). Indeed, the government need not prove *whose* property a defendant sought to obtain through fraud. *See United States v. Crawford*, 239 F.3d 1086, 1092 (9th Cir. 2001) (holding that the identity of the victim need not be proven in a fraud scheme).

Defendant claims that his violations of his employer's policies is not material to the fraud against his employer. Although this is surely a matter for the jury to consider, Defendant's concealment of bribes in exchange for his access of the company's users' identifiable information, and his repeated accesses of that information at the request of a foreign official, is precisely what allowed him to perpetrate a fraud against his employer and avoid being fired for several months prior to his resignation. The harm to Twitter is hardly speculative: the compromise of personally identifiable user information is clearly harmful to the victim, which is the basis of Twitter's data handling policy, and the Superseding

Indictment properly alleges that Defendant made some gainful use of the information, that is, keeping tabs on a Twitter user at the request of a third party willing to pay large sums for that access. Defendant's claims that he would not have had to identify the source of the gift is equally ridiculous. But Defendant deprived his employer of the opportunity to do so, giving rise to these well-grounded bribery charges.

As with virtually all of the Defendant's arguments, these are nothing more than a premature challenge to the government's trial evidence. *See Buckley*, 689 F.2d at 897 (in reviewing a motion to dismiss, "the issue in judging the sufficiency of the indictment is whether the indictment adequately alleges the elements of the offense . . . not whether the Government can prove its case."). However, the government intends to prove both harm to Twitter and gain to Defendant at trial. *See Czubinski*, 106 F. 3d at 1074 ("[E]ither some articulable harm must befall the holder of the information as a result of the defendant's activities, or some gainful use must be intended by the person accessing the information, whether or not this use is profitable in the economic sense").[8]

IV. CONCLUSION

The Superseding Indictment details the Defendants' scheme to defraud Twitter both of user data and of its right to Ahmad Abouammo and Ali ALzabarah's honest services as employees and fiduciaries of the company. For the foregoing reasons, the government respectfully requests that the Court deny Defendant's Motion to Dismiss Counts Four through Twenty-Three.

DATED: December 7, 2020.

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney,

/s/ Colin Sampson
COLIN C. SAMPSON
Assistant United States Attorney
BENJAMIN J. HAWK
Trial Attorney, National Security Division

[8] *Czubinski* related to government information, which the Court did not appear to consider commercially valuable, unlike information about a user with over one million followers on the platform. *Id.*