STEPHANIE M. HINDS (CABN 154284)
United States Attorney

THOMAS A. COLTHURST (CABN 99493)
Chief, Criminal Division

COLIN SAMPSON (CABN 249784)
ERIC CHENG (CABN 274118)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
FAX: (415) 436-7009
Colin.Sampson@usdoj.gov
Eric.Cheng@usdoj.gov

MATTHEW G. OLSEN
Assistant Attorney General
National Security Division

CHRISTINE A. BONOMO (NYBN B10113801)
Trial Attorney, National Security Division
950 Pennsylvania Avenue NW
Washington, DC 20530-0001
Telephone: (202) 514-0313
Christine.Bonomo@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-1 GOVERNMENT'S SENTENCING MEMORANDUM Date: December 14, 2022 Time: 10:30 a.m. Judge: Edward M. Chen, U.S. District Judge

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

I. INTRODUCTION

For hundreds of thousands of dollars and a luxury watch, Ahmad Abouammo ("Defendant") helped transform one of the world's largest social media companies based here in San Francisco into a covert surveillance tool for a foreign government. Defendant knew he was working as an agent of "the King's team" and what officials of the Kingdom of Saudi Arabia (KSA) demanded from him when he knowingly joined their scheme, repeatedly accessing the information of KSA critics while laundering bribes to himself through an offshore bank account in Lebanon. When the FBI arrived at Defendant's doorstep after he reaped the benefits of his crimes, he lied to them and falsified a document to obstruct justice.

Defendant's conduct as established at trial calls out for a sentence strong enough to deter others in the technology and social media industry from selling out the data of vulnerable users around the world who seek to speak freely and share information, and as a warning to foreign powers wishing to offer lavish bribes to infiltrate the troves of valuable user data stored by companies here in this District. For Defendant's serious crimes and in view of his lack of any acceptance of responsibility, and to send an important message of deterrence to any others who may be tempted to follow the same path for unlawful profit over responsibility—as well as those paying bribes to encourage the same, the government recommends that the Court impose a custodial sentence in this matter of 87 months imprisonment, followed by three years of supervised release, along with a $30,000 fine, a forfeiture money judgment of $242,000, and the $600 mandatory special assessment. This is a sentence at the low-end of the applicable Guidelines. The low-end recommendation accounts for the Government's assessment of 18 U.S.C. § 3553(a) factors as it concerns the defendant's lack of criminal history and family circumstances.

II. FACTUAL AND PROCEDURAL BACKGROUND

The Court is familiar with the factual and procedural background of this matter provided by the government in its Opposition to Defendant's motion for judgment of acquittal and motion for new trial, and the government incorporates those sections by reference rather than repeating them here. *See* ECF No. 399, Part II. However, the convictions and facts in support of sentencing factors are discussed below.

III. THE PRESENTENCE INVESTIGATION REPORT ("PSIR")

A. Conviction for 18 U.S.C. § 951 – Acting as an Agent of a Foreign Government Without Prior Notice to the Attorney General

Defendant was convicted by the jury of acting in the United States as an agent of a foreign government without providing prior notice to the Attorney General, in violation of 18 U.S.C. § 951. The offense carries a maximum sentence of 10 years and is not referenced by any applicable Sentencing Guideline provision. Indeed, while such prosecutions are rare, a March 2020 sentence in this District for a conviction of such a violation following a defendant's waiver of indictment and guilty plea yielded a sentence of 48 months. *See United States v. Xuehua Peng*, 4:19-CR-00589 HSG.

The government respectfully requests that the Court impose a significant, deterrent sentence for Defendant's violation of 18 U.S.C. § 951 separate from and in addition to the grouped fraud, money laundering, and obstruction conduct discussed below.

B. Conspiracy to Commit Wire Fraud and Honest Services Fraud

The United States Probation Office calculates the Sentencing Guidelines in the PSIR for the grouping of fraud, money laundering, and obstruction counts of conviction as Total Offense Level of 27, resulting in a guidelines range of 70 to 87 months of imprisonment. PSIR ¶¶ 41–54. While the government largely agrees with the calculations in the PSIR for this grouping of counts, Probation's calculation misses the enhancement for a scheme affecting more than ten victims, U.S.S.G. § 2B1.1(b)(2)(A)(i), resulting in a two-point higher Total Offense level of 29:

Offense Level Computation	**#**	**Calculation in PSIR**
Base Offense Level, § 2B1.1(a)(1)	7	Probation Agrees, PSIR ¶ 45
Losses between $150,000-$250,000, § 2B1.1(b)(1)(F)	+10	Probation Agrees, PSIR ¶ 45
Risk of death or bodily injury, § 2B1.1(b)(16)(A)	+2	Probation Agrees, PSIR ¶ 45
More than 10 victims, § 2B1.1(b)(2)(A)(i)	+2	Government's position
Money laundering § 1956 conviction, § 2S1.1(b)(2)(B)	+2	Probation Agrees, PSIR ¶ 46
Sophisticated means, § 2S1.1(b)(3)	+2	Probation Agrees, PSIR ¶ 47
Abuse of position of trust, § 3B1.3	+2	Probation Agrees, PSIR ¶ 49
Obstruction of justice, § 3C1.1	+2	Probation Agrees, PSIR ¶ 50
Total Offense Level for Fraud Grouping	**29**	

At **Offense Level 29**, the applicable range for incarceration on the grouping of fraud, money laundering, and obstruction counts is **87 to 108 months**. As explained below, there is no basis for a departure or variance here. Defendant is and at all times was an educated, well-paid, high powered technology employee who used his position of influence to enrich himself despite working for a high paying, high-growth Silicon Valley company. Defendant's crimes are squarely within the heartland the Guidelines ranges were designed to address. His conduct was extensive and well-hidden from Twitter long after he left the company, and he lied and obstructed justice when the FBI ultimately uncovered his crimes.

Moreover, Defendant's conduct was not simply economic in nature, as it implicated the safety and privacy of users of a global social media platform from powerful foreign government officials.[1] Absent consideration of the factors discussed in 18 U.S.C. § 3553(a), which the government separately addresses below, the Guidelines calculation submitted by the government captures the scope of the fraudulent and obstructive conduct underlying Defendant's convictions.

1. Loss or Gain Calculation

Although the losses to the victims of the fraud—including Twitter and many of its users—are undoubtedly substantial, the fraud loss cannot reasonably be calculated. "The court shall use the gain that resulted from the offense as an alternative measure of loss only if there is a loss but it reasonably cannot be determined." U.S.S.G. § 2B1.1, App. N. 3(B). Much of Twitter's losses as a result of the crimes proven at trial would result in lost business and lost user revenues and to sunk costs of employee time spent investigating the fraud. Twitter also compensated Defendant with a six-figure salary and stock options for his employment from 2013 to 2015, and any value he did, in fact, provide to the company is offset by him selling out the company and its users for the benefit of the Kingdom of Saudi Arabia. Moreover, the losses to the Twitter users whose data was accessed by Defendant and Alzabarah – while undeniably significant – would also be extremely challenging to quantify.

[1] Although the government does not request an upward variance here, the Guidelines provide for consideration of a variance where "[a] primary objective of the offense was an aggravating, non-monetary objective;" and where "[t]he offense caused or risked substantial non-monetary harm.[. . .f]or example, the offense caused physical harm, psychological harm, or severe emotional trauma, or resulted in a substantial invasion of a privacy interest." U.S.S.G. § 2B1.1, App. N. 21(A)(i) and (ii).

As a result, the appropriate alternative calculation should be Defendant's gain from the unlawful scheme, which was at least $242,000 – amounts attributable to funds and jewelry Defendant received for his agreement to access, monitor, and convey user information using his Media Partnership Manager role at Twitter. This figure is easily calculable from the evidence at trial:

- A $42,000 watch given to Defendant by Bader Binasaker in London on December 5, 2014 (*see* Ex. 608);
- The $100,000 wire transfer by Binasker to Defendant's father's Bank Audi Account in Beirut, Lebanon, on February 11, 2015 (*see* Exs. 23, 24); and
- The $100,000 wire transfer by Binasaker to the same Bank Audi account on July 13, 2015 (*see* Exhs. 23, 33, 801T).

Pursuant to U.S.S.G. §§ 2B1.1(a)(1) and (b)(1)(i), the base offense level for Defendant's fraud convictions with a loss above $150,000 and under $250,000, is **17**.[2]

2. Specific Offense Characteristic: Risk of Bodily Harm

A two-level enhancement under U.S.S.G. § 2B1.1(b)(16)(A) is also warranted. As relevant here, that provision provides that, if "the offense involved [] the conscious or reckless risk of death or serious bodily injury" an enhancement of two levels should be applied. Notably, the enhancement does not require evidence that a defendant subjectively knew of the risk he or she caused. As the Ninth Circuit has held, a defendant cannot "escape the application of the serious risk of injury enhancement by claiming that he was not aware that his conduct created a serious risk, that is, a defendant does not have to subjectively know that his conduct created the risk." *United States v. Johansson*, 249 F.3d 848, 859 (9th Cir. 2001) (citations omitted).

Further, arguments that the defendant's actions did not actually result in serious injury, or arguments that the defendant's actions were not likely in most cases to result in serious injury, are not relevant for purposes of applying the enhancement. As the Ninth Circuit has also explained:

> A district court need not engage in a sophisticated probability analysis to apply the adjustment. It is the *creation of risk*, not the infliction of injury, that is required for application of this guideline provision. A district court does not abuse its discretion in applying it when the defendant has acted in

[2] The wire fraud conviction carries a maximum sentence of 20 years, and results in a base offense level 7 pursuant to U.S.S.G. § 2B1.1(a)(1). The alternative calculation of gain between $150,000 and $250,000 results in an additional 10 points pursuant to § 2B1.1(b)(1)(F). for a total of 17, before any additions.

> conscious or reckless disregard of a known risk of serious bodily injury *even if the ultimate probability of occurrence is found to be relatively low*.

United States v. West Coast Aluminum Heat Trading Co., 265 F.3d 986, 993 (9th Cir. 2001) (emphases added); *see also United States v. Thorsted*, 439 F. App'x 580, 582 (9th Cir. 2011) ("The law is clear that no showing that the injury did or was likely to occur is necessary."). And "[o]nly 'some' evidence that the conduct created a risk of serious bodily injury is required." *Thorsted*, 439 F. App'x at 582. In *United States v. Awad*, 551 F.3d 930 (9th Cir. 2009), for example, the court affirmed the district court's application of the enhancement in a health care fraud case in which the physician defendant had lied about being present for the administration of respiratory therapy. The defendant had argued that the respiratory therapies at issue were basic non-invasive procedures without risk of injury, serious or otherwise, to patients. *Id.* at 942. But the court rejected the argument, observing that there was nevertheless evidence that there was some risk created by the physician's absence: namely, trial testimony of a therapist who had testified that the defendant should have been present for the administration of the respiratory therapies because of the risk of adverse side effects. *Id.*

Ample evidence supports a finding that Defendant was consciously aware or should have been aware that his conduct – passing private user information about dissidents to a repressive foreign government – created at least some risk of serious bodily injury to those dissidents, such as a result of arrest and possible corporal punishment and torture. At trial, KSA expert, Dr. Kristin Diwan, testified extensively about KSA's absolute monarchy and the power "above all" others wielded by the Saudi Royal Family and those closest to the throne. *See generally* ECF No. 399 at 9-14 (discussing expert testimony). She also testified that, during the relevant period, and as MbS ascended to greater levels of power, the Saudi government became increasingly repressive of dissenting views. "Critical voices were shamed or depicted as traitors" and "prominent" dissidents with "influential followings" were arrested. *See id.* The government also engaged in "**increased surveillance**" "**in an attempt to silence or control through the media critical views**." *See* Trial Tr. 732:14-735:5 (Diwan) (emphasis added). Critics and dissenters had to leave the Kingdom **out of fear for their own safety**. *See id.* 734:21-735:5. Dr. Diwan's expert report observes that this increased repression of dissenting voices on social media began with passage of a restrictive anti-terrorism law in January 2014, which classified political activities such

as participation in protests and demonstrating sympathy for suspect currents of thought on social media as prosecutable offenses. *See* Ex. 901 at 13; *see also* Ex. 651T at 5-6 (English translation of Saudi Arabian Anti-Cyber Crime Law sent to Defendant by Binasaker September 8, 2015 with sentences up to 10 years in prison); Ex. 653Tat 2-3 (English translation of Saudi Arabian law under a "specialized court" punishable 20 years or "**a more severe legally imposed penalty**" for disseminating documents causing harm to Saudi Arabia's "interests" (emphasis added)). Dr. Diwan's report also provides more detail about specific events and consequences certain dissenters faced: namely, arrest, detention, torture. See Ex. 901 at 12-15. Tragically, at least one victim of the conspiracy, who posted satirical commentary on the KSA government, suffered such consequences. In March 2018, he was arrested, detained, and tortured as a result of his Twitter posts, and remains detained to this day. *See* PSIR ¶ 37; *see also* Trial Tr. 1195:10-1197:15 (Al Sadhan) (describing @sama7ti's satirical commentary of KSA), *id.* 1200:5-1201:6 (describing loss of contact with @sama7ti after March 2018).

The preponderance of the evidence demonstrates that Defendant understood the risks associated with speaking out against the Royal Family and the Kingdom of Saudi Arabia's government. He had lived in Saudi Arabia as recently as 2010; he was the head of MENA for Twitter with experience and expertise in the region; and he was the self-described "government liaison" with KSA officials, including Binasaker. *See* Trial Tr. 993:10-17 (Walker) (describing Defendant's experience in Saudi Arabia specifically), *id.* 1002:5-8 (same); *id.* 426:3-12 (Stanton) (describing Defendant's experience in the MENA region); Trial Tr. 1459:14-18, 1460:8-14 (Wu) (Defendant describing himself as a "government liaison between Twitter and the KSA government"); PSIR ¶¶ 85-86 (describing Defendant's prior employment in Saudi Arabia and experience working for the Middle Eastern Broadcasting Network).

And if there was any doubt that Defendant knew or should have known of the risks to dissidents, email correspondence during the relevant period demonstrates that it was undoubtedly apparent to him. Indeed, in January 2015, Binasaker emailed Defendant a document asserting that the @mujtahidd account Defendant accessed repeatedly was violating KSA's laws by spreading a rumor about King Salman's health and voicing other critical commentary about the Saudi Royal Family, including MbS. Ex. 610 at 1-2; *see also* Ex. 651T.

Defendant also received other emails from coworkers describing KSA's repression of dissidents. As early as September 2014, Defendant was specifically aware of the potential risks to the user behind the @mujtahidd account. In an email that month, Abouammo's Twitter colleagues sent him a link to an NPR article, "Twitter User Airs Saudi Arabia's Dirty Laundry," discussing the @mujtahidd account and its critical commentary on the Saudi Royals. *See* Exs. 466, 467. The linked NPR article observed that social media activists like @mujtahidd "have been sentenced to prison" and that the state itself "has a very robust internal security apparatus." Ex. 467. In response to receiving this link, Abouammo stated that he was "of course . . . aware :)" of this account and had discussed it with unnamed individuals from KSA. Ex. 466. Further, in a January 2015 email thread in which Defendant described to coworkers that he had spent months "buil[ding] a strong relationship with the team of HRH Crown Prince Salman" and announced King Salman's imminent ascension to the throne, a colleague shared a Daily Mail article describing the harsh consequences KSA critics faced, referencing detention and corporal punishment specifically: "The case of blogger Raef Badawi serves as an example of the Gulf state's ever-tightening freedom of expression. Badawi is serving a 10-year jail sentence for insulting Islam, and he has also been sentenced to 1,000 lashes, having received 50 of them in public this month." Ex. 441 at 2.

It is in the context of this evidence – as well as Defendant's repeated accesses of the @mujtahidd and @HSANATT accounts at the behest of the KSA, and his receipt of a luxury watch and hundreds of thousands of dollars in wire payments – that one can reasonably infer Defendant knew the risks faced by dissidents when he wrote to Binasaker in March 2015, "Proactive and reactively we will delete evil my brother." Ex. 810T. The two-level enhancement under U.S.S.G. § 2B1.1(b)(16)(A) should apply.

3. Money Laundering Adjustments

i. Method of Calculation

The government agrees with the PSIR's calculation of the Base Offense Level using U.S.S.G. § 2S1.1(a)(1), which begins with the "offense level for the underlying offense from which the laundered funds were derived." As described above, the Base Offense Level is **21**.

//

ii. Conviction for 18 U.S.C. § 1956

Defendant laundered some of the funds deposited by Binasaker into the Bank Audi account in his father's name in Lebanon by transferring smaller amounts into his Bank of America account in the United States in the following amounts:

$9,945 on March 12, 2015: "Family Fund" (Ex. 26);

$10,000 on June 15, 2015: "Family Fund" (Ex. 28); and

$30,000 on July 7, 2015: "Down payment of an appartment in USA" (Ex. 30)

Further, account notifications for Defendant's father's account in Lebanon went to Defendant's Google account. *See* Exs. 612, 613. Defendant communicated bank instructions for Bank Audi to his sister. *See* Exs. 31, 32, 614; *see also* Trial Tr. 1801:1-19 (Amany Abouammo). Defendant also gave his sister a debit card to withdraw money from the Bank Audi account and wired her $6,000. *Id.*, *see* Ex. 27. Defendant was convicted after trial of two violations of 18 U.S.C. § 1956(a)(2)(B)(i) in relation to the international wire transfers on March 12, 2015, and June 15, 2015. As a result, and pursuant to 2S1.1(b)(2)(B), a two-level upward adjustment is applied, resulting in an Offense Level **23**.

iii. Sophisticated Laundering

The government agrees with the PSIR's application of the two-level increase for sophisticated money laundering. Bader Binasaker could have – and later did (*see* Ex. 13, p. 1) – wire funds directly to the United States. But during Defendant's time at Twitter and shortly after, two bribe payments were made through a newly-opened account in Defendant's father's name in Beirut, Lebanon, before some of the funds were withdrawn or wired to the United States to Defendant.

Note 5 of the applicable Guideline provision states that "'sophisticated laundering' means complex or intricate offense conduct pertaining to the execution or concealment of the 18 U.S.C. § 1956 offense" and lists, among other things, "offshore financial accounts." Here, there is simply no legitimate reason to have the bribe payment made to a relative's account and not sent directly to the Defendant, other than to cover up and conceal Binasaker as the source of the original payment. Using Defendant's father's account served no other purpose than to keep evidence of the source offshore. That the account was opened in early February 2015 (*see* Ex. 22, p. 7) and the two $100,000 payments from Binasaker are the only deposits demonstrates that its use was to be a vehicle of concealment. Defendant's use of

an offshore financial account in a relative's name thus satisfies the definition of sophisticated laundering for applicability of the two-point enhancement, resulting in an Offense Level **25**.[3]

4. Chapter 3 Adjustments

i. Abuse of Position of Private Trust

Pursuant to U.S.S.G. § 3B1.3, a defendant may receive an enhancement of two points where they "abused a position of public or private trust, or used a special skill, in a manner that significantly facilitated the commission or concealment of the offense." Here, the jury convicted defendant of two[4] schemes as they related to Twitter: a conspiracy and scheme to defraud Twitter of money and property by accessing, monitoring, and conveying information about users to officials of the Kingdom of Saudi Arabia, and a conspiracy and scheme to defraud Twitter of its intangible right to Abouammo's honest services. While the Court may ultimately agree that the 18 U.S.C. § 1346 offense "is included in the base offense level or specific offense characteristic" for that crime, the Court should find that this enhancement is applicable to Defendant's wire fraud and conspiracy conviction. Defendant's autonomy and trust given by Twitter to assist notable and important partners in the Middle East and North Africa region was never questioned before he left the company in May 2015 and is precisely what allowed him to ensure that he could covertly monitor and provide users' data to foreign officials that bribed him and his associate Alzabarah while they worked at Twitter. For officials of KSA, the value was clear: for a

---

[3] In the alternative, a two-level enhancement may be appropriate pursuant to U.S.S.G. § 2B1.1(b)(10)(B) where "a substantial part of a fraudulent scheme was committed from outside the United States." The scheme to defraud Twitter of user data involved numerous acts abroad. Binasaker, with whom Defendant conspired, lived and worked as a government official in KSA. Defendant met Binasaker in London to discuss the @mujtahidd account and received the luxury watch, and all subsequent wire payments from Binaskaer to Defendant originated outside of the United States. Further, according to Defendant's passport, he was abroad when numerous acts occurred, including:

(i) Two of Defendant's seven dates of access of @mujtahidd were while he was abroad: January 27, 2015 (see Ex. 229 at 2; Ex. 951 at 1), and February 18, 2015 (Ex. 951 at 1 (12/18/2015));

(ii) Defendant was in Lebanon when the first wire transfer was made from the Bank Audi account to his account in the United States on February 20, 2015 (Ex. 23 at 1; Ex. 229, p. 2); and

(iii) Defendant was in Lebanon when $14,990 was withdrawn in cash from the Bank Audi account (Ex. 23, p. 1).

[4] Defendant's actions as an agent of the Kingdom of Saudi Arabia were also related to his role and access at Twitter.

few hundred thousand dollars, you could unmask the anonymous dissenters followed by millions in your country, chill free speech by silencing your critics, and influence the online conversation. Defendant's position of "managerial discretion" that was "subject to significantly less supervision than employees whose responsibilities are primarily non-discretionary in nature" is precisely what this enhancement was meant to cover. *See* U.S.S.G. § 3B1.3, *Comment* N. 1.

As a result of the above, a two-point upward adjustment for abuse of a position of trust is warranted, resulting in an Offense Level **27**.

ii. Obstruction of Justice

Defendant was convicted of falsification of records in a federal investigation pursuant to 18 U.S.C. § 1519. At trial, the government proved that Defendant, during an interview with FBI Special Agents on October 20, 2018, offered to provide the agents with an invoice for a $100,000 payment he received from Bader Binasaker. He excused himself for approximately 30 minutes and emailed one of the agents a document that purported to be an invoice for $100,000 for "[o]ne year of consultancy." Ex. 807. The document's metadata demonstrated that, although it purported to be for 2016, the document was created during the pause in the interview. The document also reflected Defendant's current home address, which he did not yet reside in and was not yet built in 2016.

As is clear from this evidence, Defendant provided a false document to the agents in an attempt to convince the investigators of the legitimacy of the financial transactions between him and Binasaker, which he continued to assert during and after trial. Defendant's claims – and the purported documents to support them – were materially false and misleading as Defendant wanted the agents to believe that he was paid for something other than accessing users' information while employed at Twitter. *See* U.S.S.G. § 3C1.1, App. N. 6 ("Material" evidence, fact, statement, or information, as used in this section, means evidence, fact, statement, or information that, if believed, would tend to influence or affect the issue under determination"). But even aside from his conviction for falsification of records, the obstruction enhancement would be applicable for Defendant's lies to the Special Agents during the interview, including his description of the luxury Hublot watch he received from Binasaker in London as "plasticky" and "junky," and his description of the $100,000 wire transfer in July 2015 (*See* Ex. 802) as a payment for consulting services of Cyrcl, LLC, which occurred months later, and for deleting images

and communications from his Twitter app on his iPhone after showing certain conversations to the agents during the interview.

Notably, the Court has already ruled against Defendant on his challenge of venue for the obstruction offense. *See* ECF No. 95, p. 2. Even if it had not rejected Defendant's argument, the enhancement would nevertheless apply as "any relevant conduct" or "a closely related offense." U.S.S.G. §§ 3C1.1(2)(A) and (B). As a result of the above, a two-point upward adjustment for obstruction of justice is warranted, resulting in an Adjusted Offense Level **29**.

C. Restitution: The Government's and Twitter's Restitution Calculations

Defendant was found guilty of violating, among other offenses, 18 U.S.C. §§ 1343, 1346, and 1349, which are covered by the Mandatory Victim Restitution Act of 1996, 18 U.S.C. §§ 3663A(b)(1)(B)(ii). This statute provides that restitution is mandatory when a defendant has been convicted of certain enumerated offenses. 18 U.S.C. § 3663A(a). The enumerated offenses include any Title 18 offense against property, including any offense committed by fraud or deceit. 18 U.S.C. § 3663A(c). Defendant's conspiracy, wire, and honest services fraud convictions are Title 18 offenses against property, and were committed by fraud or deceit. At this time, however, no victims have provided a calculation of economic losses for purposes of a restitution order, and the government cannot readily calculate such a loss.

D. Forfeiture

The government has sought a preliminary order of forfeiture of $242,000, representing the two $100,000 deposits to Defendant's father's Bank Audi account and Defendant's claimed value of the Hublot Unico King Gold Ceramic watch given to him by Bader Binasaker on December 5, 2014. *See* ECF. No. 412.

E. Fine

A significant fine is appropriate for the profitable, greed-based offense the government proved at trial. Defendant provided Probation with information about a single bank account and vehicle. *See* PSIR ¶ 88. Defendant has not provided Probation with information about the disposition of the valuable Hublot watch that could not be located in the search of his residence, or his large cash withdrawals from the Cyrcl, LLC bank account (*see* Ex. 13, pp. 51, 89) and purchases of computer equipment (*see id.*, pp.

43, 48) with funds paid to him by Binasaker. The government disagrees with Probation's assessment, based only on self-serving information provided by Defendant, that he does not have the present ability to pay any fine. A low-end Guidelines fine of $30,000 (based upon an offense level 29) is appropriate for all the reasons argued in this memorandum.

IV. OBJECTION TO PSIR CALCULATIONS

1. Specific Offense Characteristic: 10 or More Victims

The government respectfully disagrees with the PSIR's exclusion of an enhancement for 10 or more victims pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(i). The scheme Defendant joined involved accessing, monitoring, and conveying Twitter users' information of interest to the Kingdom of Saudi Arabia and the Saudi Royal Family. The scheme was not limited to harming Twitter or accessing a single Twitter user. Indeed, Binasaker had a shopping list of eight dissidents on April 12, 2015 whose personal information KSA wanted, including @mujtahidd, as well as the accounts of Abdulrahman Al Sadhan and Omar Abdulaziz. Ex. 521T, p. 2. Defendant also received a dossier on @HSANATT from Binasaker, which he accessed in February 2015. Ex. 450T; Ex. 951. Alzabarah's accesses of scores of accounts, including his accesses of the information of at least five more accounts on June 6, 2015 which Binasaker and Alzabarah recorded on two additional digital notes, further demonstrate that the scheme involved far greater than 10 victims. Ex. 646T at 2; 523T at 3; see also Ex. 952 at 1. The two-level enhancement for the number of victims of the scheme to infiltrate Twitter should be applied here, bringing the Adjusted Offense Level to **29**.

V. DISCUSSION REGARDING 18 U.S.C. § 3553(a) FACTORS

Section 3553(a)'s factors also strongly support the government's recommended sentence of 87 months' imprisonment because Defendant committed his crimes at the expense of his employer and its vulnerable users around the world at the behest of a foreign power, causing hundreds of thousands of dollars of gain for himself.

District courts are to impose a sentence sufficient, but not greater than necessary, to comply with the purposes set forth in the Sentencing Reform Act. *See* 18 U.S.C. § 3553(a). In so doing, the courts are to consider, among other things: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the need for the sentence imposed (A) to reflect the seriousness of

the offense, to promote respect for the law, and to provide just punishment for the offense, (B) to afford adequate deterrence to criminal conduct, (C) to protect the public from further crimes of the defendant, and (D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range established by the Guidelines; (5) any pertinent policy statement; and (6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct. *Id.* While all of the Section 3553(a) factors should be considered, the government highlights a few that are particularly important in this case.

A. Nature and Circumstances of the Offense

Title 18, U.S.C. Section 3553(a)(1), requires that "the nature and circumstances of the offense" be considered in sentencing. As discussed at length above, the offenses at issue here involve the Defendant's violation of his duty of loyalty to Twitter by accessing private user data at the request of a foreign government. The conduct poses a severe risk of harm to Twitter's users as many of them were targeted for their speech and dissent, and the value of the information is reflected in the amounts paid to the Defendant—far exceeding his salary at the time. The sentence imposed upon Defendant should reflect the seriousness of the crime as reflected through loss to Twitter, gain to Defendant, and the potential harm that could be caused when the users' information was not protected.

B. Defendant's History and Characteristics

Title 18, U.S.C. Section 3553(a)(1) also requires that a defendant's "history and characteristics" be considered in sentencing. Defendant reported no major childhood trauma or other family characteristics which would have impacted his decision to accept the bribes in exchange for defrauding his employer, which paid him a $180,000 per year including stock options. PSIR § 84. He has strong family support. Moreover, Defendant is a naturalized United States citizen and the Kingdom of Saudi Arabia did not otherwise appear to have any particular power over him or any family members that might affect his decision to join in the scheme.

In other words, Defendant did it for the money. However, the government's recommendation of a low-Guidelines sentence, despite several aggravating factors supported in the record that might call for

a mid- to high-Guidelines sentence, reflects Defendant's lack of other criminal history and his support for his immediate family (including care for his sister and her child) during the period of the offenses.

C. General and Specific Deterrence – Respect for the Law

Section 3553(a) requires that the sentence imposed provide "adequate deterrence." *Id.* The government's recommended sentence of 87 months' imprisonment is appropriate for both general and specific deterrence. General deterrence is one of the prescribed goals of every sentencing, *United States v. Pugh*, 515 F.3d 1179, 1194 (11th Cir. 2008), but it occupies an especially important role in sentencing for fraud offenses because prosecutions of high-level employees are rare and are afforded great attention by others in positions of power. Nowhere is that need higher than in Silicon Valley, where the opportunity to abuse power with the promise of assistance related to technology companies is a constant temptation for employees looking to line their pockets with kickbacks and bribes. A sentence of 87 months' imprisonment would be sufficient, but not more than necessary to accomplish this goal. Members of the industry, who pay attention to cases like these, are likely to have an appropriate respect for the law with such a sentence, and would help underscore that the potential losses in such cases would far outweigh the gains.

A below-Guidelines sentence for Defendant's crimes could send the wrong public message and certainly would not fulfill the need for general deterrence. Instead, it would foster a belief that certain white-collar crimes are not serious, and when caught are not punished like other crimes. The admonition of the Court of Appeals in *United States v. Ture* applies aptly: "the goal of deterrence rings hollow if a prison sentence is not imposed in this case." 450 F.3d 352, 358 (8th Cir. 2006). As courts have often recognized, there is a great need for imposing a meaningful custodial sentence in cases involving white collar crimes to reflect the seriousness of the offense, promote respect for the law, and, importantly, provide deterrence to further and similar conduct. *See, e.g.*, *United States v. Khan*, Case No. 12-CR-0860 YGR, 2014 WL 2930656, at *5 (N.D. Cal., June 27, 2014). Indeed, "[a] non-custodial sentence would not achieve any of those goals" and "a non-custodial sentence would encourage, not deter, [defendant] and others similarly situated to proceed with financial crimes, reap the financial benefit, and then expect the proverbial slap-on-the-hand as punishment." *Id.*; *cf. also United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) ("Defendants in white collar crimes often calculate the

financial gain and risk of loss, and white collar crime therefore can be affected and reduced with serious punishment. Yet the message of Martin's 7-day sentence is that would-be white-collar criminals stand to lose little more than a portion of their ill-gotten gains and practically none of their liberty."). Along those lines, there is a public perception in cases like this of defendants being charged and getting away with probation or a sentence significantly below the Guidelines, while other defendants in different sorts of cases are not so fortunate. That should not be the case here, especially in a case with such serious and pervasive criminal activity. This case is not unusual in any way that warrants a downward departure from the Guidelines.

In addition to serving as adequate general deterrence, a sentence of 87 months' imprisonment also affords sufficient specific deterrence. Without a significant sentence of imprisonment, Defendant may make a calculated decision in the future that the risks of being caught again by his employer or by law enforcement and punished are outweighed by the substantial financial rewards of cheating. Accordingly, a Guidelines sentence is warranted to adequately deter Defendant from future criminal conduct, which appears particularly important given that – at least to date – Defendant has not acknowledged any wrongdoing here.

D. Avoidance of Sentencing Disparities

i. Judiciary Sentencing Information (JSIN)

According to JSIN, at Offense Level 29, 130 offenders were sentenced under 2B1.1 at Offense Level 29 between FY 2017 and 2021. **The average length of imprisonment was 67 months**, with the median sentence 66 months. Additionally, 110 offenders were sentenced under 2S1.1 at Offense Level 29 between FY 2017 and 2021. The **average length of imprisonment was 66 months**, with the median sentence 63 months.

The Court should enter a deterrent sentence within the applicable Guideline for an Adjusted Offense Level of 29 of imprisonment of 87 months. Title 18, U.S.C. § 3553(a)(1), requires that "the nature and circumstances of the offense" be considered in sentencing. As detailed above, the nature and circumstances of Defendant's offenses demonstrate that his scheme to defraud his employer was not out of financial distress but greed. The scheme further involved numerous separate instances and manners of deceit.

VI. CONCLUSION

Any piece of information about users of interest – a Twitter user's recovery email address or telephone number of an anonymous dissenter, for example – could identify, unmask, arrest, and be used to imprison and prosecute a person for their speech or beliefs halfway around the world. That context demonstrates that this case is much more than simply one of business-related bribery. By accepting undisclosed bribes from the head of the private office of MbS to access, monitor, and convey information about dissidents of interest to the Saudi Royal Family and the government they controlled, Defendant exposed certain vulnerable users of his employer's social media platform to potential harassment and even arrest.

An 87-month term of incarceration followed by three years of supervised release, forfeiture of $242,000, and a deterrent fine of $30,000 pursuant to U.S.S.G. § 5E1.2[5] is sufficient but no greater than necessary to address the conduct at the core of this case: the offering and taking bribes to sell out the private information about a company's users to foreign government officials interested in quelling dissident views.

Respectfully submitted,

STEPHANIE M. HINDS
United States Attorney

Dated: December 7, 2022.

/s/ Colin Sampson
COLIN SAMPSON
ERIC CHENG
Assistant United States Attorneys
CHRISTINE A. BONOMO
Trial Attorney, National Security Division

[5] For his 6 counts of conviction, Defendant will also be responsible for the mandatory Special Assessment of $600.