UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- *v.* -	:	19 Cr. 64 (GHW)
NATALIE MAYFLOWER SOURS EDWARDS, a/k/a "Natalie Sours," a/k/a "Natalie May Edwards," a/k/a "May Edwards,"	:	
Defendant.	:	

THE GOVERNMENT'S SENTENCING MEMORANDUM

AUDREY STRAUSS
Acting United States Attorney
Southern District of New York

Kimberly J. Ravener
Daniel C. Richenthal
Assistant United States Attorneys
- Of Counsel -

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

BACKGROUND 2

I. The Offense 2

A. The Defendant, FinCEN, and an Overview of Her Offense 2

B. The Defendant's Initial Communications with Reporter-1 and Her Unsubstantiated Complaints Concerning FinCEN 4

C. The Defendant's Unrelated Sharing of SARs with Reporter-1 6

D. The Defendant's Running of Searches for Reporter-1 10

II. The Interview With Law Enforcement 10

III. The Searches 11

IV. The Charges And The Guilty Plea 12

V. Post-Plea Events 12

THE PRESENTENCE REPORT 14

ARGUMENT 15

I. A Meaningful Term of Imprisonment is Warranted 15

A. The Nature and Circumstances of the Offense 15

B. The Seriousness of the Offense 24

C. The History and Characteristics of the Defendant 26

D. The Need for General Deterrence and to Promote Respect for the Law 28

II. The Defendant's Arguments Are Unpersuasive 29

CONCLUSION 31

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- *v.* -	:	19 Cr. 64 (GHW)
NATALIE MAYFLOWER SOURS EDWARDS, a/k/a "Natalie Sours," a/k/a "Natalie May Edwards," a/k/a "May Edwards,"	:	
Defendant.	:	

THE GOVERNMENT'S SENTENCING MEMORANDUM

Defendant Natalie Mayflower Sours Edwards, a/k/a "Natalie Sours," a/k/a "Natalie May Edwards," a/k/a "May Edwards," is scheduled to be sentenced on November 9, 2020, at 10:00 a.m. The Government respectfully submits this memorandum in connection with sentencing and in response to the defendant's memorandum (Dkt. No. 81) ("Def. Mem.").

PRELIMINARY STATEMENT

For more than a year, the defendant, a senior official at the Financial Crimes Enforcement Network, abused her position, unlawfully providing to a reporter thousands of Suspicious Activity Reports ("SARs") and other materials containing sensitive personal and financial information of numerous individuals. She did so not because it was, in her misguided view, in the public interest to disclose such materials—but because she believed it was in her *own* interest. Nothing about her disclosing of SARs was akin to "bl[owing] the whistle" (Def. Mem. 2). It was a betrayal of the public, risked hindering both ongoing and future investigations, and was a deliberate, serious, and repeated crime. It demands serious punishment.

To serve the legitimate purposes of sentencing, including promotion of respect for the law and general deterrence, the Government requests that the Court impose a meaningful term of imprisonment, of at least the top of the applicable United States Sentencing Guidelines range of zero to six months' imprisonment.

BACKGROUND

I. The Offense

A. The Defendant, FinCEN, and an Overview of Her Offense

The defendant, who previously worked for multiple federal government agencies, most recently served as Senior Advisor to the then-head of the Intelligence Division at the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the United States Department of the Treasury. (Presentence Investigation Report ("PSR") ¶¶ 74-75.) The mission of FinCEN is to "safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities." (PSR ¶ 8.)

One of the primary functions of FinCEN is to manage the collection, maintenance, and analyses of confidential reports, including SARs. (*Id.*) Under the Bank Secrecy Act of 1970 (the "BSA"), financial institutions are required to generate SARs to report potentially suspicious financial transactions and to transmit the SARs securely to FinCEN. FinCEN maintains a database of SARs that are available to law enforcement, pursuant to regulations and procedures that protect the confidentiality of the information. The mission of the Intelligence Division, in particular, is to carry out FinCEN's responsibility to collect, analyze, and disseminate financial intelligence, including by identifying trends and disseminating reports to law enforcement. FinCEN also issues public reports, based on its analysis of BSA-protected and other data. *See, e.g.*, *Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19)*

Pandemic (July 30, 2020), *available at* https://www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

Under the BSA and its implementing regulations, unauthorized disclosure of the existence of a SAR or its contents is unlawful. (PSR ¶ 8.) This is so for good reason: because SARs not only contain highly sensitive and personal financial information, but also because law enforcement cannot act to detect, investigate, and prosecute crimes if the persons committing them are aware that a financial institution has informed the Government of their alleged conduct. Moreover, if individuals know with precision what triggers the filing of a SAR by a given financial institution, they might alter their conduct, thereby making it more difficult to detect. As FinCEN explains in an enclosed statement:

> The public policy underlying SAR confidentiality serves critical regulatory, law enforcement, and privacy objectives. Notifying the subject of a SAR of its existence or content can impede an investigation leading to the destruction of evidence, the chilling of potential witnesses, expose the reporting financial institution and its personnel to harm, and encourage SAR subjects to divert funds and continue potentially unlawful activity, among other things. In addition, rigorous nondisclosure requirements protect individual and corporate privacy and due process interests. A SAR is not a report of confirmed illegal activity; rather, it identifies suspicious activity based upon a financial institution's reasonable assessment of available information. The subject of a SAR may have a legitimate basis for the identified conduct, and therefore, should be protected against unauthorized exposure that could damage an innocent person's reputation.

(Ex. A, at 3); *see also* Government Accountability Office, *Anti-Money Laundering: Opportunities Exist to Increase Law Enforcement Use of Bank Secrecy Act Reports, and Banks' Costs to Comply with the Act Varied* (Sept. 22, 2020), at 8 (The BSA "framework is designed to simultaneously prevent criminals from using private individuals, banks, and other financial institutions to launder

the proceeds of their crimes and to detect those criminals who have successfully used the system to launder those proceeds."); *available at* https://www.gao.gov/assets/710/709547.pdf.

The defendant knew all of this. She was as a senior official at FinCEN, an experienced federal employee, and someone with both top secret security clearance and ongoing training. Indeed, these principles regarding the need for confidentiality of SARs are publicly-known, emphasized to FinCEN's employees, and critical to FinCEN's operations and maintaining the public trust. *See Law Enforcement Overview*, FinCEN, https://www.fincen.gov/resources/law-enforcement-overview ("Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its employees—a responsibility that strongly imprints all of its data management functions, and indeed, all that the agency does.") (last visited Oct. 26, 2020). But starting in summer 2017, the defendant began to abuse her access to FinCEN's confidential systems and her trusted position, and did so for more than a year—ultimately sharing with a reporter more than 2,000 SARs, as well as law enforcement-sensitive reports and analyses, and searching internal FinCEN databases at the reporter's request on multiple occasions.

B. The Defendant's Initial Communications with Reporter-1 and Her Unsubstantiated Complaints Concerning FinCEN

In or about July 2017, the defendant began communicating with a particular member of the news media ("Reporter-1") by email, telephone, and through an encrypted application on the defendant's personal cellphone (the "Encrypted Application"). (PSR ¶ 12.) The defendant coordinated with Reporter-1 to "[m]ak[e] sure we cover our tracks" by, among other things, arranging for Reporter-1 to send her a phony message via LinkedIn pretending to cold-contact her

for a story about purported issues at FinCEN.[1] In reality, the defendant herself had generated the story and was already in touch with Reporter-1.

Among other things, the defendant and Reporter-1 discussed the defendant's claims of certain perceived improprieties at FinCEN, and the defendant's desire to have articles written about these claims and to pursue a lawsuit relating to them. These claims primarily involved (1) an allegation that FinCEN had improperly revoked certain technical items, called "PKI certificates," used by its employees, which allegedly prevented those employees from providing a timely response to law enforcement requests related to spring 2017 terrorist attacks in London and Manchester, and (2) legal concerns about a proposal to move several employees from FinCEN to another bureau within the Treasury Department, called the Office of Intelligence Analysis. (*See, e.g.*, Def. Mem. 37-45.) Both of these matters were wholly unrelated to the content of any SARs. The defendant also raised claims of the same alleged misconduct within FinCEN, to Congress, and to the Office of Special Counsel ("OSC").[2]

Consistent with established policy and procedures, the defendant's complaints were examined, and, as appropriate, investigated. None was substantiated. On the contrary, as the defendant now appears to acknowledge (*see id.* at 45-46, 48), her complaints were thoroughly examined by the Treasury Office of Inspector General ("OIG"), which concluded in public reports that no violation of law or other misconduct had occurred. *See Audit of the Office of Intelligence and Analysis' Management of the Office of Terrorism and Financial Intelligence Employees'*

---

[1] The Government will provide the communications excerpted herein, which were produced in discovery, and are lengthy and contain BSA-protected and other sensitive information, upon request, under seal.

[2] OSC is an independent federal agency, the primary mission of which is to safeguard the merit-based system of federal civil employment by protecting federal employees and applicants from prohibited personnel practices, including reprisal for whistleblowing.

Intelligence Community Public Key Infrastructure Certificates (Oct. 30, 2017), *available at* https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-18-006.pdf; *Audit of the Office of Intelligence and Analysis' Authorities and Actions Related to U.S. Persons' Financial Information* (Apr. 30, 2018), *available at* https://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-18-044.pdf.[3]

Similarly, OSC informed the defendant in May 2018, following the issuance of OIG's reports:

> Based on OSC's review of the record, OIG appears to have reviewed and/or investigated all of your disclosures. We understand that you allege that OIG's work has been incomplete and dishonest, but OSC does not have evidence to support your allegations.

(Def. Ex. HHH, at 3.) OSC also concluded that the defendant had not established a "case for whistleblower retaliation." (*Id.* at 4.) In any event, whatever their merits, the defendant's claims of whistleblowing on alleged misconduct at FinCEN had nothing to with SARs. (*See id.* at 1-6.)

C. The Defendant's Unrelated Sharing of SARs with Reporter-1

Dissatisfied with the treatment of her complaints, and seeking to be promoted or to get a financial settlement, the defendant began to illegally make unauthorized disclosures of SARs and other materials, filled with details on the private financial dealings of myriad companies and individuals—and having nothing do with the defendant's complaints about alleged misconduct at FinCEN—to Reporter-1. This conduct commenced prior to the issuance of OIG's reports, and continued after they were issued.

---

[3] The defendant provides an incorrect link in her submission to the first of these reports. (*See* Def. Mem. 45.)

On at least 12 occasions between on or about October 29, 2017 and October 15, 2018, Reporter-1 published articles featuring some of these SARs. These publications (collectively, the "SARs Disclosures") related to investigations being conducted by Special Counsel Robert S. Mueller III, the United States Attorney's Office for the Southern District of New York, and/or the National Security Division of the Department of Justice, involving alleged financial transactions of Paul Manafort, Richard W. Gates, Russian diplomatic accounts, and other matters associated with the 2016 federal election. (*See* Complaint 19 Mag. 8861 ("Compl.") (Dkt. No. 1) ¶ 10; PSR ¶¶ 9-10.)[4]

There can be no dispute that the defendant disclosed these SARs to Reporter-1 knowing both that the information related to ongoing investigations and other sensitive matters, and that Reporter-1 intended to publish the information. To choose only a few examples:

- As early as on or about August 19, 2017, approximately one month after meeting Reporter-1, the defendant started providing sensitive information to Reporter-1, Reporter-1 asked: "Hey. I have to ask you a question non related to anything [that is, not related to her whistleblower claims]. Does [a specific bank] mean anything to you?" The defendant responded in part, "we found networks associated w Hezbollah," and discussed confidential intergovernmental requests made to partner nations with Reporter-1.[5] Shortly thereafter, Reporter-1 made clear this question was linked to a potential news article, sending a draft to the defendant.

- On or about January 12, 2018, Reporter-1 told the defendant, "I am trying to write up my story on these Russia SARs and the banks and it's painstaking." Several days later, on or about January 14, 2018, the defendant advised, "What you need to find out or determine is whether Treasury sent any records to FBI regarding election and what are the 2500 records already turned over either to [the Senate Select Committee on Intelligence] or Finance/Judiciary. . . . Key question is what are the SARs on [specific individual]."

---

4 As described below, *see supra* p.13, other articles were published subsequently.

5 The United States and other countries have designated Hezbollah a terrorist organization. The defendant nevertheless expressed no hesitation in providing non-public information about it to Reporter-1.

- On or about January 25, 2018, Reporter-1 referenced a prior article Reporter-1 had published using SARs obtained from the defendant on Paul Manafort, who was then-presumed innocent and indicted in an ongoing federal prosecution, sending the defendant a link to the published article. Reporter-1 then asked the defendant, "Can additional files from the list be sent so I can push the story forward a bit more? . . . . I realize this is a big ask. No worries if too much. But I wanted to ask. The story needs to be that explosive to make the right amount of noise." The defendant responded by sending files with the requested SAR information to Reporter-1. On or about February 20, 2018, Reporter-1 sent the defendant a draft of an article featuring the SAR information, which she read and consulted on in advance of publication.

Nor did the defendant stop providing SARs and other protected information to Reporter-1 after articles were published about the defendant's claims of alleged misconduct at FinCEN, those claims were investigated, and they were found to be without merit. To choose only a couple of examples:

- On or about July 24, 2018, Reporter-1 told the defendant, "I'm writing a story on [Maria] Butina, [two other individuals] and [an entity]. This will really piss off the senate because it's based on shit they could have had." Two days later, Reporter-1 claimed to have files from another source that Reporter-1 could not open relating to these same people and entity. The defendant then offered to get the records for Reporter-1, stating in part, "Hummm let me see if I can search and find the folder," and promised to send the files the next day, stating, "will not forget about [the] files. Sorry if you asked me in the past for them . . . ." (*See* PSR at 23.) Butina had been arrested just nine days earlier and her criminal case was then ongoing.

- On or about August 3, 2018, the defendant compiled a list of the titles and internet links for a number of the articles published based upon the SARs she unlawfully disclosed, confirming her knowledge that Reporter-1 was publishing the contents of the SARs. (PSR ¶ 16.) She emailed this list to Reporter-1, asking Reporter-1 to add any other similar articles. (*Id.*; Compl. ¶ 26(a).) Records from the defendant's personal email account also revealed numerous internet searches for the published articles and evidence that she had visited the news organization website where the articles were published. (PSR ¶ 17.)

Aware that she was illegally disclosing information that could impact ongoing investigations, starting early on, and continuing, the defendant took steps to conceal what she was

doing, including through use of the Encrypted Application, ensuring that messages she sent could not be intercepted.

The defendant also took steps to hide her connection to the SARs she was disclosing, by collecting them without directly accessing the primary FinCEN database and then transmitting files overtly to Reporter-1. Instead, between in or about October 2017—the month when the SARs Disclosures began to be published—and January 2018, the defendant saved more than 24,000 internal FinCEN files, including all of the SARs in the SARs Disclosures, thousands more SARs, and other highly sensitive material relating to Russia, Iran, and the terrorist group known as the Islamic State of Iraq and the Levant (more commonly known as "ISIL" or "ISIS"), to a flash drive. (Compl. ¶¶ 12(b), 14(b); PSR ¶ 11.) She saved the majority of the files to a folder she labeled "Debacle – Operation-CF," and subfolders bearing names such as "Debacle\Emails\Asshat." (Compl. ¶ 14(b); PSR at 22.) There was no official FinCEN project or task bearing these titles or names, and no legitimate purpose for the defendant to collect and save these files to the flash drive, much less to do so and then remove the files from FinCEN's office, where they were protected from being made public, intentionally or inadvertently. (Compl. ¶¶ 14-15; PSR ¶ 11.) Forensic data indicates that she first began saving SARs to the flash drive by at least on or about October 18, 2017, approximately 11 days prior to the publication of the first SAR Disclosures article. She then transmitted them to Reporter-1 using the Encrypted Application. In total, the defendant sent approximately 50,000 documents, including more than 2,000 SARs, to Reporter-1.

As the sheer quantity of the disclosures shows, the defendant did not limit the information she shared with Reporter-1 to certain discrete "issues" (Def. Mem. 47). Nor did the defendant only share with Reporter-1 what the defendant purportedly thought the public should know with respect to such issues. (*Contra id.* (claiming she merely acted to seek "to get the proper attention

for the issues she believed were of vital importance to national security.").) Rather, she unlawfully disclosed thousands of SARs, and other documents, on a vast range of topics and persons.

D. The Defendant's Running of Searches for Reporter-1

In addition to providing Reporter-1 with SARs, the defendant also repeatedly ran searches within FinCEN's internal systems at Reporter-1's request, gathering information Reporter-1 wanted, and provided Reporter-1 with the results. For example, on or about December 17, 2017, Reporter-1 asked the defendant, "Hey do you have any insight or details about this you can share?" and provided her with a link to a news article describing an ongoing investigation into potential terrorism funding. The defendant responded with BSA-protected information, writing in part, "4 SARs [at a specific] Bank in [a specific place]." She expressed no hesitation, notwithstanding that the article said the investigation was ongoing, and the subject was terrorist financing and not one about which she had expressed concern in her various complaints.

This was not an isolated event. (*See* PSR ¶ 15.) Rather, as described above, none of the contents of any SAR or analysis thereof unlawfully disclosed by the defendant concerned alleged misconduct at FinCEN (or at any other government agency). (PSR at 23, 25.)

II. The Interview With Law Enforcement

On October 16, 2018, federal law enforcement agents approached and interviewed the defendant. (PSR ¶ 20.) She initially falsely denied having contact with any member of the news media. (*Id.*) Instead, she attempted to deflect the investigation away from herself by stating that two *other* FinCEN employees were in contact with the news media. (Compl. ¶ 22.)

Upon direct questioning regarding Reporter-1, the defendant changed her story and admitted that, on numerous occasions, she accessed SARs, photographed them, and sent those photographs to Reporter-1 using the Encrypted Application. (PSR ¶ 20.) During the same interview, the defendant claimed that although she did this, she was a "whistleblower" who merely

provided the SARs to Reporter-1 for "record keeping." (*Id.*) That was false. The defendant similarly claimed not to have read the articles published by Reporter-1, and to have no knowledge that the SAR information she disclosed to Reporter-1 was in fact published. That too was false.

As noted above, these claims were expressly refuted by the defendant's own internet search history—and her own contemporaneous words to Reporter-1. (Compl. ¶¶ 22, 26.) The defendant was placed under arrest following the interview.

III. The Searches

In conjunction with the interview of the defendant, multiple premises and electronic searches were conducted pursuant to judicially-authorized warrants. The search of her personal cellphone revealed hundreds of messages between her and Reporter-1 exchanged using the Encrypted Application. (PSR ¶ 12.) These messages included the direct transmission by the defendant of more than 2,000 SARs to Reporter-1, as well as numerous other sensitive analyses taken from FinCEN, such as reports on criminal trends or particular persons charged with or suspected of committing crimes. (PSR ¶ 14.) A search of the defendant's person resulted in the seizure of the flash drive containing thousands of SARs. (Compl.¶ 23; PSR ¶ 11; PSR at 22.)

A search of her home revealed that she also improperly stored sensitive government information in her home, including internal FinCEN communications. (PSR ¶ 18.) On one occasion, she wrote to Reporter-1 about this conduct, stating that her young daughter found this material and astutely asked, "mom is this suppose[d] to be here in the house[?]" (*Id.*) The defendant recounted that when she told her daughter that the material was intentionally kept there, her own daughter responded in part, "great . . . . We have govt secrets in a big box in the middle of o[u]r floor." (*Id.*)

The defendant also shared at least some of the same sensitive information improperly stored in her home with Reporter-1. (PSR ¶ 18; PSR at 24.) In or about 2016, officials at the

Treasury Department informed the defendant that a particular electronic document she circulated within FinCEN was believed to contain classified information and was accordingly removed from Treasury's non-classified electronic system. (PSR at 24.) The defendant's security clearance was temporarily suspended as a result of this incident and another similar incident (facts she omits in her submission, suggesting that there was no legitimate basis for the suspension (*see* Def. Mem. 40)). Subsequently, the defendant took a hard copy of that same document home without authorization. (PSR at 24.) Then, in or about late July 2017, the defendant sent the relevant portion of that document to Reporter-1 via the Encrypted Application. (*Id.*) When transmitting the document to Reporter-1, the defendant told Reporter-1 that Treasury had previously told the defendant that the document was classified. (*Id.*)

IV. The Charges And The Guilty Plea

Following her interview and the searches executed on October 16, 2018, the defendant was charged in Complaint 18 Mag. 8861 with unlawfully disclosing SARs, and conspiracy to do the same, in violation of 31 U.S.C. § 5322(a), 31 C.F.R § 1020.320(e)(2), 18 U.S.C. §§ 371 and 2. On January 30, 2019, she waived indictment and was arraigned on a two-count information, charging the same offenses. (PSR ¶ 1.) She entered a guilty plea to Count One of the Information on or about January 13, 2020, pursuant to a written plea agreement. (PSR ¶ 4.)

V. Post-Plea Events

Since the defendant's guilty plea and during the pendency of sentencing in this case, the impact of her unlawful SAR disclosures has grown. Reporter-1 shared thousands of SARs unlawfully disclosed by the defendant with publications around the world, and recently published

an analysis and descriptions of the trove as "The FinCEN Files."[6] Reporter-1 has promoted the trove through a podcast series, which publicly described the materials supplied as "a vast x-ray of the entire international banking system" "sent to [Reporter-1 and a colleague] for some reason" that they did not understand. *Suspicious Activity: Inside the FinCEN Files* Podcast, Episode 1, 24:28-24:45, 24:56-25:20, *available at* https://podcasts.apple.com/us/podcast/suspicious-activity-inside-the-fincen-files/id1531918384.

Meanwhile, the defendant has used a Twitter account (@WhyRUanId10t), registered to her personal email address but publicly appearing in the name "Isabella," to attempt to generate support for herself and to draw attention to her disclosures. Beginning on or about September 20, 2020, the day the "FinCEN Files" were published, the defendant used this account repeatedly to re-tweet articles broadcasting the illegally disclosed information. She also repeatedly used the same account to re-tweet information about her own case, claiming, among other things, that she is a "whistleblower" unfairly suffering criminal consequences, and attempting to popularize a hashtag in support of herself ("#treasurenat") while speaking of herself in the third-person. As recently as on or about September 4, 2020, she re-tweeted a statement, using her "Isabella" account, that read, in part, "Natalie Mayflower Sours Edwards was framed." (*See* Ex. B.) That is, of course, nonsense. She admitted her guilt under oath, and the evidence of her guilt is overwhelming.

The defendant's disregard for the BSA and the personal information of uncharged individuals also continued. Despite her guilty plea, the defendant claimed in an administrative

---

[6] The Government does not expect the defendant to dispute her responsibility for the unlawful disclosures underlying The FinCEN Files, nor could she reasonably do so. The data disclosed in the The FinCEN Files matches unlawful disclosures of more than 1,000 SARs made by the defendant to Reporter-1, largely on or about September 1, 2018, as discussed *infra*, and the entirety of the published trove predates her arrest.

proceeding that she was suspended from FinCEN in retaliation for purported whistleblowing, when she was in fact suspended after she was charged criminally in this case. In that administrative proceeding, in which she proceeded *pro se*, on or about June 2, 2020, she filed BSA-protected information with detailed data on the financial transactions of others. An emergency motion to seal this material then had to be filed, which the administrative law judge promptly granted. (PSR ¶ 26; *see also* Ex. C (published at *Edwards v. Dep't of the Treasury*, M.S.P.B. No. DC-1221-20-0480-W-1, 2020 WL 4048396 (July 17, 2020)), at 3, 7.)

THE PRESENTENCE REPORT

Consistent with the plea agreement, the presentence report reflects a total offense level of 6, and that the defendant is in criminal history category I. (PSR ¶¶ 36, 39.) The advisory United States Sentencing Guidelines ("Guidelines") range is therefore zero to six months' imprisonment. (PSR ¶ 86.)

The Probation Office recommends a sentence of two years' probation, effectively the bottom of the Guidelines range, because the defendant is a first-time, non-violent offender, and has certain health or mental conditions. (*See* PSR at 29.) The Government strongly disagrees with that recommendation.

As an initial matter, the applicable advisory Guidelines range does not account for the pertinent factors in this case. Rather, the offense of conviction has no Guideline unique to it, and thus none that accounts for the nature, circumstances, and scope of the offense. Indeed, the range would be the same regardless of whether the defendant shared one SAR, or one hundred SARs, or, as she did, thousands of SARs. It also would be the same regardless of whether she shared SARs once, or over a short period, or, as she did, repeatedly over approximately a year. It would similarly be the same regardless of whether she was a low-level or inexperienced employee, or whether, as was the case, she had a PhD, had worked for multiple agencies in the federal government, and was

a senior official. The Guidelines range thus merits less weight than it does in many cases because it fails to account for the pertinent factors relevant to determining an appropriate sentence.

Consideration of the factors set forth in 18 U.S.C. § 3553(a)(1)-(2) should play the principal role at sentencing. As set forth below, those weigh strongly in favor of a meaningful term of imprisonment.

ARGUMENT

I. A Meaningful Term of Imprisonment is Warranted

A. The Nature and Circumstances of the Offense

The magnitude of the defendant's unlawful disclosures is unparalleled in FinCEN's history. She disclosed approximately 50,000 FinCEN records, containing at least 2,000 individual SARs, along with highly sensitive reports and analyses, including with respect to pending matters. As noted above, and is not disputed, many of these materials related to ongoing investigations of significance, such as those involving Paul Manafort, Richard W. Gates, Russian diplomatic accounts, and other matters associated with the 2016 federal election, as well as financing of Hezbollah and other foreign terrorist organizations, and the activities of countless other persons under potential or actual investigation. In addition, numerous materials released by the defendant exposed the private financial dealings of uncharged persons merely suspected of potential wrongdoing, who are presumed innocent unless charged and proven guilty, and whose personal information is entitled to respect and confidentiality.

In her submission, the defendant repeatedly makes sweeping, generalized claims that she was a "whistleblower," and broadly asserts that she has been prosecuted for revealing "[p]olicies and practices [that were] were putting American lives at risk." (Def. Mem. 52.) That is both inflammatory and false.

As discussed above, the defendant's claims of alleged misconduct at FinCEN were thoroughly vetted, considered, and refuted. In any event, that she may have been believed incorrectly, at one time, that FinCEN engaged in wrongdoing does not explain, much less excuse, her own engagement in wrongdoing. The defendant was well aware that there were channels available within the federal government to raise claims of alleged government misconduct, and she in fact availed herself of those channels, contacting OIG, OSC, and Congress. But in addition to availing herself of these channels, the defendant disclosed thousands of disparate SARs, implicating myriad people, entities, and investigations, the contents of which had no relationship whatsoever to her claims of government misconduct.

In her submission, the defendant does not dispute that she did this, but suggests it can be understood because in addition to her claims of alleged wrongdoing within FinCEN, she also believed that FinCEN had improperly failed to provide to Congress certain SARs that it had requested, and thus she disclosed them to Reporter-1. (*See* Def. Mem. 49-50.) That does not make sense.

As an initial matter, even if the defendant sincerely held the view that FinCEN was improperly withholding SARs on certain subjects from Congress, it does not explain why she provided SARs about a variety of private parties, having nothing to do with those subjects, to Reporter-1. Likewise, this view does not explain why she provided SARs to Reporter-1 so Reporter-1 could publish the contents of those SARs. The defendant did not transmit the SARs for which she stands to be sentenced to Congress; she transmitted them to Reporter-1, with the knowledge and understanding that Reporter-1 was publishing the information. (*See* Def. Mem. 51 (acknowledging the defendant "disclosed SARs of her own volition. [Reporter-1] did not force

her or trick her. [Reporter-1] used the material to publish articles. She read the articles and provided more SARs.").)

Moreover, it appears that the defendant attempted to manufacture a basis to say that FinCEN withheld information from Congress, as she now asserts in an attempt to excuse her criminal conduct. For example, on or about October 28, 2017, she wrote to Reporter-1, "We can roll w a 'conspiracy theory' but make sound factual to get the Hill to write more letters to FinCEN requesting info . . . depends on how ya want to spin it . . . ya want to put info out on Manafort and lead it as it is . . . smoke and mirrors and then say why . . . ."

Similarly, in another exchange, on or about January 18, 2018, the defendant told Reporter-1, in part, "I cannot dig without a justification. I did the other [request from Reporter-1] bc it was in the Congressional letter ... I havnt seen a letter w this name ???" In short, the defendant knew that she was not permitted to search FinCEN's records ("dig") for Reporter-1, and was able to do so undetected previously by cloaking those searches as part of purportedly complying with a Congressional request—just as she now appears to claim she was doing—and needed another way to "justif[y]" her actions.

In any event, the defendant was herself *directly* able to contact and meet with congressional staff members multiple times, as she acknowledges, to air her claims. (Def. Mem. 2-3, 38-39, 41, 51; *see also* Def. Ex. DDD; Def. Ex. H at 3 n.3.) She did not need to use Reporter-1 as some kind of secret intermediary. But even if she did, that still does not explain her conduct. Not a single one of the defendant's claims of alleged wrongdoing by FinCEN involved the detailed personal information contained in a SAR, but that is precisely what she illegally and repeatedly shared with Reporter-1, and while knowing that Reporter-1 was going to publish the contents. These are the

actions for which she stands to be sentenced, not "uncovering" what she blithely and baselessly calls "corruption in the Treasury Department" (Def. Mem. 51).

Indeed, the defendant's repeated reference to herself as a "whistleblower," a word she uses throughout her submission, is misleading, at best. This past summer, in the proceeding in which the defendant contested her suspension from her position at FinCEN (from which she subsequently resigned), the administrative law judge considered the defendant's claims and found that she "failed to make a non-frivolous allegation that she engaged in whistleblowing activity." (Ex. C, at 8; *see also* Def. Ex. HHH, at 4.) In any event, providing SARs and other materials to a reporter that have nothing do the subjects on which one is attempting to "bl[ow] the whistle" (Def. Mem. 2) is not whistleblowing. Nor could the defendant, an experienced and well-educated individual, have possibly thought that providing SARs to a reporter somehow was in service of protecting the "privacy of the American people" (*id.* at 52). The opposite is true.

At bottom, what the defendant did, and why she did it, is far more disturbing than the picture she gives in her submission. And the most powerful proof of her state of mind is her own, contemporaneous words, sent over the Encrypted Application.

For example, on or about March 24, 2018, after Reporter-1 had published multiple articles reflecting SAR information disclosed by the defendant, the defendant complained that "[t]hey [a media outlet] keep talking about the fbi whistleblower [a different person] and I'm getting *sick of my stuff not coming* out. . . . Thx [first name of Reporter-1] but it's crazy you have to lobby on behalf of a government employee who has evidence of crimes being committed and had linked all the pieces I have with evidence tied to the former administration." (Emphasis added.)

Contrary to what she told Reporter-1, none of the SARs, or any other information that the defendant removed from FinCEN without authorization, related to alleged misconduct by "the

former administration." It appears that the defendant said this to seek to interest Reporter-1, and as part of an effort to seek to advance the defendant's own political agenda, which included disrupting or distracting from the investigation of Special Counsel Robert S. Mueller III, who she said, in a conversation with Reporter-1 in February 2018, "needs to go down too." Of course, none of the SARs called into question the basis or propriety of the Special Counsel's investigation either, although leaking certain of the SARs might reasonably have been expected to negatively impact it. And that was precisely what it appears the defendant hoped would happen.

The defendant's contemporaneous statements also make clear that she understood she did not have an ongoing relationship with Congress that involved her sharing sensitive information with Reporter-1 as a secret conduit. For example, on or about July 24, 2018, nearly a year into the defendant's illegal and repeated SAR disclosures, the defendant complained to Reporter-1, "Congress shouldn't have sat on their ass and not respond[ed] to me." Approximately one month later, on or about August 31, 2018, in the course of a conversation in which Reporter-1 stated that Reporter-1 would be speaking with congressional staff, the defendant told Reporter-1, "Oh and while we are on the wish list . . . I want to be Deputy Director of FinCEN so tell the powerful people to make that happen because I can run that operational bureau better than any of those assterds and I have the qualifications to do it. Yeah let me dream about that . . . ." A few weeks later, on or about September 20, 2018, the defendant again made clear that she was looking for a personal benefit, not merely serving Congress, stating:

> Yes, until Congress deleivers [sic] me something I'm inclined not to share anymore shit. I have yet to see anything concrete or they actually do anything for me other than meet. . . . It's just been a long two years with no tangible benefit to me. If Congress so calls has Kens ear [the Director of FinCEN] then they could tell him to promote me next week or do something tangible, but they hav[e]n['']t delivered and the mtg I had with [a congressional staffer] appeared as if they cannot deliver.

These are not the words of someone who cared only about the "American people" (Def. Mem. 52) and "the country's well-being" (*id.* at 53).

Nor are these isolated words. Rather, it appears that defendant was motivated from the inception, at least in material part, by her pursuit of a personal benefit and her interest in harming FinCEN. The defendant began communicating with Reporter-1 via the Encrypted Application on or about July 22, 2017. As the conversation continued over the next few days, the defendant expressed a desire to burn down FinCEN's proverbial house ("I burned the town and crops cleared out all the livestock and now I'm ready to catch the water on fire. Nothing left but ash!"), said she hoped to receive financial compensation for the purported "turmoil" and "retaliation" she claimed to have experienced at FinCEN, and wanted to have her perceived opponents prosecuted ("I want them all to go down and to jail"). On or about September 9, 2017, the defendant similarly stated, "[w]e want momma name on court settlement papers not on the front page of any news outlet . . . lol ."

Also telling is how the defendant reacted when a different federal employee leaked SARs. During the period of the defendant's criminal conduct, another government employee, at a different agency, also illegally disclosed SARs, namely those relating to Michael Cohen, to a third-party, lawyer Michael Avenatti, and admitted this conduct in an interview with *The New Yorker*. *See Missing Files Motivated the Leak of Michael Cohen's Financial Records*, The New Yorker (May 16, 2018), *available at* https://www.newyorker.com/news/news-desk/missing-files-motivated-the-leak-of-michael-cohens-financial-records; *Internal Revenue Service Analyst Pleads Guilty To Making Unauthorized Disclosure Of Suspicious Activity Reports*, Press Release, U.S. Attorney's Office for the Northern District of California (Aug. 15, 2019), *at*

https://www.justice.gov/usao-ndca/pr/internal-revenue-service-analyst-pleads-guilty-making-unauthorized-disclosure; *United States v. Fry*, 19 Cr. 102 (N.D. Cal. 2019).

Unlike the defendant here, that defendant publicly, though anonymously, asserted he had done so because he was concerned that these particular SARs allegedly were being hidden from or were unknown to criminal investigators, whom he believed needed them to complete their investigation. When learning of Fry's then-anonymous statements to *The New Yorker* on or about May 18, 2018, the defendant did not draw a parallel to herself; instead, she told Reporter-1, "What he did was illegal . . . why the fuck would he want to out himself?" She continued, "I swear if he has a fucking attorney is going for a lawsuit settlement I am going to be pissed the fuck off." Moments later, she disclosed more detailed SAR information to Reporter-1, and further disclosed that it was part of an "active case" at FinCEN.

Nor was the defendant's conduct confined to an isolated incident of poor judgment, or to a short period. On the contrary, the defendant transmitted SARs to Reporter-1 on multiple occasions over at least a year. She watched as Reporter-1 repeatedly published the SAR information she unlawfully provided. She expressed a desire to damage FinCEN ("Nothing left but ash!"), for her perceived opponents to be prosecuted for unspecified purported wrongs ("I want them all to go down and to jail"), and to hinder lawful investigations by leaking potentially relevant or distracting material (Special Counsel Mueller "needs to go down too"). She paid no heed to the harm she was causing, because, it appears, that harm was one of her objectives.

Indeed, nearly a year deep into her crime, on or about September 1, 2018, the defendant illegally disclosed approximately *1,500* more SARs to Reporter-1. This was months after Reporter-1 had published articles centering on the defendant's purported whistleblower claims. And by this time, as noted above, independent audits had been conducted of the defendant's

complaints of wrongdoing within FinCEN, which found no wrongdoing. It is inconceivable that, at this point, the defendant could have believed that a mammoth disclosure of BSA-protected, confidential material, which did not describe alleged misconduct at FinCEN, nevertheless served her professed interest in remedying alleged misconduct at FinCEN.

To be sure, in the course of the lengthy conversation, the defendant also complained, as she had previously, about FinCEN's alleged failure to respond properly to congressional requests. But the defendant did not attempt to limit what she shared with Reporter-1 only to that which allegedly had been improperly withheld from Congress—even assuming *arguendo*, and contrary to both common sense and the undisputed record, that she somehow believed that she could not send materials to Congress directly. Nor could a disclosure of this magnitude possibly have been narrowly targeted to include only information that the defendant thought otherwise should be made public, despite the law requiring its confidentiality. Indeed, in addition to the numerous SARs, the defendant also sent Reporter-1 multiple confidential, law enforcement-sensitive reports and analyses of financial and criminal trends and/or the actions of individuals who had been criminally charged or were under investigation. One was titled "[last name of charged individual]_i2 Analytic Report v6 - final version for FBI.doc." Another was "SAR Subject Country Study Summary by Suspicious Activity Type.xls." A third was "261869_[foreign country]_Report.doc." The defendant omits these disclosures from her submission. They plainly had nothing do with purported whistleblowing or a belief that specific materials had been improperly withheld from Congress.

Notably, these disclosures occurred only one day after the defendant's "I want to be Deputy Director of FinCEN" statement described above, and the 1,500 SARs were shared in batches only

four minutes after Reporter-1 stated, "Your 'demands' will definitely be met I can tell you that much." The defendant did not express surprise or confusion at the word "demands."

Nor was this the first or the only time when the defendant sent Reporter-1 sensitive law enforcement reports and analyses. For example:

- On or about November 8, 2017, she sent Reporter-1 a memorandum with the title "[Certain foreign country] Transactions May Be Linked to [event]."
- On or about January 26, 2018, she sent Reporter-1 a targeting report for the FBI Chicago Field Office, titled "Money Laundering Network and Illicit Financial Activities of [certain foreign national]."
- On or about September 2, 2018, the day after she shared the numerous SARs and reports discussed above, she sent Reporter-1 a memorandum "to the FBI pertaining to Foreign Suspicious Wires to [certain state] Real Estate Company."
- The same day, she sent other reports, including another memorandum for the FBI, titled "The [name] Financial Network . . . .", which concerned organized crime.
- Less than two weeks later, on or about September 13, 2018, she sent more reports, including one drafted for both internal use and for sharing with a foreign partner of FinCEN, concerning transactions in a certain part of the world, and an unclassified intelligence assessment containing BSA information titled "Financial Nexus between [certain foreign area] Crime Figures and US Residents."

Again, none of this had anything to do with purported whistleblowing or a belief that specific materials had been improperly withheld from Congress.

The vast scope of the unlawful disclosures; the repetition of the crime over the course of a year; the defendant's knowledge that the information would be published again and again; the lack of any conceivable reason to believe that public disclosure would serve the public, coupled with the partisan hope that, on the contrary, public disclosure might hinder or distract from lawful investigations; and the defendant's interest in both damaging a public institution and gaining a personal benefit, all set this case far apart from *United States v. Fry*, 19 Cr. 102 (N.D. Cal. 2019), the prosecution for unlawful SAR disclosures referenced above. In *Fry*, the defendant engaged in

a single act of disclosure regarding a single subject, indisputably motivated by a mistaken belief that the SARs he disclosed had been wrongfully hidden from law enforcement, and sent the information to an attorney, whom the defendant did not expect to publicly publish the information. *See Fry*, Dkt. No. 47 (Sentencing Tr.). Observing the defendant's "deep regret" for his error of judgment, the court imposed a sentence of probation for this singular "aberration" in the defendant's otherwise "spotless" record of professional and personal conduct. *Id*. at 26.

The nature and circumstances of the offense here bear no resemblance to that in *Fry*. Unlike the defendant in *Fry*, this defendant leaked thousands of SARs and other materials, on repeated occasions, directly to the news media, on an array of topics ranging from potential foreign interference in the 2016 federal election to terrorism funding, and has offered no credible explanation, let alone shown remorse, for her conduct. To the contrary, she took steps to cover up her conduct, concocted false cover stories, lied to the FBI, and both continued to disclose sensitive information in another forum (her baseless administrative proceeding) and to engage in deceptive acts to cast herself as a victim (through her Twitter account in another name). As noted above, she scoffed at Fry's sincerity, stating, "I swear if he has a fucking attorney is going for a lawsuit settlement I am going to be pissed the fuck off." Those words speak volumes. In short, the defendant could not believe that someone would disclose SARs, and risk criminal prosecution, purely out of a desire to serve the public—because that is not what she was doing.

B. The Seriousness of the Offense

The defendant's crime was also incredibly serious. As the court noted in *Fry*, "the integrity of [a federal agency] and its enforcement process is compromised and the breach of the public's trust [is] severely compromised" by unauthorized disclosures of SARs, particularly when this crime is committed by a federal employee. *Fry*, Dkt. No. 47, at 26. The fact that the consequences

of the defendant's actions cannot be readily quantified does not make those consequences less real. As FinCEN explains:

> When SAR information is mishandled, it erodes public confidence in the financial sector's—and FinCEN's—ability to safeguard private financial information. Moreover, the reporting financial institution's security, and that of its personnel, is jeopardized when SAR information is improperly disclosed, producing a chilling effect on financial institutions' willingness to file SARs, and SARs that contain sufficiently detailed, and thereby useful, information.
>
> . . . An average of 30,000 searches of the BSA database are conducted each day by approximately 12,000 law enforcement and other authorized government agencies nationwide. Countless investigations are originated and informed by the sensitive and confidential information included in SARs and other BSA reports. Unauthorized disclosures of this protected material undermine ongoing law enforcement investigations and can result in the destruction of evidence, witness intimidation, and other serious consequences.
>
> . . . FinCEN and financial intelligence units around the world work together every day to exchange significant intelligence in support of law enforcement efforts. Such international cooperation is anchored in trust that each country will handle the information appropriately, as well as confidence that the systems used to transmit and store the information is secure. Unauthorized disclosures by senior inside officials, such as Defendant, undermine FinCEN's relationships and can cause irreparable harm to the United States' reputation and operational partnerships with foreign stakeholders.

(Ex. A, at 3-4; *see also id*. at 5 ("Defendant's actions are a breach of trust that is unprecedented in FinCEN's 30-year history.").) Our governmental institutions rely upon holding themselves and their employees to the highest standards, to gain the public's trust, and to build lasting domestic and international partnerships needed to perform their duties. Misconduct from within the organization, especially vast misconduct like the defendant's, shatters those principles and threatens irreparable harm to the institution and its public mission.

C. The History and Characteristics of the Defendant

The seriousness of the defendant's crime, and the need for a meaningful sentence, is only heightened by the flippancy and hypocrisy with which she continues to regard that crime. The defendant illegally disclosed thousands of records of private information, belonging to countless individuals, for public consumption, yet now claims that she did so because she feared "[t]he privacy of the American people—an almost reverence for which had been imprinted on her during service in the [Intelligence Community]—was not being respected." (Def. Mem. 52.) That hyperbolic claim is untethered from reality.

It was the defendant who demonstrated no respect for the "privacy of the American people." It was the defendant who put at risk countless investigations by revealing the existence and contents of SARs. It was the defendant who aided potential money launderers, terrorist financing networks, and other criminal actors by publicly disclosing the sensitive government analyses meant to assist in the detection and tracking of their conduct. Blinded by her own apparent sense of self-righteousness, the defendant remains unwilling to acknowledge the gravity of what she did. It is wholly appropriate that the Court take that into account at sentencing.

The Court should also take into account that the defendant indisputably knew—and knows—far better. She is highly educated and holds a master's degree and a PhD. (PSR ¶ 68.) She had prior experience working in the federal government. (PSR ¶¶ 75-76.) She rose to a high-level position within FinCEN, serving as a Senior Advisor to the then-head of the Intelligence Division, earning more than $160,000 a year, and supervising others. (PSR ¶ 74.) As a senior official in that division, the defendant was charged with helping to "carr[y] out FinCEN's statutory responsibility to collect, analyze, and disseminate financial intelligence," including by working with "law enforcement, regulators, foreign financial intelligence units, industry, and the public; produc[ing] proactive, cutting edge, multi-source financial intelligence analysis; [and serving] as

global experts on illicit finance, providing data-driven tactical and strategic perspectives." *Intelligence Division*, FinCEN, https://www.fincen.gov/intelligence-division (last visited, Oct. 26, 2020). The defendant abused her knowledge, experience, and role to betray this mission—repeatedly. (*See* Ex. A, at 4-5 ("Defendant's position required an FBI background check, a TS/SCI security clearance, relevant training, and an oath of office, as she was entrusted with unique and unfettered access to FinCEN's repository of financial intelligence. By virtue of her position of trust, Defendant understood the innermost operations of the United States' financial intelligence system, an advantage she ultimately exploited for criminal purposes.").)

Moreover, notably absent from the defendant's letters of support are any from her former colleagues at FinCEN. Unlike in the *Fry* case, not a single former colleague has endorsed the defendant's character, let alone endeavored to explain, much less defend, her actions. That is telling. It is also unsurprising, because the evidence shows that the defendant's tenure at FinCEN, even apart from her crime, was far from admirable. Throughout the time of the investigation, the defendant took improper advantage of a generous telework arrangement from FinCEN (one that predated the COVID-19 pandemic), often not even logging on to FinCEN's systems when purportedly teleworking, and appearing at FinCEN offices only three days in a nearly one-month period in fall 2018. (*See* PSR ¶ 19.) Indeed, she boasted to Reporter-1 about not working when she should have been, sending Reporter-1, on or about August 28, 2018, what appeared to be a photograph of her by a pool during the workday, responding "fuck Em," when Reporter-1 called that "[p]laying hooky," and adding she would be "home tomorrow too."

During this same period, while the defendant appears to have been performing few, if any, of her actual duties, she unlawfully disclosed approximately 1,500 SARs and other sensitive materials to Reporter-1. Judicially-authorized interceptions and the search of the defendant's

home also reveal that, around this same time, in or about October 2018, the defendant was taking illegal steroids and importing them from foreign suppliers, including Dianabol, a Schedule III controlled substance. (PSR ¶ 40.) In one intercepted call, the defendant expressed her agreement that "we're doing some illegal shit right here" and understanding that it was not possible to legally acquire this drug in the United States for personal use. (*Id.*) The defendant added that a doctor with whom she spoke was "not going to say anything," had omitted her drug use from her file, and advised her "you're not going to get your [security] clearance if you keep taking that." (*Id.*) However, when interviewed by the Probation Office in this case, the "defendant disclaimed the use of illicit substances." (PSR ¶ 66.) While the offense for which she stands to be sentenced marks the defendant's first criminal conviction, her illicit drug activity, and her duplicity in attempting to hide it, demonstrate that she was not leading an otherwise law-abiding life.

D. The Need for General Deterrence and to Promote Respect for the Law

Finally, a meaningful sentence is also necessary to adequately deter criminal conduct—in this case, an egregious abuse of public trust with reverberating ramifications for ongoing law enforcement investigations and interests worldwide—and to promote respect for the law prohibiting such destructive conduct. *See* 18 U.S.C. § 3553(a)(2)(A)-(B). It is imperative to send a resounding message to individuals with access to sensitive, protected information that with access comes responsibility, and flagrant violations of the public trust will be met with real consequences. (*See* Ex. A, at 5 ("Because of the seriousness of Defendant's breach, and the far-reaching consequences of her actions, FinCEN requests that the Court impose a significant sentence of incarceration that will stress the seriousness of this offense, and deter Defendant and others from engaging in similar criminal conduct in the future.").)

Moreover, the investigation here required the full panoply of investigative techniques and countless hours of work by a joint investigative team from the FBI and OIG, precisely because the

defendant took steps to conceal her criminal conduct. When such a case is successfully prosecuted, a substantial sentence is warranted. *See, e.g.*, *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) ("Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it."); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) ("Because economic and fraud-based crimes are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence." (internal quotation marks omitted)).

The defendant's suggestion that she need not be sentenced to any prison time to achieve robust general deterrence (*see* Def. Mem. 54) flies in the face of case law, logic, and human experience. And to the extent that this suggestion is grounded on the assertion that the defendant has suffered embarrassment or discomfort in light of case "publicity" (*id.* at 55), it should be rejected out of hand. The approach for which the defendant advocates would lead to the perverse result that sentences in those cases in which a defendant's crime is particularly violative of the public trust—and thus attracts public attention—would be the *lowest*. Moreover, in this case, the defendant herself has encouraged media attention (albeit while pretending to be someone else). She cannot reasonably do so and then argue that such attention warrants a lower sentence.

II. The Defendant's Arguments Are Unpersuasive

In her submission, the defendant seeks a non-incarceratory sentence on three principal grounds. None warrants what she seeks.

First, the defendant asserts that she merely acted to serve the public. That is false, as discussed at length above. Simply put, as evidenced by, among other things, the defendant's contemporaneous words, the story of this case is not of a government employee selflessly sharing confidential information, at great personal cost, so that the information could be published for the

sake of "the country's well-being" (Def. Mem. 53). It is far more disturbing, unjustified, and dangerous. The defendant's failure to show remorse, and attempts to mischaracterize her conduct "as an act of conscience" (*id.* at 55), further militate in favor of a meaningful term of imprisonment.

Second, the defendant asserts that she "has already been severely punished for this offense." (*Id.* at 56.) But publicity and resigning from one's position after abusing that position are not punishment—and to the extent they are, they are not sufficient in this extraordinary case.

Finally, she refers, without elaboration, to certain medical conditions. (*Id.*)[7] While it is of course appropriate for the Court to take such conditions into account, none here is unique, none prevented the defendant, who is only forty-two years old, from committing her crime or engaging in the post-plea conduct described above, and all can be treated appropriately, to extent treatment is necessary, in prison. As the Court is aware, the Federal Bureau of Prisons is well-equipped to handle all such conditions, including, if warranted, in a Federal Medical Center (although the defendant's conditions, some of which involve simply avoiding certain foods or being bitten by a particular insect, are not of the type for which a medical center is necessary).

[7] Although immaterial for present purposes, the document the defendant cites in support of this point is unsigned, and the Government understands that it was written by the defendant, not a doctor. (*See* Def. Ex. KKK, at 6 (referring to "my" conditions and what "I" have).)

CONCLUSION

For the reasons set forth above, the Government respectfully requests that the Court impose a meaningful term of imprisonment, at least as long as the top of the Guidelines range, a sentence that is sufficient but not greater than necessary to serve the legitimate purposes of sentencing.

Dated: New York, New York
October 26, 2020

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney

By: s/ Kimberly J. Ravener/Daniel C. Richenthal
Kimberly J. Ravener
Daniel C. Richenthal
Assistant United States Attorneys
(212) 637-2358/2109