Exhibit 1

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

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)

ONE APPLE IPHONE XS (IMEI [redacted]), LOCATED ON THE PERSON OF RICHARD MAUZE BURR, UNDER RULE 41

Case No. 20-sw-132

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 Attachment A, herein incorporated by reference.

located in the _____ District of Columbia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B and Attachment C, herein incorporated by reference.

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*
15 U.S.C. § 78j(b)	Insider Trading
18 U.S.C. § 1348	Securities Fraud

The application is based on these facts:

See Affidavit in Support of Application and Search Warrant, which is incorporated herein by reference.

- ☐ 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

Brandon Merriman, 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: 05/13/2020

Judge's signature

City and state: District of Columbia

Beryl A. Howell, Chief Judge - U.S. District Court
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)* ONE APPLE IPHONE XS (IMEI [redacted]), LOCATED ON THE PERSON OF RICHARD MAUZE BURR, UNDER RULE 41	)	Case No. 20-sw-132

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):

One APPLE IPHONE XS (IMEI [redacted]), located on the person of Richard Mauze Burr.

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 B and Attachment C

YOU ARE COMMANDED to execute this warrant on or before May 27, 2020 *(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 Chief Judge Beryl A. Howell .
(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: 05/13/2020, 2:45 pm

Judge's signature

City and state: District of Columbia

Beryl A. Howell, U.S. District Court Chief Judge
Printed name and title

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

Return

Case No.: 20-sw-132	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 an **APPLE IPHONE XS (IMEI** [redacted]**)**, hereinafter the "Device." The Device is currently **located on the person of Richard Mauze Burr**. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in **Attachment B**, pursuant to the Special Search Procedures described in **Attachment C**.

ATTACHMENT B

Property to be seized

The items, information, and data to be seized are fruits, evidence, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 15 U.S.C. § 78j(b) (Insider Trading) and 18 U.S.C. § 1348 (Securities Fraud), as described in the search warrant affidavit, for the period December 31, 2019, to the present, including, but not limited to:

a. All records, communications, and information relating to Senator Burr's and Brooke Burr's (1) January 31, 2020, stock sales; (2) Senator Burr's February 12, 2020, purchase of $1,189,000 in the Federated U.S. Treasury Cash Reserves Fund; and (3) Senator Burr's and Brooke Burr's February 13, 2020, stock sales.

b. All records, communications, and information relating to Gerald and Mary Fauth's February 13, 2020, sale in the stock of any company, including sales of Altria Group Inc. (MO), BP PLC (BP), Chevron Corp. (CVX), Mondelez International Inc. (MDLZ), Royal Dutch Shell (RDS.B), and Williams Sonoma (WSM).

c. All records, communications, and information relating to Senator Burr's February 7, 2020, Senator Burr article on FoxNews.com, and his statements to members of the Tar Heel Circle at the Capitol Hill Club in Washington, D.C. on February 27, 2020.

d. All communications with Gerald Fauth, Mary Fauth [redacted] relating to the trading of securities, the stock market, the economy, and/or COVID-19.

e. All records, communications, and information concerning Senator Burr's public statements concerning (1) COVID-19 and (2) the public news reports on his trading activity.

f. All records, communications, and information concerning (1) COVID-19, (2) the trading of securities, (3) the stock market, and (4) the economy.

g. Records and information that constitute evidence of the state of mind of Richard Mauze Burr and Gerald W. Fauth, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation.

h. Records and information that constitute evidence concerning persons who either (1) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation, or (2) communicated with Senator Burr about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

i. Evidence of who used, owned, or controlled the Device 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.

j. Evidence of software, or the lack thereof, that would allow others to control the Device, 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.

k. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence.

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

m. Evidence of the times the Device was used.

n. Passwords, encryption keys, and other access devices that may be necessary to access the Device.

o. Documentation and manuals that may be necessary to access the Device or to conduct a forensic examination of the Device.

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

q. Records of or information about the Device'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.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT C

Special Search Procedures

1. I have been informed by the Prosecutors overseeing the investigation in this matter that they have decided to adopt special procedures in light of the possibility the Device contains materials created that are protected by the Speech or Debate Privilege, U.S. Const. art I, § 6, cl. 1 (the "Privilege").

2. The special search procedures will be employed with respect to the Device to ensure that an appropriate opportunity is afforded to Senator Burr to either waive or assert the Privilege, prior to any review of the content of the Device by employees of the Executive Branch.[11] These special search procedures are as follows:

a. Attorneys for the U.S. Attorney's Office for the District of Columbia and the Criminal Division of the U.S. Department of Justice will contact counsel for Senator Burr.

b. Before conducting any review of the contents of the Device, attorneys for the U.S. Attorney's Office for the District of Columbia and the Criminal Division of the U.S. Department of Justice will request that Senator Burr waive the Speech or Debate Privilege and consent to the search of the Device pursuant to the instant Warrant. If Senator Burr agrees to waive the Speech or Debate Privilege, the agents will be authorized to search the Device for evidence, fruits, and instrumentalities of violations of 15 U.S.C. § 78j(b) (Insider Trading) and

---

[11] The D.C. Circuit has held that even incidental review of Speech or Debate privileged material by agents during the execution of a search of a Member's office violates the Privilege unless the member is provided an opportunity to review and assert the Privilege. *United States v. Rayburn House Office Building, Room 2113*, 497 F.3d 654, 662 (D.C. Cir. 2007).

18 U.S.C. § 1348 (Securities Fraud), consistent with the other procedures set forth in this affidavit.

c. If Senator Burr declines to waive the Speech or Debate Privilege with respect to the search of the Device pursuant to the instant Warrant, the agents executing the Warrant will obtain an image of the Device (hereinafter, "Image") and, using a forensic software program, deliver the Image to Senator Burr, through counsel, to give him the opportunity to assert the Speech or Debate privilege over information in the Image. In doing so, neither the agents nor any attorneys for the Government will review the Image or the contents of the Device.

d. Senator Burr will have thirty (30) days to review the Image and provide attorneys for the U.S. Attorney's Office for the District of Columbia and the Criminal Division of the U.S. Department of Justice with a log of the records contained in the Image over which the Privilege is being asserted. That log shall identify the record by date, recipient, sender, and subject matter if such information is available. As needed, the Government shall then request that the District Court review the records over which Senator Burr has asserted privilege in order for the Court to make a final determination whether they contain privileged information.

e. If Senator Burr fails to complete the privilege review within 30 days, the Government will seek relief from the District Court, including requesting a determination that Senator Burr waived the privilege through non-compliance, providing the contents of the Image to the Court for its review, or such other relief that may be appropriate.

f. Neither attorneys for the U.S. Attorney's Office for the District of Columbia and the Criminal Division of the U.S. Department of Justice nor the agents executing the Warrant—nor any other employee of the Executive Branch—shall review the contents of the

Image until: (1) Senator Burr consents to such a review, as set forth in Paragraph (b); (2) Senator Burr identifies non-privileged material in the Image that can be reviewed, as set forth in Paragraph (d); or (3) pursuant to further order of the Court.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF ONE APPLE IPHONE XS (IMEI [redacted]), LOCATED ON THE PERSON OF RICHARD MAUZE BURR, UNDER RULE 41	**SW No. 20-sw-132**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEAR CH AND SEIZE

I, Brandon Merriman, 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 Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of Richard Mauze Burr, the seizure of an electronic device (the "Device") as described in **Attachment A**, and the extraction from that property of electronically stored information as described in **Attachment B**.

2. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and I have been so employed since January 10, 2016. My principal duties include the investigation of criminal allegations of bribery and corruption involving public officials, mail and wire fraud, and government fraud. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of search warrant affidavits and in conducting search warrants. I have had both training and experience in the investigation of crimes involving electronic media and have worked with other FBI agents who have such experience, and who have provided me with additional information about such crimes.

3. The statements contained in this affidavit are based on my review of records and documents obtained during this investigation, information received from other individuals,

including witnesses and members of other law enforcement agencies, and my experience and training as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation, but rather those facts that I believe are necessary to establish probable cause. Where statements of others are set forth in this affidavit, they are set forth in whole or in part. The dates and times of events described in this affidavit are intended to reflect "on or about" the date and time the events occurred.

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 15 U.S.C. § 78j(b) (Insider Trading) and 18 U.S.C. § 1348 (Securities Fraud) have been committed by United States Senator Richard Mauze Burr ("Senator Burr") and Gerald W. Fauth. There is also probable cause to search the Device, further described below and in **Attachment A**, for the things described in **Attachment B**.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is an APPLE IPHONE XS (IMEI [redacted]), that is, the "Device."

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As discussed below, acts or omissions in furtherance of the above-listed offenses occurred in the District of Columbia and elsewhere.

7. Furthermore, this Court has jurisdiction to issue the requested warrant because it is anticipated that Senator Burr and the Device will be located in the District of Columbia, where Senator Burr maintains an office, during the week of May 11, 2020. Furthermore, based on toll records that I reviewed, the Device appears to be Senator Burr's primary cellular phone. The Device was issued to Senator Burr by the United States Senate. Therefore, I believe that Senator Burr will have the Device in his possession during the week of May 11, 2020, while he is in the District of Columbia.

BACKGROUND

A. Relevant Individuals

8. Richard Mauze Burr is a United States Senator for the State of North Carolina (hereinafter, "Senator Burr"). His cellular phone number, [redacted], is associated with the Device.

9. Brooke Fauth Burr is Senator Burr's wife. Her cellular phone number is [redacted].

10. Gerald W. Fauth III is Brooke Fauth Burr's brother (*i.e.*, Senator Burr's brother-in-law), and a presidentially appointed member of the National Mediation Board. His cellular phone number is [redacted].

11. Mary Fauth is Gerald Fauth's wife (*i.e.*, Senator Burr's co-sister-in-law). Her cellular phone number is [redacted].

12. [redacted]

13. [redacted]

14. Coronavirus disease (COVID-19) is a viral respiratory illness that was first reported in Wuhan, China in November 2019. On January 31, 2020, Health and Human Services Secretary Alex M. Azar II declared COVID-19 a public health emergency, and on March 11, 2020, the World Health Organization (WHO) declared COVID-19 a pandemic. Since early 2020, the spread of COVID-19 globally and within the United States has presented an urgent public health issue for U.S. government officials.

B. The Stop Trading on Congressional Knowledge Act of 2012 ("STOCK Act")

15. The general prohibitions against "insider trading" in securities are found in Section 10(b) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder.

16. Section 10(b) of the Exchange Act makes it:

---

1 [redacted]

2 *Id*.

> . . . unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange –
>
> . . .
>
> (b) To use or employ, in connection with the purchase or sale of any security registered on a national securities exchange . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j(b).

17. Rule 10b-5 promulgated thereunder by the United States Securities and Exchange Commission makes it:

> . . . unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of national exchange,
>
> (a) To employ any device, scheme, or artifice to defraud . . . .

17 C.F.R. § 240.10b-5(a).

18. A person violates Section 10(b) and Rule 10b-5:

> when he [or she] misappropriates confidential information for securities trading purposes, in breach of a duty owed to the source of the information. Under this theory, a fiduciary's undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him [or her] with access to confidential information.

United States v. O'Hagan, 521 U.S. 642, 652 (internal citation omitted).

19. The STOCK Act of 2012 amended existing securities laws to clarify and confirm that Members of Congress are prohibited from engaging in insider trading because they owe:

> a duty arising from a relationship of trust and confidence to the Congress, the United States Government, and the citizens of the United States with respect to material, nonpublic information derived from such person's position as a Member of Congress or employee of Congress or gained from the performance of such person's official responsibilities.

15 U.S.C. § 78u-1(g).

20. The core elements of an insider trading charge incorporating the fiduciary duty codified in the STOCK Act are the following: (1) the person traded in securities registered on a national exchange; (2) the person was in possession of material, non-public information when he or she traded in the securities; (3) the person had a duty arising from a relationship of trust and confidence to the Congress, the United States Government, and the citizens of the United States to not trade on material, nonpublic information derived from such person's position as a Member of Congress or employee of Congress or gained from the performance of such person's official responsibilities; (4) the person acted knowingly, willfully, and with the intent to defraud in connection with the sale or purchase of the securities; and (5) the person used the means or instrumentalities of interstate commerce, or the mails or the facilities of a national securities exchange, in connection with the trade.

PROBABLE CAUSE

21. Senator Burr and his wife, Brooke Burr, hold brokerage accounts [redacted]. Specifically, Senator Burr and Brooke Burr hold the following accounts [redacted].: (1) a Joint Account (the "Burrs' Joint Account"); (2) an Individual Retirement Account ("IRA") belonging to Senator Burr ("Senator Burr's IRA Account"); and (3) an IRA account belonging to Brooke Burr ("Brooke Burr's IRA Account").

A. January 31, 2020 Stock Trades by Senator Burr

22. On January 31, 2020, at approximately 8:51 a.m., [redacted] called Senator Burr's cellular phone and left a voicemail.

23. Approximately three minutes later, [redacted] sent the following text message to Senator Burr's cellular phone: [redacted] Senator Burr responded with the following text message: [redacted]

24. Later that morning, at approximately 11:34 a.m., [redacted] the following text message to Senator Burr's cellular phone: [redacted] Senator Burr responded with the following text message [redacted]

25. Within one minute of receiving Senator Burr's response, at approximately 11:35 a.m., [redacted] called Senator Burr's cellular phone. The call lasted a little less than two minutes. In an interview that I conducted [redacted]

26. At the time [redacted], it was not public information.

27. Less than two minutes after his call [redacted] at approximately 11:38 a.m., Senator Burr placed a call from his cellular phone to [redacted]. The call lasted 19 seconds.

28. At approximately 11:55 a.m. on that same day, Senator Burr's trading account [redacted] was accessed from an Internet Protocol ("IP") address resolving back to the United States Senate, which is located in the District of Columbia.

29. Three minutes later, at approximately 11:58 a.m., [redacted] used his landline at [redacted] to call Senator Burr's office landline at the United States Senate. That call lasted approximately 3 minutes.

30. In an interview that I conducted [redacted] Burr directed that the sales go forward.

31. Within five minutes of this call, [redacted] entered a sell order in Brooke Burr's IRA Account for the sale of 300 shares of Aon PLC stock for a total of approximately $66,582 and another sell order for the sale of an additional 95 shares of Aon PLC, an insurance company, for a total of approximately $21,089. In addition, [redacted] entered a sell order in Senator Burr's IRA Account for the sale of 300 shares of GCI Liberty Inc., a telecommunications company, for a total of approximately $21,976.

32. At 3:43 p.m. on that same day, approximately three hours and forty minutes after Senator Burr directed [redacted] the stock sales, the White House held a press briefing—attended by [redacted] HHS Secretary Alex M. Azar [redacted]—and publicly announced that the United States would temporarily ban the admission of travelers who had been in China for up to 14 days prior to their attempted travel to the United States.[3]

---

[3] *Available at* https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-immigrants-nonimmigrants-persons-pose-risk-transmitting-2019-novel-coronavirus/ (last checked May 12, 2020).

33. During that same briefing, Secretary Azar announced his decision to declare "a public health emergency for the entire United States to aid the nation's healthcare community in responding to 2019 novel coronavirus."[4]

B. Senator Burr's Article on FoxNews.com

34. On February 7, 2020, Senator Burr co-authored an article with Senator Lamar Alexander, which was published on FoxNews.com.[5] In the article, Senators Burr and Alexander stated: "Thankfully, the United States today is better prepared than ever before to face emerging public health threats, like the coronavirus, in large part due to the work of the Senate Health Committee, Congress, and the Trump Administration. The work of Congress and the administration has allowed U.S. public health officials to move swiftly and decisively in the last few weeks." That same day, a tweet was issued from Senator Burr's official Twitter account providing the link to the article on FoxNews.com.[6]

C. Senator Burr's Treasury Fund Purchase on February 12, 2020

35. On February 12, 2020, at approximately 2:50 p.m., [redacted] placed a call to Senator Burr's office landline. That call lasted 23 minutes. According to an interview [redacted] Senator Burr authorized [redacted] purchase $1,189,000 in the Federated U.S. Treasury Cash Reserves Fund, using approximately 76% of the total holdings in the Burrs' Joint Account. Your affiant knows, based on his training and experience, that investors often purchase

---

4 *Available at* https://www.whitehouse.gov/briefings-statements/press-briefing-members-presidents-coronavirus-task-force/; *see also* https://www.hhs.gov/about/news/2020/01/31/secretary-azar-declares-public-health-emergency-us-2019-novel-coronavirus.html (last checked May 12, 2020).

5 *Available at* https://www.foxnews.com/opinion/coronavirus-prevention-steps-the-u-s-government-is-taking-to-protect-you-sen-alexander-and-sen-burr (last checked May 12, 2020).

U.S. Treasury funds to hedge against a potential market downturn. [redacted] at no time [redacted] on February 12, 2020, did Senator Burr mention any intention to imminently sell almost all of his equity positions and a large portion of his wife's equity positions. This transaction did not contemplate the liquidation of Senator Burr's or his wife's equity positions; it did not involve the sale or purchase of any stock.[7]

36. Later that same day, on February 12, 2020, at approximately 3:01 p.m., [redacted] entered the purchase order for $1,189,000 in the Federated U.S. Treasury Cash Reserves Fund for the Burr's Joint Account.

37. That day, the Dow Jones closed at 29,551.42, which was its highest closing level ever.

D. <u>Senator Burr's Stock Sales on February 13, 2020</u>

38. On February 13, 2020, at approximately 7:55 a.m., Senator Burr placed a call [redacted]. That call lasted approximately 14 minutes. [redacted] in an interview conducted by your affiant [redacted]

---

[6] *Available at* https://twitter.com/SenatorBurr/status/1225879401147064321 (last checked May 12, 2020).

[7] [redacted] prior to the COVID-19 outbreak, Senator Burr had invested approximately one million dollars in a treasury money market account but then moved the money to a bank deposit program. [redacted] the yield on the bank deposit program was significantly lower than the treasury money market account. [redacted] suggest that he move the money back to a higher yield investment such as a treasury money market account, which Senator Burr ultimately authorized [redacted] February 12, 2020[redacted]

[redacted]

39. Approximately 30 minutes later, at 8:22 a.m., Senator Burr's trading account at [redacted] was accessed from an IP address resolving back to the United States Senate.

40. At approximately 8:54 a.m., Senator Burr placed a call from his office landline to [redacted]. That call lasted 12 minutes. [redacted] Senator Burr instructed [redacted] to sell nearly all of the stock in his and Brooke Burr's IRA Accounts. [redacted] Senator Burr explained that he was uncomfortable with a lot of things in the market and other things generally happening around the world; that Burr discussed the fact that there had been a long bull market and that it was due for a correction; and that the surge of Bernie Sanders in the Democratic party's nomination process was a risk to the market. [redacted] Senator Burr also discussed COVID-19, saying that it was a concern, that the virus could affect the stock market, and that it was an epidemic in China. [redacted] Senator Burr also discussed supply chains and the fact that U.S. companies depended on Chinese suppliers. [redacted] Senator Burr did not specifically reference any briefings or information he received in his capacity as a Member of Congress. [redacted] did not recall Burr mentioning CNBC during the conversation. [redacted] Senator Burr [redacted] directed [redacted] to sell nearly all of the stock in his and his wife's IRA Accounts.

41. Consistent with Burr's orders, beginning at 11:38 a.m., [redacted] began executing the large-scale sale of the Burrs' IRA holdings.

a. From approximately 11:38 a.m. to 11:43 a.m. on that same day, February 13, 2020, sell orders were placed in Senator Burr's IRA account [redacted] selling approximately $262,884.35 in stock, which was all but one $11,670 equity position in his account. These sales represented over 95% of Burr's holdings in the IRA account. As a result of Senator Burr's sales on February 13, 2020, his portfolio went from approximately 83% in equities to approximately 3% in equities.

b. From 11:45 a.m. to 11:49 a.m. on that that same day, February 13, 2020, sell orders were placed into Brooke Burr's IRA Account [redacted] selling approximately $804,341.09 in stock, all but three equity positions in her account. These sales represented approximately 58% of the holdings in this account. As a result of these sales on February 13, 2020, Brooke Burr's portfolio went from having approximately 73% in equities to approximately 12% in equities.

42. Also that same day, at 4:34 p.m., an iPad logged into Senator Burr's trading account [redacted] from an IP address that resolved back to Gerald and Mary Fauth's residence in Virginia. Notably, approximately one hour before, at 3:38 p.m., Senator Burr's [redacted] account generated an automated email with a one-time passcode for access to Burr's [redacted] account. This automated email was sent to [redacted] and, a minute later, [redacted] forwarded the email to Senator Burr. I believe that this automated email was generated when the iPad accessed Senator Burr's [redacted] Account.

43. On February 17, 2020, at approximately 10:43 p.m., Senator Burr sent a text [redacted]

[redacted]

44. In total, between January 31, 2020, and April 7, 2020, [redacted] and Senator Burr exchanged approximately 32 text messages, nearly all of which concerned, in one way or another, the COVID-19 pandemic. Those text messages include those discussed above, as well as others regarding other issues [redacted]

E. Gerald Fauth's Stock Sales on February 13, 2020

45. After Senator Burr spoke with his own broker and directed a massive sale of his and his wife's equity, at approximately 11:07 a.m., a call was placed from Gerald Fauth's cellular phone to the cellular phone of Brooke Burr, Gerald Fauth's sister and Senator Burr's wife. That call lasted approximately 2 minutes.

46. At approximately 11:32 a.m., a call was placed from Senator Burr's cellular phone to Gerald Fauth's cellular phone. That call lasted a little less than 1 minute.

---

[8] The prior Thursday morning was February 13, 2020, the date Senator Burr ordered the equity sales.

47. Within minutes of this call, at approximately 11:34 a.m., a call was placed from Gerald Fauth's cellular phone to [redacted] a wealth management company [redacted] where Gerald Fauth and Mary Fauth held a trading account. That call [redacted] lasted approximately 24 minutes and 30 seconds.

48. In an interview [redacted] conversation with Gerald Fauth. [redacted].[9] [redacted] Fauth sounded hurried [redacted] to sell some of his stock, including stock in oil and energy companies. [redacted] Fauth [redacted] implied that he knew more [redacted] about the stock market by virtue of his position and associations in Washington, D.C. [redacted] Fauth mentioned that he knew a Senator.

49. Minutes later, consistent with Gerald Fauth's orders, [redacted] began executing the sale of some of Mary Fauth's stock. From approximately 11:55 a.m. to 11:58 a.m, sell orders were placed into an account held by Mary Fauth [redacted] selling approximately $159,100 in stock, approximately half of which consisted of stock in oil and energy companies.

---

[9] I also interviewed [redacted] February 12, 2020, [redacted] Gerald Fauth discussed generally the possibility of selling stock for two reasons: (1) COVID-19 generally, and (2) renovations to a vacation home owned by the Fauths. [redacted]

50. Later that same day, on February 13, 2020, at approximately 2:48 p.m., a call was placed from Brooke Burr's cellular phone to Mary Fauth's cellular phone. That call lasted less than one minute.

F. Senator Burr's Statements on February 27, 2020, and the March 19, 2020, Media Reports on Senator Burr's Stock Sales

51. On February 27, 2020, Senator Burr spoke to members of the Tar Heel Circle at the Capitol Hill Club in Washington, D.C. At least one person in attendance recorded Senator Burr's remarks. In that recording, Senator Burr told the group: "There's one thing I can tell you about this: It is much more aggressive in its transmission than anything we have seen in recent history. It's probably more akin to the 1918 pandemic."

52. On March 18, 2020, the day before various newspapers and media outlets began publishing reports on Senator Burr's February 13, 2020, stock trades, Senator Burr and [redacted] spoke for a lengthy period. In [redacted] interview, [redacted] However, emails show that staffers in Senator Burr's office were first notified of the media's impending coverage of the February 13 stock sales when an NPR reporter emailed the office at 11:24 a.m. Senator Burr spoke on the phone with [redacted] at 12:19 p.m., and then again at 3:02 p.m., for a total of 55 minutes and 43 seconds. Moreover, that same day, calls were placed between Brooke Burr and Gerald Fauth's phones which lasted more than 20 minutes.

53. The following day, on March 19, 2020, several media outlets began to report on Senator Burr's trading activity from February 13, 2020. On that day, the following telephone calls and emails occurred:

a. At approximately 8:23 a.m., [redacted] called Senator Burr's cellular phone. That call lasted approximately 8 minutes.

b. At approximately 11:50 a.m., a call was placed from Senator Burr's cellular phone to [redacted] cellular phone. That call does not appear to have connected.

c. At approximately 12:08 p.m., [redacted] called Senator Burr's cellular phone. That call lasted approximately 3 minutes and 40 seconds.

d. At approximately 1:55 p.m., [redacted] sent an email from his personal account to his email account [redacted] attaching a news article published by National Public Radio discussing Senator Burr's comments to members of the Tar Heel Circle at the Capitol Hill Club in Washington, D.C., discussed in paragraph 51, *supra*.

e. At approximately 3:59 p.m., [redacted] called Senator Burr's cellular phone. That call lasted for approximately 7 minutes and 40 seconds.

f. At approximately 4:10 p.m., a call was placed from Senator Burr's cellular phone to [redacted]. That call lasted approximately 3 minutes.

g. At approximately 4:14 p.m., Senator Burr placed a call from his cellular phone to [redacted] That call lasted approximately 5 minutes and 35 seconds.

h. At approximately 7:31 p.m., a call was placed from Senator Burr's cellular phone to Gerald Fauth's cellular phone. That call lasted approximately 4 minutes and 30 seconds.

54. The next day, on March 20, 2020, Senator Burr issued the following public statement on Twitter regarding the reporting of his February 13, 2020, stock trades:

> I relied solely on public news reports to guide my decision regarding the sale of stocks on February 13. Specifically, I closely followed CNBC's daily health and science reporting out of its Asia bureaus at the time. Understanding the assumption many could make in hindsight however, I spoke this morning with the

> chairman of the Senate Ethics Committee and asked him to open a complete review of the matter with full transparency.[10]

55. On March 28, 2020, FBI Special Agents called Senator Burr's cell phone and asked if they could interview him at his residence in North Carolina; he declined. At approximately 10:10 a.m., FBI Special Agents [redacted] requesting documents related to his stock trades. Following [redacted], the following communications occurred:

a. At approximately 11:49 a.m., a call was placed from Senator Burr's cellular phone to [redacted] That call lasted 32 seconds.

b. At approximately 6:10 p.m., [redacted] placed a call to Senator Burr's cellular phone. That call lasted approximately 5 minutes.

58. Beginning on February 20, 2020—six days after Senator Burr's sale of the majority of his equity—the stock market endured a dramatic and substantial downturn. In total, Senator Burr avoided more than an estimated $87,000 in loss as a result of his well-timed stock sales, and profited more than $164,000.

G. Probable Cause to Believe a Violation of the STOCK Act Occurred and that Records of that Violation Will Be Found on the Device

59. Based on the foregoing, I believe that probable cause exists that Senator Burr used material, non-public information regarding the impact that COVID-19 would have on the economy, and that he gained that information by virtue of his position as a Member of Congress, [redacted]

---

[10] *Available at* https://twitter.com/SenatorBurr/status/1241008837479542786 (last checked May 12, 2020).

[redacted] Senator Burr then [redacted] placed sell orders in Senator Burr's IRA Account and Brooke Burr's IRA Account. In total, these transactions resulted in the sale of nearly all of Senator Burr's equity positions and approximately 61% of Brooke Burr's equity positions.

60. As discussed above, this belief is based on: (1) the timing of a majority of stock sales in question, including sales directed by Senator Burr and Gerald Fauth to their respective brokers, which were effectuated on February 13, 2020; (2) the call records showing that Senator Burr directed his broker [redacted] to sell stock [redacted] on January 31, 2020 and February 13, 2020) and that Gerald Fauth directed his spouse's broker to sell stock within minutes of speaking with Senator Burr on February 13, 2020, almost at the same time that Senator Burr's broker effectuated his stock sells; (3) [redacted] (4) [redacted] that Senator Burr referenced COVID-19 among several factors that were informing his decision to sell his equities; and (5) Senator Burr's statements on February 27, 2020, which were surreptitiously recorded and which showed that Senator Burr believed at the time that the impact of COVID-19 on our nation's economy would be severe (and which contradicted his previous public statements that our nation was well-positioned to confront COVID-19).

61. Furthermore, based on the foregoing, probable cause exists to believe that communications regarding Senator Burr's possible violations of the STOCK Act will be found on the Device. Specifically, between January 31, 2020, and April 6, 2020, [redacted] text messages, nearly all of which concerned, in one way or another, the COVID-19 pandemic. Those text messages include those discussed above, and included ones regarding other issues, such as efforts to provide facemasks to the public, the "global outlook" regarding COVID-19, and a proposed "national lockdown." Therefore, there is probable cause to believe that evidence [redacted] will be found on the Device in the form of text messages. The government now seeks the instant search warrant to seize those text messages and any other evidence that may be contained on the device that relate to the investigation of whether Senator Burr, Gerald Fauth, and others violated the STOCK Act or other federal criminal statutes.

TECHNICAL TERMS

62. 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. "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.

b. 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.

c. 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.

d. "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.

e. "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.

f. 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.

g. 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.

h. "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.

i. "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.

j. "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.

k. "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.

l. "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.

m. "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.

n. "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.

63. Based on my training, experience, and research, I know that the Device, an **APPLE IPHONE XS (IMEI [redacted])**, has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. 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 offense(s) under investigation.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

64. 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 Device, 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 Device for at least the following reasons:

a. [redacted]

[redacted]

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.

a. 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.

65. 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.

f. I know that when an individual uses a digital device to engage in insider trading, fraud, and theft, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

66. 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. [redacted]

[redacted]

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. [redacted]

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.

67. 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.

BIOMETRIC ACCESS TO DEVICE

68. The proposed warrant permits law enforcement agents to obtain from the person of Burr (but not any other individuals present at the time of seizure of the execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the Device. The grounds for this request are as follows:

69. 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.

70. 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.

71. 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.

72. 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.

73. 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.

74. As discussed in this Affidavit, your Affiant has reason to believe that the Device will be found in Senator Burr's possession. The passcode or password that would unlock the Device 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, making the use of biometric features necessary to the execution of the search authorized by this warrant.

75. 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 of time. 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.

76. Due to the foregoing, if the Device may be unlocked using one of the aforementioned biometric features, the proposed warrant permits law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the Device, including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the Device found at the time of seizure; (2) hold the Device found at the time of seizure in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the Device found at the time of seizure in front of the face of the aforementioned person 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.

77. The proposed warrant does not authorize law enforcement to require that the aforementioned person state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask the aforementioned person for the password to the Device, or

to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the Device, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

AUTHORIZATION TO SEARCH AT ANY TIME OF THE DAY OR NIGHT

78. 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.

CONCLUSION

79. I submit that this affidavit supports probable cause for a warrant to search the Device described in **Attachment A** and to seize the items described in **Attachment B**, under the special search procedures set forth in **Attachment C**.

Respectfully submitted,

Brandon Merriman
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on May 13, 2020.

CHIEF JUDGE BERYL A. HOWELL
UNITED STATES DISTRICT COURT JUDGE