UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* *IN THE MATTER OF THE SEARCH OF ONE DIGITAL STORAGE MEDIA DEVICE, SERIAL NUMBER S3Z6NW0K713033N, CONTAINING THE IMAGES OF TWO WIRELESS TELEPHONES LOCATED AT 601 4TH ST NW, WASHINGTON, D.C. 20535*	)	Case No. 21-sw-101

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):* one digital storage media device, serial number S3Z6NW0K713033N, containing the images of two wireless telephones located at 601 4th St NW, Washington, D.C. 20535 (as further described in Attachment A) located in the _____ District of Columbia, there is now concealed *(identify the person or describe the property to be seized)*:

evidence of violations of 52 U.S.C. §§ 30122 and 30119 (as further described in Attachment B)

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:

Code Section	*Offense Description*
52 U.S.C. 30122	Contributions in the Name of Another Prohibited
52 U.S.C. 30119	Prohibiting Contributions by Government Contractors

The application is based on these facts:

Please 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.

Applicant's signature

Michelle Ball, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 04/07/2021

Judge's signature

City and state: Washington, D.C.

G. Michael Harvey U.S. Magistrate Judge

Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
IN THE MATTER OF THE SEARCH OF ONE DIGITAL STORAGE MEDIA DEVICE, SERIAL NUMBER S3Z6NW0K713033N, CONTAINING THE IMAGES OF TWO WIRELESS TELEPHONES LOCATED AT 601 4TH ST NW, WASHINGTON, D.C. 20535

Case No. 21-sw-101

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 _____ District of Columbia
(identify the person or describe the property to be searched and give its location):

Search of one digital storage media device, serial number S3Z6NW0K713033N, containing the images of two wireless telephones located at 601 4th St NW, Washington, D.C. 20535 for investigation of violation of 52 U.S.C. §§ 30122 and 30119 (as further described in the attached affidavit in support of search warrant, incorporated fully herein, including Attachment A)

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)*:

Evidence, fruits, and instrumentalities of violation of 52 U.S.C. § 30122 (Contributions in the name of another prohibited) and § 30119 (prohibiting contributions by Government contractors) (as further described in the attached affidavit in support of search warrant, incorporated fully herein, including Attachment B)

YOU ARE COMMANDED to execute this warrant on or before April 21, 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 G. Michael Harvey .
(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: 04/07/2021

Judge's signature

City and state: Washington, DC

G. Michael Harvey, U.S. Magistrate Judge
Printed name and title

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

Property to be searched

The property to be searched is a Digital Storage Media Device, specifically, a Hard Drive, with the Serial Number S3Z6NW0K713033N (hereinafter the "Device"). It contains an image of Subject Phone One, an Apple iPhone 11 Pro serial number DNPZC2KDN6Y1, and Subject Phone Two, an Apple iPhone Xr serial number DNPXNGX9KXL0. The Device is currently located at the FBI Washington Field Office, 601 4th Street NW, Washington, DC 20535.

ATTACHMENT B

Property to be seized

1. The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 52 U.S.C. § 30122 (Contributions in Name of Another Prohibited) and 52 U.S.C. § 30119 (prohibiting contributions by Government contractors) as described in the search warrant affidavit, including, but not limited to:

a. Evidence relating to or constituting evidence that one or more persons was facilitating contributions in the name of another and contributions by Navatek and its employees, including but not limited to any communications;

b. Evidence relating to the decision to form Society of Young Women Scientists and Engineers and any activities taken by the organization to include opening a P.O. Box, creating an account at BoxJelly and the political donation to 1820 PAC;

c. Any communications or records associated with political donations made by SYWSE, Navatek, any Navatek employee, or family member of any Navatek employee;

d. Communications or documents related to members of congress or their staffers relating to government contracts;

e. Communications to, from, or concerning any congressional campaign or any political action committee to include “Collins to Senator” and 1820 PAC and their agents and representatives;

f. Any evidence relating to any payment or gift provided to any member of congress or their staffers;

g. Preparatory steps taken in furtherance of the scheme;

h. Records and information relating to the identity or location of other subjects or co-conspirators;

i. Records and information that constitute evidence of the state of mind of Kao, Chen or other Navatek employees or family members *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;

j. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with Kao, or Chen about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

k. Evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

l. Evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

m. Evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

n. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

o. Evidence of the times the Device(s) was used;

p. Passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

q. Records of or information about Internet Protocol addresses used by the Device(s); and

r. Records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF ONE DIGITAL STORAGE MEDIA DEVICE, SERIAL NUMBER S3Z6NW0K713033N, CONTAINING THE IMAGES OF TWO WIRELESS TELEPHONES LOCATED AT 601 4TH ST NW, WASHINGTON, D.C. 20535	**No. 21-sw-101**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANT TO SEARCH AND SEIZE

I, Michelle Ball, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a warrant to search a one digital Storage Media Device with the serial number S3Z6NW0K713033N currently in law enforcement's possession as described in Attachment A, and the extraction from that property of electronically stored information as described in Attachment B. The Storage Media Device contains images of (1) Apple iPhone 11 Pro (IMEI 353247100759018) belonging to Martin Kao (hereinafter Subject Phone One) AND (2) Apple iPhone Xr (IMEI 35734809605544) belonging to Clifford Chen (hereinafter Subject Phone Two).

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and am currently assigned to the FBI's Washington, D.C. Field Office. I have been employed as an FBI Special Agent since 2015. In my capacity as a Special Agent of the FBI, I have participated in and conducted federal criminal investigations, including investigations involving bribery, wire fraud, financial fraud, money laundering and investigations related to violations of the Foreign Agents Registration Act. I have also participated in search warrants in which I have searched, and also

directed other agents in the searches of electronic evidence as well as residential and business locations for evidence of the aforementioned crimes. I have not included every detail of every aspect of my training, education, and experience, but have highlighted those areas most relevant to this application.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of Title 52, United States Code, Section 30122 (Contributions in Name of Another Prohibited), and Title 52, United States Code 30119 (prohibiting contributions by Government contractors) have been committed by Martin Kao, Clifford Chen, and Navatek LLC (Navatek), and there is probable cause to search Subject Phone One and Subject Phone Two as described in Attachment A for items described in Attachment B, which constitute evidence, instrumentalities, contraband or fruits of those crimes.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The Internal Revenue Service and the Small Business Administration, Office of the Inspector General are conducting a separate investigation into fraud relating to the Paycheck Protection Program. The Subject Phones were seized and imaged during that investigation consistent with a search warrant issued by a magistrate judge in the District of Hawaii. The images were saved on the subject Storage Media Device. The Storage Media Device was subsequently sent by law enforcement to the FBI Washington Field Office located at 601 4th Street NW in the District of Columbia.

6. Subject Phone One is an Apple iPhone 11 Pro (IMEI 353247100759018). It was seized from Martin Kao. It is associated with the phone number 808-371-0371. According to records from AT&T, this phone number is registered to a Navatek business account assigned to Martin Kao.

7. Subject Phone Two is an Apple iPhone Xr (IMEI 35734809605544). It was seized from Clifford Chen. According to subscriber records, Subject Phone Two is associated with phone number 808-379-8877. According to emails I have reviewed, I know this is the same number that Chen uses in his Navatek business email signature block. Further, records from AT&T confirm that the phone number is registered to a Navatek business account assigned to Chen.

PROBABLE CAUSE

8. The United States is investigating allegations that Martin Kao, Clifford Chen, and Navatek (now known as the Martin Defense Group) illegally donated money to the Collins for Senator campaign committee and 1820 PAC in violation of 52 U.S.C. § 30122 (Contributions in Name of Another Prohibited) and 52 U.S.C. § 30119 (prohibiting contributions by Government contractors).

Relevant Persons and Entities

9. Martin Defense Group (known as Navatek LLC during the activity discussed herein) is based in Hawaii and operates additional offices in Maine, Washington, D.C., Rhode Island, Michigan, Oklahoma, Kansas, and South Carolina. It designs and analyzes ship hull forms, ocean structures, underwater lifting bodies, and coupled hydrodynamic systems. The company frequently contracts with the United States Department of Defense. Title 52, United States Code,

Section 30119 prohibits federal contractors from making political contributions, subject to certain exceptions involving segregated funds.[1]

10. During the time period of the activity discussed herein: (1) Martin Kao was the President and CEO of Navatek; (2) Lori Bofman was an executive assistant at Navatek; (3) Lawrence Lum Kee was Navatek's Hawaiian-based accountant; (4) Clifford Chen was Navatek's Chief Financial Officer; and (5) Christopher Michael Todd Lam is Martin Kao's brother-in-law, and was the Vice President of Information Technology for Navatek.

11. The Society of Young Women Scientist [sic] and Engineers LLC (SYWSE), was established as a limited liability corporation incorporated in Hawaii on November 26, 2019. On March 24, 2020, it changed its name to Society of Young Women Scientists and Engineers LLC.

12. Tiffany Jennifer Lam is Martin Kao's wife, and Christopher Michael Todd Lam's sister.

13. George Kao is Martin Kao's father.

14. Rachael Kao is Martin Kao's mother.

15. JoAnn Lam is Tiffany Lam's mother.

16. Christopher Maxim Tory Lam is Tiffany Lam's brother.

17. Christopher Mark Toby Lam is Tiffany Lam's brother.

18. Hsiu Chuan Chen is Clifford Chen's mother.

19. Joy Lum Kee is Lawrence Lum Kee's wife.

[1] According to the Business Registration Division of the State of Hawaii, Department of Commerce and Consumer Affairs, Navatek LLC became Martin Defense Group LLC in July 2020.

20. The "Collins for Senator" campaign committee was the official campaign committee established to support the reelection of United States Senator Susan Collins in the November 2020 election.

21. 1820 PAC is a political action committee supporting the reelection of Senator Collins.

Contributions and Reimbursements

SYWSE and 1820 PAC

22. On August 7, 2019, Senator Susan Collins announced Navatek had received a Department of Defense contract worth $8,000,000 for advanced hull planing research. A press release posted on the Senator's official website quoted her as saying, "[a]s a senior member of the Defense Appropriations Subcommittee, I strongly advocated for the funding that made this research possible and am so proud of the work Navatek and other Maine industries do to support our Navy and our nation's defense."

23. On November 26, 2019, Lori Bofman opened P.O. Box 2394 in the name of SYWSE in Honolulu, Hawaii. The same day, SYWSE was formed as a limited liability corporation in Hawaii, using the P.O. Box opened by Bofman as its mailing address. Jennifer Lam was named as the company's registered agent and manager and signed the organization documents. Bank records for SYWSE confirm Jennifer Lam is Martin Kao's wife, Tiffany Jennifer Lam.

24. According to documents I have reviewed, one month after SYWSE was incorporated, on December 26, 2019, Lawrence Lum Kee wrote a check for $150,000 from Navatek's corporate account at Central Pacific Bank to SYWSE as the payee.

25. On December 27, 2019, the check from Navatek to SYWSE was deposited into SYWSE's checking account at Central Pacific Bank.

26. On December 27, 2019, SWYSE donated $150,000 to 1820 PAC by check. The check was originally signed by Martin Kao on behalf of SWYSE, but it was rejected because he was not an authorized signatory for SWYSE's checking account. Later, Tiffany Lam signed the check and it cleared.

27. The $150,000 contribution from SWYSE to 1820 PAC was reported by 1820 PAC to the Federal Election Commission, located in Washington, D.C., on December 31, 2019.

28. Based on information and belief, informed by my experience investigating corruption-related offenses, and research in this matter, in 2019, SWYSE had no other source of revenue beyond donations from Navatek.

29. Accordingly, there is probable cause to believe that Navatek, a federal contractor prohibited from making political campaign contributions, used SWYSE to conceal a donation to 1820 PAC in violation of 52 U.S.C. § 30122 and 52 U.S.C. § 30119.

30. On February 3, 2020, the Campaign Legal Center filed a complaint against SYWSE with the FEC. The complaint alleges that Jennifer Lam and SYWSE may have violated 52 U.S.C. § 30122 by making contributions to 1820 PAC in the name of another person, namely SYWSE, and that SYWSE violated 52 U.S. C. § 30122 by knowingly permitting its name to be used for the making of such contribution. On February 3, 2020, the same day the Campaign Legal Center complaint became public, Bofman closed the P.O. Box for SWYSE.

Personal Donations to Collins for Senator

~~31.~~ Between June 2019 and September 2019, George Kao, Rachael Kao, Christopher Michael Lam, Christopher Maxim Tory Lam, Joann Lam, Hsiu Chuan Chen, Joy Lum Kee,

Lawrence Lum Kee, and Clifford Chen gave to Senator Collins' campaign. When these contributions were submitted, the contributor had to certify that the contribution was from their personal funds and not drawn from an account maintained by an incorporated entity or other prohibited sources. The contributors also have to certify that he or she is not personally a federal government contractor.

32. Bank records I have reviewed indicate that Martin Kao reimbursed his family members for their donations to the Collins for Senator campaign committee, in violation of federal law. Specifically, bank records show that on July 1, 2019, Kao, from his First Hawaiian Bank Account, wrote a series of $5,600 checks to Christopher Maxim Tory Lam, Christopher Mark Toby Lam, Christopher Michael Todd Lam, JoAnn Lam, Rachael Kao and a $5,200 check to George Kao. FEC records show that the same amounts were subsequently donated to the Collins for Senator campaign from Christopher Maxim Tory Lam, Rachael Kao, George Kao, Christopher Michael T. Lam, Christopher Michael Tory Lam.

33. In September 2019, Clifford Chen, Navatek's Chief Financial Officer, and his mother Hsiu Chuan Chen along with Lawrence Lum Kee, Navatek's accountant, and his wife Joy Lum Kee, each donated $5,600, the maximum allowed by law, to the Collins for Senator campaign committee. Financial records indicate that Navatek reimbursed the Chen and Lum Kee families for their contributions in violation of federal law as follows:

a. On September 26, 2019, checks were written to Clifford Chen and Lawrence Lum Kee from the Navatek LLC general account at Central Pacific Bank. This account appears to be used by Navatek to reimburse employees or pay expenses, other than payroll. The check to Clifford Chen was for $6,000 and the check to Lum Kee was for $5,218.88. The checks were sequential and signed by Navatek's treasurer.

b. Also on September 26, 2019, the same day the aforementioned checks were written to Clifford Chen and Lawrence Lum Kee, FEC records show Hsiu Chan Chen and Joy Lum Kee made $5,600 donations to the Collins for Senator campaign committee.

c. On or about September 27, 2019, Clifford Chen deposited $5,600 cash into his Central Pacific Bank account.

d. On October 1, 2019, Clifford Chen wrote a $5,600 check from the same account to Hsiu Chuan Chen. The check was used as a credit towards the balance of the same credit card Hsiu Chuan Chen used to make the aforementioned donation to the Collins for Senator campaign committee.

e. In November 2021 Hsiu Chuan Chen told law enforcement that her son Clifford Chen gave her money and asked her to donate it to the Collins for Senator campaign committee, which she did.

34. Documents law enforcement received from American Express reveal that Chen and Lum Kee paid for their donations using a Navatek corporate credit card. Bank records show that these Navatek credit card payments are made from the same Navatek bank account which receives federal funding from the United States government; the funds are not segregated.

35. Accordingly, there is probable cause to believe that Martin Kao, Clifford Chen and Navatek, a federal contractor prohibited from making political campaign contributions, used family members associated with Kao, Chen and Navatek as conduits for contributions to the Collins for Senator campaign committee in violation of 52 U.S.C. § 30122 and 52 U.S.C. § 30119.

Use of the Subject Phones

36. According to information I have received from Navatek, I know that Martin Kao and Clifford Chen used the subject phones to communicate by email and text message, using both personal and business accounts.

37. On May 28, 2019, Martin Kao received by email a receipt from the Collins for Senator campaign for a $5,600 donation. It was sent to mkao@navatekllc.com. The receipt showed Kao listed his phone number for the donation as 808-371-0371, which is associated with Subject Phone One.

38. On May 29, 2019, using mkao@navatekllc.com, Martin Kao sent an email to a lobbyist for Navatek with the subject line, "RE: event for Sen. Collins in Maine." Kao wrote in part, "I actually did sent [sic] the [Collins for Senator Director of Finance] a note yesterday and no response. Interesting enough, I also received in the mail yesterday a solicitation for donations for Susan Collins. I responded online and made the following contribution. I maxed out...that usually gets their attention… This will clearly make them have to proactively look further into my donation and I'm sure get the [Collins for Senator Direct of Finance's] involvement. Either way...very strange...usually they jump on this stuff." The email also included a picture of a receipt for a donation made in Kao's name for $5,600. The receipt also included Subject Phone One's phone number.

39. On August 2, 2019, Christopher Maxim Tory Lam emailed a file to Kao at mkao@navatekllc.com titled, "Collins for Senator Contribution Form.pdf." He also wrote, "All good? wasn't sure if I filled it out right." Kao responded, "All good! Thanks!" Kao's signature line included Subject Phone One's phone number.

40. On September 16, 2019, Kao sent an email from mkao@navatekllc.com to the Collins Campaign's Maine Director of Finance with the subject line, "Thank you!" It stated in

part, "Thanks again for all the support from Sen Collins. I've been involved in may [sic] tight races in the past and understand last minute 'needs' come up. We are here to help anyway we can … financially or whatever." The campaign representative responded in part, "[y]ou have already maxed (which we so appreciate), but if you have friends or family members that would be willing to donate please don't hesitate to send them my way." Kao responded, "[j]ust want to let you know, you're going to see two more max out donation [sic] of $5,600/each come in later today." He indicated that they would come from Navatek's Chief Operating Officer and Lori Bofman. Approximately six hours later Kao noted there would be a slight change and the donations would come from Hsiu Chuan Chen and Joy Lum Kee instead.

41. On September 17, 2019, Chen received an email at cchen@navatekllc.com containing a receipt for a $5,600 Collins for Senator donation. The receipt included the phone number associated with Subject Phone Two.

42. On September 17, 2019, Kao sent an email from mkao@navatekllc.com to Chen at cchen@navatekllc.com and Lum Kee. The email included a copy of a receipt provided for a $5,600 donation to Collins for Senator made by Chen. Kao said, "Kahele: Please do one also for $5,600 on your Amex and send me confirmation. Thx."

43. On November 21, 2019, Lum Kee sent an email to Kao at mkao@navatekllc.com and Chen at cchen@navatekllc.com with the subject, "New LLC." It stated, "Looks like we can setup a new LLC Pretty vaguely. Let me know who you want to list as the registered agent, manager and the address to use and I can get started when you are read. Thanks." Kao responded in part, "Name of LLC: Society of Young Women Scientists and Engineers." Lum Kee responded on November 26, 2019 writing in part, "Lori obtained PO box. Once obtained, I will fill in address in the attached Operating Agreement and file Articles of Organization, obtain FEIN number."

44. On December 13, 2019, Kao sent an email form mkao@navatekllc.com to Scott Reed and Mackenzie Dolan who are both associated with the 1820 PAC. The email subject was, "RE: Navatek/Martin Kao – Thanks!" and stated in part, "I just received confirmation from our bank that the new account for the Society of Young Women Scientists and Engineers will be up and ready to go by early next week." Kao also wrote," I will be in touch next week re getting 1820 a check by year end."

45. Accordingly, there is probable cause to believe the Subject Phones contain evidence that Chen, Kao and Navatek, used SYWSE and family members as conduits for contributions to the Collins for Senator campaign committee in violation of 52 U.S.C. §§ 30122 and 30119.

TECHNICAL TERMS

46. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books";

sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the

Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at

the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption

algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

47. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://apple.com, I know that the Subject Phones have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and calendar. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offenses under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

48. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found within the Subject Phones in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this

investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the Subject Phones for at least the following reasons:

a. Individuals who engage in criminal activity, use digital devices, like the Subject Phones, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Subject Phones, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; and (2) keep a record of illegal transactions for future reference.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as

a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

49. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or

texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information,

configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

50. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device

was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process

called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

51. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, 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); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic

storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the Device(s) will be specifically chosen to identify the specific items to be seized under this warrant.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

14. Because forensic examiners will be conducting their search of the digital devices in a law enforcement setting over a potentially prolonged period of time, I respectfully submit that good cause has been shown, and therefore request authority, to conduct the search at any time of the day or night.

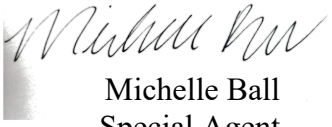
REQUEST TO SUBMIT WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

52. I respectfully request, pursuant to Rules 4.1 and 41(d)(3) of the Federal Rules of Criminal Procedure, permission to communicate information to the Court by telephone in connection with this Application for a Search Warrant. I submit that Assistant U.S. Attorney Elizabeth Aloi, an attorney for the United States, is capable of identifying my voice and telephone number for the Court.

CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully submitted,



Michelle Ball
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on April 7, 2021

_____

G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE