

UNITED STATES DISTRICT COURT

for the
Southern District of New York

21 MAG 10685

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Attachments A-1 and A-2

Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A-1 and A-2

located in the Southern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachments A-1 and A-2

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 371, 2314, 2315, 2, 3, 4	conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods, interstate transportation of stolen property, possession of stolen goods, aiding and abetting, accessory after the fact, misprision of felony

The application is based on these facts:

See Attached Affidavit

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ [Redacted] (By Court with Authorization)

Applicant's signature

[Redacted] Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Facetime (specify reliable electronic means).

Date: 11/05/2021


Judge's signature

City and state: New York, New York

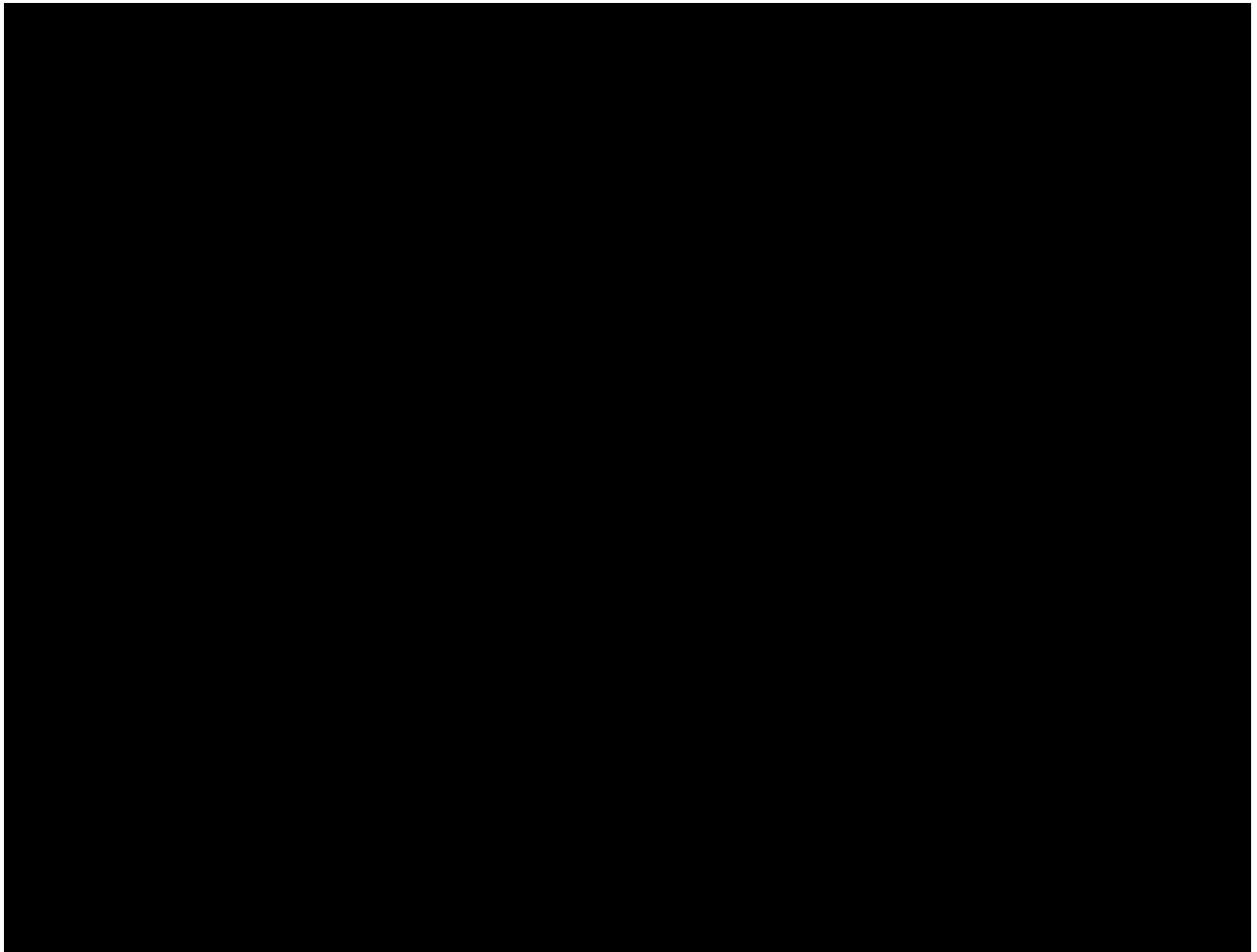
Hon. Sarah L. Cave, U.S. Magistrate Judge

Printed name and title

person (the “Subject Person”) specified below for, and to seize, the items and information described in Attachments A-1 through A-2. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

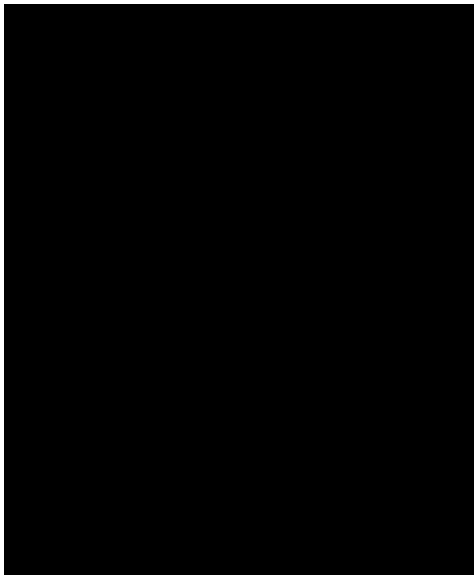
B. The Subject Premises

3. The Subject Premises, which is believed to be JAMES E. O’KEEFE, III’s residence, are particularly described as [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] in Mamaroneck, New York,
as depicted in the following photograph:



C. The Subject Person

4. The Subject Person to be searched is JAMES E. O'KEEFE, III, who was born on [REDACTED], and is depicted in the photograph below, and any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within O'KEEFE's immediate vicinity and control at the location where the warrant is executed:



D. The Subject Offenses

5. For the reasons detailed below, I believe that there is probable cause to believe that any cellphones in the possession of O’KEEFE or found within the Subject Premises contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the “Subject Offenses”).

II. Facts Establishing Probable Cause

A. Overview

6. Since in or about October 2020, the United States Attorney’s Office for the Southern District of New York and the FBI have been investigating apparently coordinated efforts by certain individuals to (a) steal personal items, some of which potentially are of significant value, from [REDACTED], who was located outside of New York at the times of the apparent thefts, and whose father, [REDACTED], was at all times relevant hereto a prominent public figure and, until his successful election in or about November 2020, a candidate for President of the United States, (b) transport one or more of those items from Florida to New York, and (c) use

what appear to be false identities to contact [REDACTED] and others associated with her by email, text message, and telephone, in an effort to induce her and her associates into confirming that the items belonged to her, including highly personal entries in a private journal.

7. Based on my participation in this investigation, I have learned, among other things, that beginning in or about September 2020, [REDACTED], an organization [REDACTED] [REDACTED]¹ engaged in what it referred to as “Operation [REDACTED],” which appears to be a coordinated undercover effort to obtain stolen items belonging to [REDACTED] from Delray Beach, Florida, transport them to [REDACTED] headquarters in Mamaroneck, New York, for their review and potential public dissemination for apparently political purposes, and, ultimately, coordinate their return to Delray Beach, Florida, in an apparent effort to obscure their prior possession of the items. Specifically, as explained in greater detail below, [REDACTED] arranged for the transportation from Florida to New York of stolen items belonging to [REDACTED] from [REDACTED] residence in Delray Beach, Florida, for potential public dissemination, and, ultimately, coordinated their return to Delray Beach, Florida, in an apparent effort to hide [REDACTED] prior possession of those items. Specifically, [REDACTED] [REDACTED], and [REDACTED], both employees of

1 [REDACTED]

[REDACTED] at the relevant time, appear to have directed and coordinated actions taken by employees of [REDACTED] and others in furtherance of Operation [REDACTED]. Further, [REDACTED] appears to have directed Robert Kurlander and Aimee Harris, both residents of Jupiter, Florida, who were not employed by [REDACTED], to transport certain of the stolen property from Delray Beach, Florida to New York in furtherance of the Subject Offenses.

B. [REDACTED]

8. [REDACTED]

[REDACTED]

9. [REDACTED]

[REDACTED]

10. [REDACTED]

[REDACTED]

11. [REDACTED]

[REDACTED]

[REDACTED]

12. [REDACTED]

[REDACTED]

13. [REDACTED]

[REDACTED]

14. [REDACTED]

[REDACTED]

15. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

17. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

C. Probable Cause that the Subject Offenses Were Committed

[REDACTED] Initiates Operation [REDACTED]

18. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] .5

d. [REDACTED]

[REDACTED]

e. [REDACTED]

[REDACTED]

f. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

g. [REDACTED]

[REDACTED]

[REDACTED]

h. Based on my participation in this investigation, and as discussed *infra*, I believe that Kurlander and Harris subsequently transported the [REDACTED] from West Palm Beach, Florida, to [REDACTED] in Mamaroneck, New York. [REDACTED]

[REDACTED]

[REDACTED]

⁵ [REDACTED]

[REDACTED]

i. On or about September 12, 2020, at approximately 2:30 p.m., Kurlander and Harris flew from Palm Beach Airport to Newark Airport, arriving at approximately 5:21 p.m. [REDACTED]

[REDACTED]

j. [REDACTED]

k. [REDACTED]

[REDACTED]

[REDACTED]

l. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

m. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

n. On or about September 18, 2020, at approximately 12:30 p.m., a phone number associated with Harris (the “Harris Cellphone Number”) placed a call to the [REDACTED] Cellphone Number, which lasted for approximately 17 minutes and 34 seconds. Later that day, at approximately 3:13 p.m., the Harris Cellphone Number placed a call to a phone number associated with [REDACTED] which lasted for approximately 1 minute and 53 seconds.⁷

6 [REDACTED]

7 [REDACTED]

o. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

p. [REDACTED]

[REDACTED]

[REDACTED]

q. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

r. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20. Based on my review of the contents of a cellphone provided by Kurlander and reviewed with his consent⁸ and records provided by AT&T, T-Mobile, and Apple, pursuant legal

[REDACTED] Accordingly, it appears that Harris lied to [REDACTED] about the disposition of [REDACTED] property.

⁸ Law enforcement agents' review of the contents of Kurlander's cellphone is ongoing. [REDACTED]

process including judicially authorized search warrants, I have learned, among other things, the following:

a. On or about August 19, 2020, Kurlander took photographs of the [REDACTED] inside his home (as confirmed by date and geolocation metadata associated with the photographs). Accordingly, it appears that Kurlander obtained the [REDACTED] on or before that date.

b. On or about September 11, 2020, Kurlander took photographs of certain other items that were stolen from [REDACTED] inside his home (as confirmed by date and geolocation metadata associated with the photographs). Accordingly, it appears that Kurlander had also acquired certain other items stolen from [REDACTED] on or before that date.

c. [REDACTED]
[REDACTED]
[REDACTED]

d. On or about September 14, 2010, at approximately 3:00 p.m., Kurlander and Harris exchanged a series of text messages in which Kurlander stated, among other things, the following: “I’m expecting that they’re gonna pay up to \$100,000 each maybe more.” Based on my training and experience, and involvement in this investigation, I believe that Kurlander was referring to the amount of money that he expected [REDACTED] to provide as payment for the [REDACTED] and other of [REDACTED] property. Kurlander further informed Harris that he had structured the Contributor Agreement such that “10,000 is NOT your only payment as it was going to be written

[REDACTED]

and if this does turn into something good or blockbusting then I'll get us more money. They of course come across as the nicest people in the world but their job is to pay the least and they aren't your or my best friends. They are literally in a sketchy business and here they are taking what's literally a stolen diary and info (since the girl was there in JUNE which I didn't know until you told them) and trying to make a story that will ruin this girls life and try and effect the election. That girl [REDACTED] can easily be thinking all her stuff is there and not concerned about it." Based on my training and experience, and involvement in this investigation, I believe that Kurlander was informing Harris that he anticipated that [REDACTED] would provide multiple payments for the [REDACTED] and other of [REDACTED] property and that the [REDACTED] had been stolen from [REDACTED] residence where [REDACTED] had been residing as recently as June 2020 and that knowledge of that fact had been communicated to employees of [REDACTED]

e. On or about September 17, 2020, Kurlander took photographs of certain of [REDACTED] stolen property inside [REDACTED] residence. Some of those photographs appear to show the feet or hands of two different people, one male (apparently Kurlander) and one female (apparently Harris). [REDACTED]
[REDACTED] Accordingly, it appears that Kurlander and Harris removed additional items of [REDACTED] property from [REDACTED] residence on that date, when [REDACTED] was not present.

f. On or about September 17, 2020, at approximately 6:19 p.m., Harris sent Kurlander an email in which she forwarded wiring instructions that she received from [REDACTED], a paralegal who appears to be employed by [REDACTED] a law firm focusing on marital and family law, stating that funds could be wired to the trust account for the [REDACTED]
[REDACTED]

g. [REDACTED]

[REDACTED]
Further, between on or about September 3, 2021, [REDACTED], and on or about September 18, 2020, [REDACTED], the Harris Cellphone Number exchanged nine calls with a phone number associated with [REDACTED] which lasted a total of approximately seventeen minutes.

h. Based on my participation in this investigation, I know that Kurlander sent [REDACTED] a text message informing him that “[w]e don’t want to do more or anything else or give anything else until we have some consideration spelled out. We are doing everything we say we will do. It’s just not fair. We are taking huge risks. This isn’t fair.” Kurlander saved a screenshot of the message, which appears to have been sent through an encrypted online messaging platform, although the original message does not appear to have been stored on Kurlander’s iCloud account. Based on the content of the message, I believe that this message was sent between on or about September 13, 2020, when Kurlander and Harris traveled to New York at the expense of [REDACTED], as discussed *supra*, and on or about October 20, 2020, when Kurlander and Harris received an executed copy of the Contributor Agreement, as discussed *infra*.

i. [REDACTED]

[REDACTED]
Kurlander saved a screenshot of this message, which appears to have been sent through an encrypted online messaging platform, although the original message was not stored on Kurlander’s iCloud account. Based on the content of the message, I

m.

[REDACTED]

n.

[REDACTED]

[REDACTED]

21.

[REDACTED]

[REDACTED]

[REDACTED]

22. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

23. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

e. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

f. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

24. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

26. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

27. [REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

d. [REDACTED]

[REDACTED]

[REDACTED]

e. [REDACTED]

[REDACTED]

[REDACTED]

f. [REDACTED]

[REDACTED]

[REDACTED]

g. [REDACTED]

[REDACTED]

⁹ [REDACTED]

h. [REDACTED]

[REDACTED]

[REDACTED]

i. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

j. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

k. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

m. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

n. On or about September 30, 2020, at approximately 9:26 a.m., Kurlander exchanged a call with a phone number associated with [REDACTED], Kurlander's attorney, which lasted for approximately one minute.

o. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

p. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

q. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

r. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

s. [REDACTED]

[REDACTED]

[REDACTED]

t. [REDACTED]

[REDACTED]

[REDACTED]

u. [REDACTED]

[REDACTED]

v. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

w. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

28. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

29. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

c. On or about October 8, 2020, at approximately 9:19 a.m., Kurlander sent a text message to an individual saved in Kurlander’s phone as [REDACTED] stating, among other things, the following: “Can a police office [*sic*] like you bring up a drivers license by full name?” Kurlander further stated that the name he wished to have run was “[REDACTED]” and inquired “Can you have it run this am?”

d. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

e. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

f. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

g. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

h. [REDACTED]

[REDACTED]

i. [REDACTED]

[REDACTED]

j. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

30. Based on my review of records obtained from T-Mobile, I know that between on or about October 13, 2020 and on or about October 16, 2020, the Kurlander Cellphone and the [REDACTED] Cellphone (which belonged to [REDACTED] Kurlander's attorney) exchanged two calls, which lasted for a total of approximately one minute and thirty-two seconds. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

31. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹² [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

32. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13 [REDACTED]

33.

[REDACTED]

34.

[REDACTED]

35.

[REDACTED]

36.

[REDACTED]

[REDACTED]

[REDACTED]

37. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

38. [REDACTED]

[REDACTED]

[REDACTED]

39. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹⁴ Scarsdale, New York, is adjacent to Mamaroneck, New York, where [REDACTED] is based.

¹⁵ [REDACTED]

[REDACTED]

40. [REDACTED]

[REDACTED]

41. [REDACTED]

[REDACTED]

42. [REDACTED]

[REDACTED]

16 [REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

43. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

44. [REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED] Further, the Kurlander Cellphone exchanged four calls with the [REDACTED] Cellphone, which lasted for a total of approximately four minutes and forty-five seconds.

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d. On or about November 6, 2020, at approximately 10:55 a.m., the Harris Cellphone Number placed a call to the [REDACTED] Cellphone Number, which lasted for approximately 41 minutes and 44 seconds.

e. On or about November 7, 2020, at approximately 3:50 p.m., the Kurlander Cellphone exchanged approximately eight text messages with the [REDACTED] Cellphone.

f. [REDACTED]

[REDACTED]

g. [REDACTED]

[REDACTED]

[REDACTED]

45. [REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

46. [REDACTED]

[REDACTED]

[REDACTED]

D. Probable Cause Justifying Search of the Subject Person and the Subject Premises

47. [REDACTED]

[REDACTED]

[REDACTED]

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

17 [REDACTED]

[REDACTED]

[REDACTED]

c.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

e.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

f.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

g.

[REDACTED]

h.

[REDACTED]

48.

[REDACTED]

a.

[REDACTED]

b.

[REDACTED]

¹⁸ Based on my training and experience, I have learned, among other things, that cellphones are capable of sending and receiving emails like the aforementioned emails.

[REDACTED]

[REDACTED]

c.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

* * *

49. In sum, based on the foregoing, there is probable cause to believe that [REDACTED] engaged in "Operation [REDACTED]," which appears to be a coordinated undercover effort to obtain the aforementioned stolen items belonging to [REDACTED] from [REDACTED] residence in Delray Beach, Florida, transport them to [REDACTED] in Mamaroneck, New York, for public dissemination, and, ultimately, coordinate their return to Delray Beach, Florida, in an apparent effort to hide [REDACTED] prior possession of those items. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

19

[REDACTED]

As specified in Attachment A-2, law enforcement agents will execute the requested warrant for cellphones in O'KEEFE's possession only if and when O'KEEFE returns to the Southern District of New York.

E. Probable Cause Justifying Search of ESI

50. Based on my training and experience, including my participation in this investigation and my review of the evidence described above, I know that individuals who engage in criminal activity such as the Subject Offenses commonly use cellphones to communicate with co-conspirators; keep track of co-conspirator's contact information; keep a record of illegal transactions and travel records; and store a digital or scanned version and/or photographs of stolen property. As a result, they often store data on their cellphones related to their illegal activity, which can include logs of online "chats" with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; photographs of stolen property; and/or records of illegal transportation or possession of stolen property. Moreover, I know that individuals generally keep their cellphones either on their persons or in their places of residence, in order to have easy access to them and to safeguard them.

51. Based on my training and experience, I also know that, where cellphones are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a cellphone for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on an electronic device, the data contained in the file does not actually disappear, but instead remains, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the device. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from an electronic device depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and user habits.

- In the event that a user changes cellphones, the user will typically transfer files from the old device to the new device, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

52. In addition to there being probable cause to believe that cellphones will be found in the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that the Subject Devices constitute instrumentalities of the Subject Offenses, because they were used to communicate with co-conspirators in furtherance of the Subject Offenses.

53. Based on the foregoing, there is probable cause to believe that any cellphones in the possession of O'KEEFE or found within the Subject Premises (collectively, the "Subject Devices"), contain evidence, fruits, and instrumentalities of the Subject Offenses. In particular, I believe the Subject Devices are likely to contain the following information:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED], [REDACTED], Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED] [REDACTED] stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED] stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

III. Procedures for Searching ESI

A. Unlocking Devices with Biometric Features

54. I further request authority to allow law enforcement agents to obtain from O'KEEFE (but not any other individuals present at the Subject Premises at the time of execution

of the warrants) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that O'KEEFE's physical biometric characteristics will unlock the device(s).

The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed above, there is reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

i. Due to the foregoing, I respectfully request that the Court authorize that, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, law enforcement

personnel may obtain from O'KEEFE the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of O'KEEFE to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O'KEEFE to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O'KEEFE to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by the proposed warrants.

B. Execution of Warrant for ESI

55. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any cellphones and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on cellphones is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because electronic data is particularly vulnerable to inadvertent or intentional modification or destruction, cellphones are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the cellphones that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of electronic hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from an electronic device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the device, which often take considerable time and resources for forensic personnel to detect and resolve.

C. Review of ESI

56. Following seizure of any cellphones and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period of August 1, 2020 through the date on which the Subject Devices are seized.

57. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation²⁰; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

²⁰ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

58. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

59. Additionally, because there is evidence that O'KEEFE communicated with attorneys with whom they or ██████████ may have had an attorney-client relationship, the review of the ESI from seized devices or storage media will be conducted pursuant to established screening procedures to ensure that the law enforcement personnel involved in the investigation, including attorneys for the Government, collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures will include use of a designated "filter team," separate and apart from the investigative team, in order to review potentially privileged communications and determine which communications to release to the investigation team.

D. Return of ESI

60. If the Government determines that the cellphones are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

61. Based on the foregoing, I respectfully request the court to issue warrants to seize the items and information specified in Attachments A-1 through A-2 to this affidavit and to the search and seizure warrants.

62. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrants and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.²¹

/s/ [REDACTED] (By Court with Authorization)

[REDACTED]
Special Agent
Federal Bureau of Investigation

Sworn to before me on this
5th day of November 2021,
by reliable electronic means.



HON. SARAH L. CAVE
UNITED STATES MAGISTRATE JUDGE

²¹ [REDACTED]

ATTACHMENT A-1

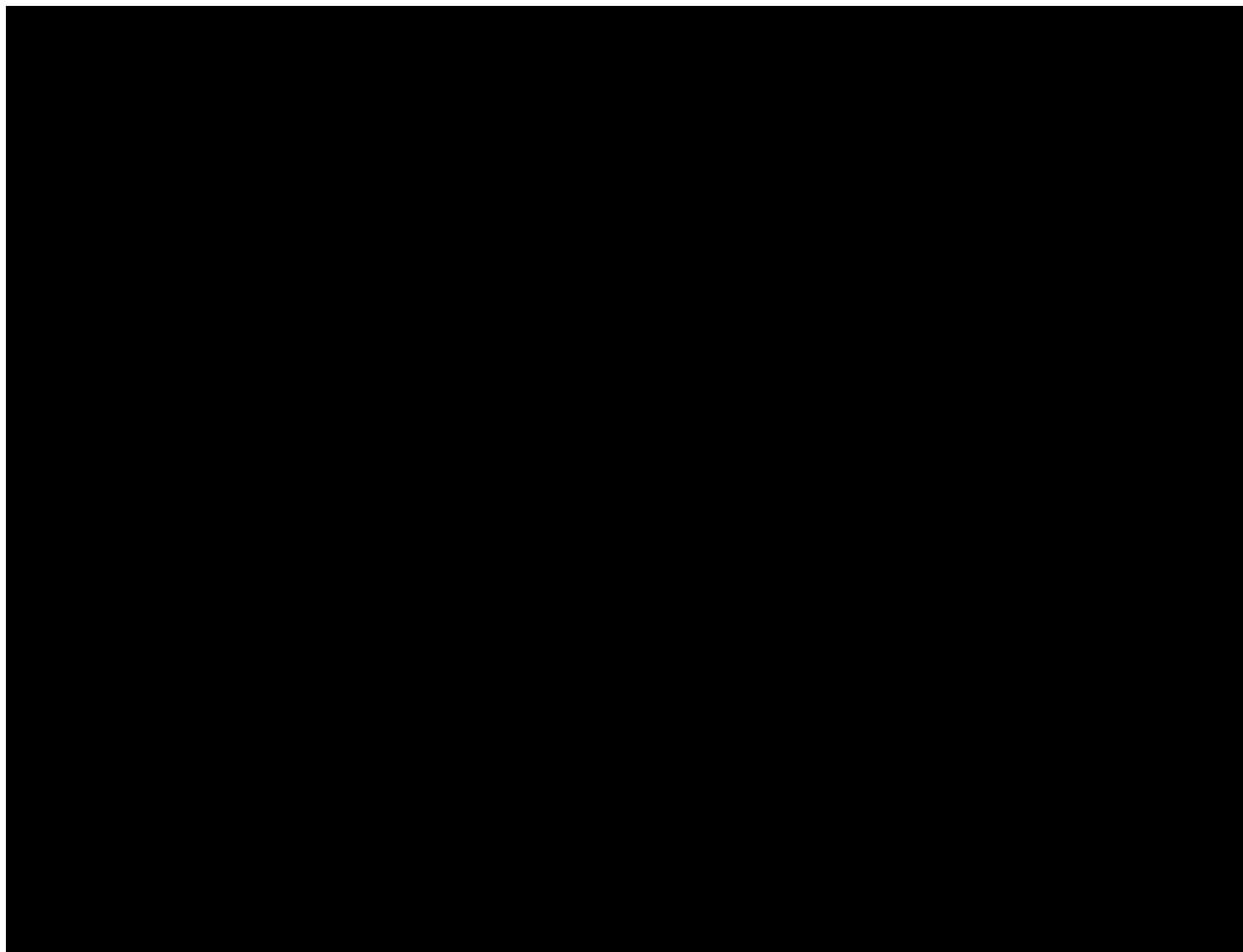
I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

An apartment known



in Mamaroneck, New York, as depicted in the following photograph:



II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the Subject Premises, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the “Subject Devices”).

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the “Subject Offenses”) for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED] Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED] stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators’ places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED] stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications

to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from James E. O’Keefe, III the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O’Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O’Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O’Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

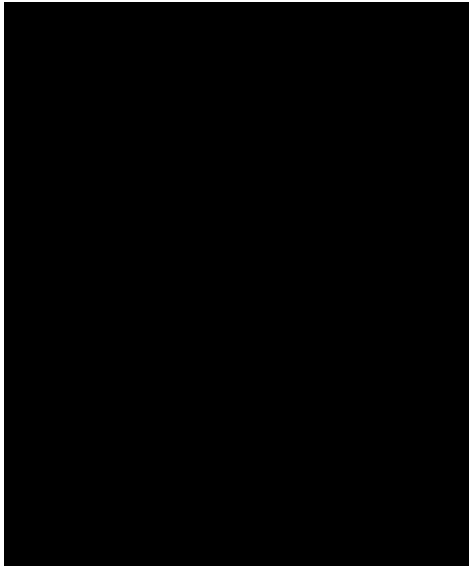
Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

ATTACHMENT A-2

I. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the possession, custody, or control of James E. O’Keefe, III, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the “Subject Devices”). The search of O’Keefe shall include any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within O’Keefe’s immediate vicinity and control at the location where the search warrant is executed. O’Keefe was born on [REDACTED] and is depicted in the following photograph:



The search of O’Keefe and seizure the aforementioned items is not authorized pursuant to this warrant unless the following condition occurs: O’Keefe is located in the Southern District of New York.

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the “Subject Offenses”) for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such

as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED] Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED] stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED] stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from [REDACTED] the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O'Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O'Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O'Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

21 MAG 10685

Case No.

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
the Premises Known and Described as)
Mamaroneck, New York)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York (identify the person or describe the property to be searched and give its location):

the Premises Known and Described as Mamaroneck, New York, as described in Attachment A-1

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A-1

YOU ARE COMMANDED to execute this warrant on or before November 19, 2021 (not to exceed 14 days)

[checked] in the daytime 6:00 a.m. to 10:00 p.m. [] at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to (United States Magistrate Judge)

[] Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

[] for days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: 11/5/2021 11:18am

Sarah L. Cave
Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A-1

I. Premises to be Searched—Subject Premises

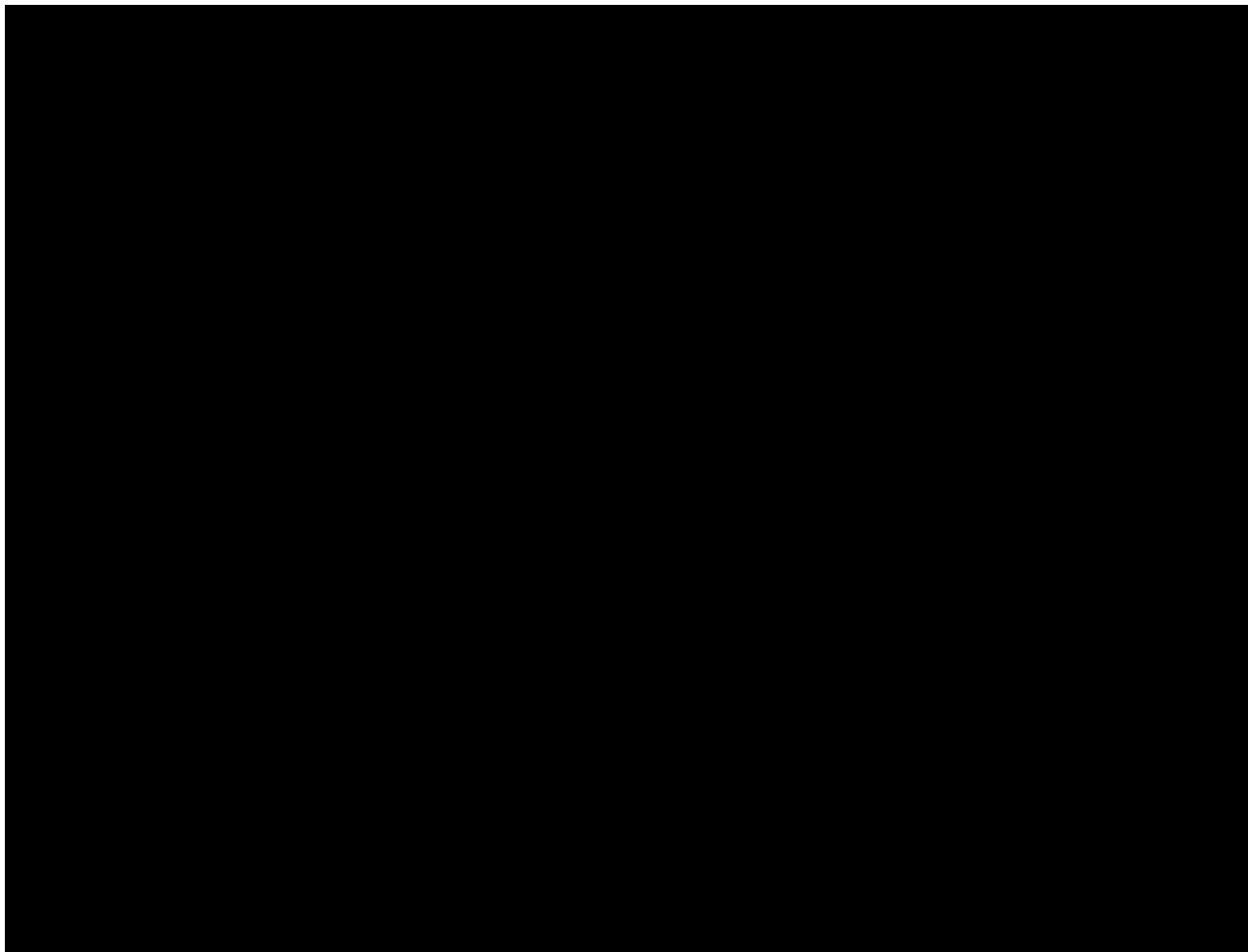
The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

An apartment known as



in Mamaroneck, New York, as depicted in the following

photograph:



II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the Subject Premises, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the “Subject Devices”).

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the “Subject Offenses”) for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED] Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED] stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators’ places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED] stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications

to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from James E. O’Keefe, III the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O’Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O’Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O’Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Any Cellphones in the Possession, Custody, or Control
of James E. O'Keefe, III

)
)
)
)
)
)
)

21 MAG 10685

Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

Any Cellphones in the Possession, Custody, or Control of James E. O'Keefe, III, as described in Attachment A-2

The search and seizure are related to violation(s) of *(insert statutory citations):*

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

See Attachment A-2

YOU ARE COMMANDED to execute this warrant on or before November 19, 2021 *(not to exceed 14 days)*

in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

for _____ days *(not to exceed 30)* until, the facts justifying, the later specific date of _____

Date and time issued: 11/5/2021 11:18am


Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
-----------	---------------------------------	--

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A-2

I. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the possession, custody, or control of James E. O’Keefe, III, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the “Subject Devices”). The search of O’Keefe shall include any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within O’Keefe’s immediate vicinity and control at the location where the search warrant is executed. O’Keefe was born on [REDACTED] and is depicted in the following photograph:



The search of O’Keefe and seizure the aforementioned items is not authorized pursuant to this warrant unless the following condition occurs: O’Keefe is located in the Southern District of New York.

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the “Subject Offenses”) for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such

as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED] Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED] stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED] stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from [REDACTED] the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O'Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O'Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O'Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

AO93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
the Premises Known and Described as [REDACTED])
[REDACTED], Mamaroneck, New York)
)

21 MAG 10685
Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

the Premises Known and Described as [REDACTED], Mamaroneck, New York, as described in Attachment A-1

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A-1

YOU ARE COMMANDED to execute this warrant on or before November 19, 2021 (not to exceed 14 days)

in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for _____ days (not to exceed 30) until, the facts justifying, the later specific date of _____

Date and time issued: 11/5/2021 11:18am


Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: <u>21 MAG 10685</u>	Date and time warrant executed: <u>11/6/21 0600</u>	Copy of warrant and inventory left with: <u>JAMES O'KEEFE</u>
-------------------------------	---	---

Inventory made in the presence of: JAMES O'KEEFE

Inventory of the property taken and name(s) of any person(s) seized:
SEE ATTACHED FD-597

Certification

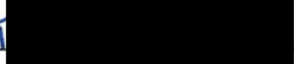
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 2/5/25



Executing officer's signature

SPECIAL AGENT



Printed name and title

ATTACHMENT A-1

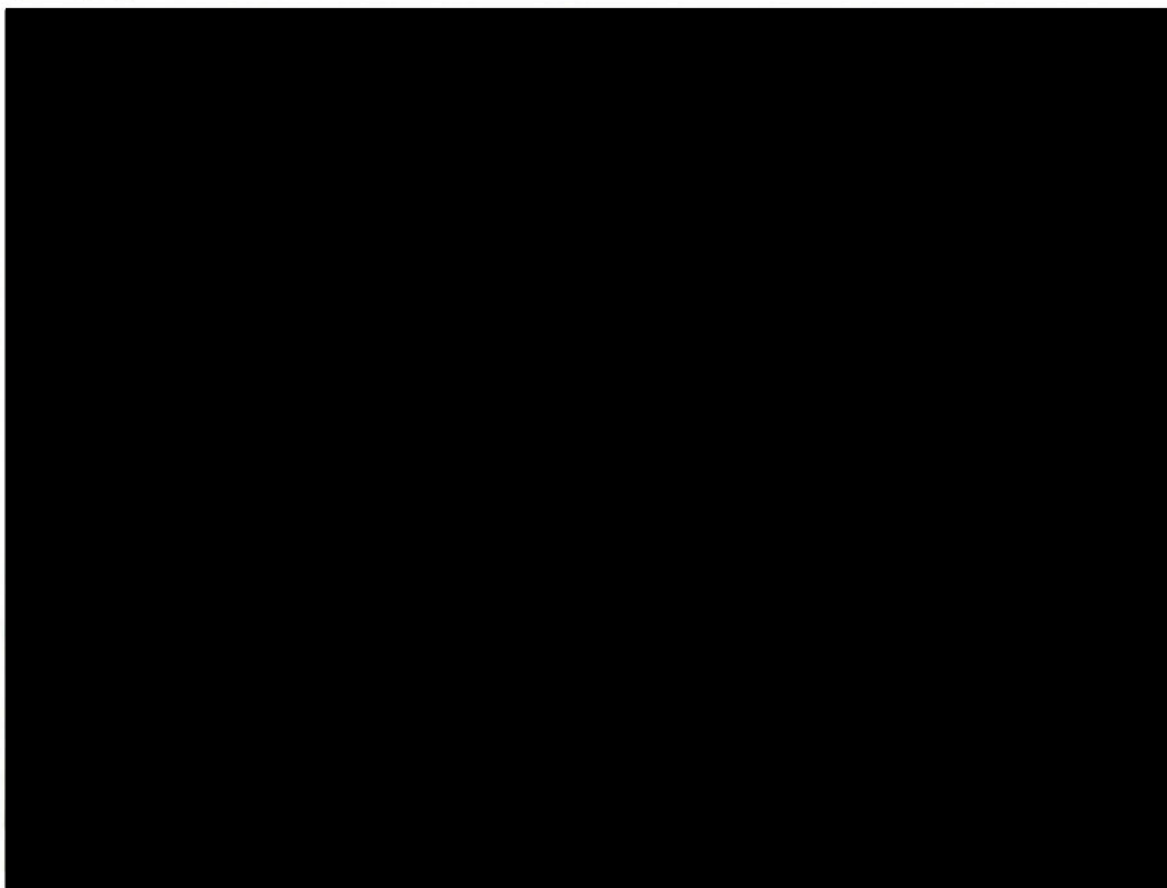
I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

An apartment known as

[REDACTED]

in Mamaroneck, New York, as depicted in the following photograph:



II. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the Subject Premises, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the "Subject Devices").

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED]'s family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED]'s property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to [REDACTED], [REDACTED], Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED]'s stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators' places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED]'s stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications

to [REDACTED]'s associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from James E. O'Keefe, III the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O'Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O'Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O'Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means

Original

Duplicate Original

UNITED STATES DISTRICT COURT

for the
Southern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Any Cellphones in the Possession, Custody, or Control)
of James E. O'Keefe, III)
)

21 MAG 10685
Case No.

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York
(identify the person or describe the property to be searched and give its location):

Any Cellphones in the Possession, Custody, or Control of James E. O'Keefe, III, as described in Attachment A-2

The search and seizure are related to violation(s) of (insert statutory citations):

18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony)

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment A-2

YOU ARE COMMANDED to execute this warrant on or before November 19, 2021 (not to exceed 14 days)
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

for _____ days (not to exceed 30) until, the facts justifying, the later specific date of _____

Date and time issued: 11/5/2021 11:18am


Judge's signature

City and state: New York, New York

Hon. Sarah L. Cave, U.S. Magistrate Judge
Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.: <u>21 MAG 10685</u>	Date and time warrant executed: <u>11/6/21 0600</u>	Copy of warrant and inventory left with: <u>JAMES OKSKE</u>
----------------------------------	--	--

Inventory made in the presence of:
JAMES OKSKE

Inventory of the property taken and name(s) of any person(s) seized:

(SEE ATTACHMENT) FD-597

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 2/5/25



Executing officer's signature

SPECIAL AGENT 

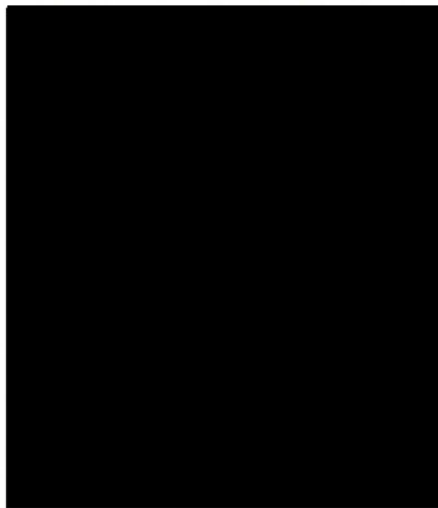
Printed name and title

ATTACHMENT A-2

I. Items to Be Seized

A. Subject Devices

Law enforcement agents are authorized to seize any and all cellphones within the possession, custody, or control of James E. O'Keefe, III, including, but not limited to, the cellphone that is or was assigned to the call number [REDACTED] (collectively, the "Subject Devices"). The search of O'Keefe shall include any and all clothing and personal belongings, backpacks, briefcases, purses, and bags that are within O'Keefe's immediate vicinity and control at the location where the search warrant is executed. O'Keefe was born on [REDACTED], and is depicted in the following photograph:



The search of O'Keefe and seizure the aforementioned items is not authorized pursuant to this warrant unless the following condition occurs: O'Keefe is located in the Southern District of New York.

B. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Devices are the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), 2315 (possession of stolen goods), 2 (aiding and abetting), 3 (accessory after the fact), and 4 (misprision of felony) (collectively, the "Subject Offenses") for the time period August 1, 2020, up to and including the date on which the Subject Devices are seized, consisting of:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses, such as user-inputted data, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user(s) such

as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or relating to [REDACTED] (and representatives thereof) and/or [REDACTED] family, friends, or associates with respect to her stolen property.

c. Evidence of the location of [REDACTED] property and the location of the user of the Subject Accounts at times relevant to the Subject Offenses, such as communications that reference particular geographic locations or refer to the property being located in a particular place.

d. Evidence of the identity, locations, knowledge, and participation in the Subject Offenses of potential co-conspirators, such as communications with other individuals—including, but not limited to, [REDACTED], Robert Kurlander, Aimee Harris, [REDACTED]—about obtaining, transporting, transferring, disseminating, or otherwise disposing of [REDACTED]’s stolen property, including but not limited to communications reflecting the knowledge of co-conspirators that the property obtained from [REDACTED] had been stolen, and communications that contain personally identifiable information of co-conspirators and references to co-conspirators’ places of residence or locations at particular points in time.

e. Evidence regarding the value of any of [REDACTED]’s stolen property, such as communications about the resale or market value of any of the items stolen from her, or any plans to sell or market the same.

f. Evidence of steps taken in preparation for or in furtherance of the Subject Offenses, such as surveillance of [REDACTED] or property associated with her, and drafts of communications to [REDACTED] associates regarding her stolen property and communications among co-conspirators discussing what to do with her property.

g. Evidence reflecting the location of other evidence with respect to the Subject Offenses, such as communications reflecting registration of online accounts potentially containing relevant evidence of the scheme.

C. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from [REDACTED] the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of O’Keefe to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of O’Keefe to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of O’Keefe to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any device(s) and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein that was sent, received, posted, created, or otherwise accessed, established, modified, or deleted between the time period August 1, 2020 and the present for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified above in this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

* * *

Review of the items described in this Attachment shall be conducted pursuant to established procedures designed to collect evidence in a manner reasonably designed to protect any attorney-client or other applicable privilege (to the extent not waived). When appropriate, the procedures shall include use of a designated “filter team,” separate and apart from the investigative team, in order to address potential privileges.

FD-597 (Rev. 4-13-2015)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

Case ID: _____

On (date) 11/6/21

item(s) listed below were:

- Collected/Seized
- Received From
- Returned To
- Released To

(Name) JAMES O'KEEFE

(Street Address) _____

(City) MAMARONCK NY

Description of Item (s):

1 WHITE IPHONE IMEI [REDACTED] 12 PRO MAX
1 SILVER IPHONE IMEI [REDACTED]

SV 11/6/21

Received By: [Signature]
(Signature)
Printed Name/Title: James O'Keefe

Received From: _____
(Signature)
Printed Name/Title: SA [REDACTED]