

# EXHIBIT A

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In Re Grand Jury Subpoena to  
Microsoft Corporation, USA, dated  
November 22, 2020, USAO  
Reference No. 2020R01153

20 Mag. 12614

§ 2705(b)  
Non-Disclosure Order  
to Service Provider

SEALED

Upon the application of the United States pursuant to 18 U.S.C. § 2705(b):

1. The Court hereby determines that there is reason to believe that notification of the existence of the attached subpoena will result in one or more of the following consequences, namely, destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Accordingly, it is hereby ORDERED:

2. Microsoft Corporation, USA (the "Provider") shall not, for a period of ~~one year~~ <sup>180 days/OTW</sup> from the date of this Order (and any extensions thereof), disclose the existence of this Order or the attached subpoena, to the listed subscribers of the accounts referenced in the subpoena, or to any other person, except that the Provider may disclose the attached subpoena to an attorney for the Provider for the purpose of receiving legal advice.

3. This Order and the Application upon which it was granted are to be filed under seal until otherwise ordered by the Court, except that the Government may without further order provide copies of the Application and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter, and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York  
November 19, 2021



UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

## **EXHIBIT A**

**20 MAG 12614**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In Re Grand Jury Subpoena to Microsoft  
Corporation, USA, dated November 22,  
2020, USAO Reference No. 2020R01153

**§ 2705(b)  
Non-Disclosure Order  
to Service Provider**

**SEALED**

Upon the application of the United States pursuant to 18 U.S.C. § 2705(b):

1. The Court hereby determines that there is reason to believe that notification of the existence of the attached subpoena will result in one or more of the following consequences, namely, endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Accordingly, it is hereby ORDERED:

2. Microsoft Corporation, USA (the “Provider”) shall not, for a period of one year from the date of this Order (and any extensions thereof), disclose the existence of this Order or the attached subpoena, to the listed subscriber of the account referenced in the subpoena, or to any other person, except that the Provider may disclose the attached subpoena to an attorney for the Provider for the purpose of receiving legal advice.

3. This Order and the Application upon which it was granted are to be filed under seal until otherwise ordered by the Court, except that the Government may without further order provide copies of the Application and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter, and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

November 23, 2020



UNITED STATES MAGISTRATE JUDGE

**United States District Court**  
**SOUTHERN DISTRICT OF NEW YORK**

TO: Law Enforcement National Security  
Microsoft Corporation, USA  
1 Microsoft Way  
Redmond, WA 98052

GREETINGS:

WE COMMAND YOU that all and singular business and excuses being laid aside, you appear and attend before the GRAND JURY of the people of the United States for the Southern District of New York, at the United States Courthouse, 40 Foley Square, Room 220, in the Borough of Manhattan, City of New York, New York, in the Southern District of New York, at the following date, time and place:

Appearance Date: November 30, 2020 Appearance Time: 10:00 a.m.

to testify and give evidence in regard to an alleged violation of :

18 U.S.C. §§ 371, 873, 1952, 2314, 2315, 2261A

and not to depart the Grand Jury without leave thereof, or of the United States Attorney, and that you bring with you and produce at the above time and place the following:

**See Attached Rider**

N.B.: Personal appearance is not required if the requested documents are: (1) produced on or before the return date to Special Agent John Vourderis, Federal Bureau of Investigation, 26 Federal Plaza, New York, New York 10278, [jvourderis@fbi.gov](mailto:jvourderis@fbi.gov), 212-384-2890; and (2) accompanied by an executed copy of the attached

Failure to attend and produce any items hereby demanded will constitute contempt of court and will subject you to civil sanctions and criminal penalties, in addition to other penalties of the Law.

DATED: New York, New York  
November 22, 2020

*Audrey Strauss / RBS*  
AUDREY STRAUSS  
*Acting United States Attorney for the  
Southern District of New York*

*Robert B. Sobelman*  
Robert B. Sobelman

Assistant United States Attorney  
One St. Andrew's Plaza  
New York, New York 10007  
Telephone: 212-637-2616



**RIDER**

Grand Jury Subpoena dated November 22, 2020

Reference # 2020R01153

1. All subscriber identifying information, including, but not limited to:
  - a. name
  - b. username or other subscriber identity or number
  - c. address
  - d. primary and alternate telephone numbers
  - e. primary and alternate email addresses
  - f. date of birth
  - g. social security number
  - h. any temporarily assigned network address
  - i. MAC address
  - j. Browser and operating system information
2. Records of session times and durations and any IP addresses used by the subscriber at the beginning, end, and at any time during these sessions;
3. Length of service (including start date) and types of service utilized; and
4. Means and source of payment for services (including any credit card or bank account number).
5. Account notes and logs, including any customer-service communications or other correspondence with the subscriber;
6. Investigative files or user complaints concerning the subscriber.

For any accounts associated with one or more of the following:

■@projectveritas.com

**20 MAG 12623**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Orders to Disclose Non-Content  
Information Associated with  
████@projectveritas.com, Pursuant to 18 U.S.C.  
§ 2703(d), USAO Reference No. 2020R001153

**TO BE FILED UNDER SEAL**

**ORDER**

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Microsoft Corporation, USA (the “Provider”), to disclose certain records and other information, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation,

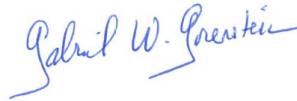
IT IS ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that the Provider will, within ten days of the date of this Order, turn over to federal law enforcement agents the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Application and this Order be sealed until otherwise ordered by the Court, and that the Provider shall not disclose the existence of this Application and/or Order of the Court, or the existence of the investigation, to the listed subscriber or to any

other person (except as necessary to carry out this Order), for a period of one year from the date of this Order.

SO ORDERED:

New York, New York  
November 24, 2020

A handwritten signature in blue ink, reading "Gabriel W. Gorenstein". The signature is written in a cursive, flowing style.

---

UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK



**ATTACHMENT A**

You are to provide the following non-content information in electronic format to Special Agent John Vourderis of the Federal Bureau of Investigation:

- any header information reflecting the names, usernames, or IP addresses of any sender(s) or recipient(s) of communications, for the time period of September 1, 2020, until the date of this Order; and
- time/date stamps, for the time period of September 1, 2020, until the date of this Order

For the following e-mail account:

■@projectveritas.com

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All  
Content and Other Information  
Associated with the Email Accounts  
[REDACTED]@projectveritas.com,  
[REDACTED]@projectvertias.com, and  
[REDACTED]@projectveritas.com,  
Maintained at Premises Controlled by  
Microsoft Corporation, USA, USAO  
Reference No. 2020R001153

**21 MAG 548**

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

**1. Warrant.** Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectvertias.com, and [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for the Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

January 14, 2021.

Date Issued

10:22pm

Time Issued

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE  
Southern District of New York

## **Attachment A**

### **I. Subject Accounts and Execution of Warrant**

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the accounts [REDACTED]@projectveritas.com, [REDACTED]@projectvertias.com, and [REDACTED]@projectveritas.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between January 1, 2020, and the date of this warrant, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator IDs GCC-1552941-K4N8V4 and GCC-1595762-L5Y8J1.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Accounts at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the

true identity of the user such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or regarding Ashley Biden, President-Elect Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding her stolen property.

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

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

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

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

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

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Account  
[REDACTED]@projectveritas.com, USAO  
Reference No. 2020R001153

21 MAG 992

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

**1. Warrant.** Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or



tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that the Provider may disclose this Warrant and Order to an attorney for the Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

1/26/2021  
Date Issued

9:56 a.m.  
Time Issued

\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE  
Southern District of New York

## **Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the account [REDACTED]@projectveritas.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between January 1, 2020, and the date of this warrant, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone

number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator ID GCC-1605213-K2V7L0.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Account at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or regarding Ashley Biden, President Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding her stolen property.

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

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

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

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

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

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Accounts  
[REDACTED]@projectveritas.com,  
[REDACTED]@projectveritas.com, and  
[REDACTED]@projectveritas.com,  
Maintained at Premises Controlled by  
Microsoft Corporation, USA, USAO  
Reference No. 2020R001153

**21 MAG 2537**

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

**1. Warrant.** Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectveritas.com, and [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 14 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 3 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

March 5, 2021  
Date Issued

8:53 am  
Time Issued

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE  
Southern District of New York

## **Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email accounts [REDACTED]@projectveritas.com, [REDACTED]@projectveritas.com, and [REDACTED]@projectveritas.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between September 1, 2020, and December 1, 2020, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Microsoft Locator ID GCC-1627882-J5F7J1.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Accounts at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the



true identity of the user such as their name, address, telephone number, email address, payment information, and other personally identifiable information.

b. Evidence of communications regarding or in furtherance of the Subject Offenses, such as communications with or regarding Ashley Biden, President Joseph R. Biden, Jr. (and representatives thereof), and/or Ashley Biden's associates regarding her stolen property.

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

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

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

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

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

**21 MAG 2711**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Order to Disclose Non-Content  
Information Associated with  
[REDACTED]@projectveritas.com, Pursuant to 18 U.S.C.  
§ 2703(d), USAO Reference No. 2020R001153

**TO BE FILED UNDER SEAL**

**ORDER**

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Microsoft Corporation, USA (the “Provider”) to disclose certain records and other information, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that disclosure to any person (including the account subscribers, the owners of any enterprise domain, and any agent, attorney, or affiliate of the foregoing) of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation,

IT IS ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that the Provider will, within ten days of the date of this Order, turn over to federal law enforcement agents the records and other information as set forth in Attachment A-1 to this Order.

IT IS FURTHER ORDERED that the Application and this Order be sealed until otherwise ordered by the Court, and that the Provider shall not disclose the existence of this Application and/or Order of the Court, or the existence of the investigation, to the listed subscriber or to any

other person (except as necessary to carry out this Order), for a period of one year from the date of this Order.

SO ORDERED:

New York, New York  
March 9, 2021

A handwritten signature in blue ink, appearing to read "Barbara Moses", is written above a horizontal line.

HON. BARBARA MOSES  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

**ATTACHMENT A-1**

You are to provide the following non-content information in electronic format to Special Agent John Vourderis of the Federal Bureau of Investigation:

- any header information reflecting the names, usernames, or IP addresses of any sender(s) or recipient(s) of communications, for the time period of September 1, 2020, until December 1, 2020; and
- time/date stamps, for the time period of September 1, 2020, until December 1, 2020

For the following email account:

██████@projectveritas.com

**21 MAG 3884**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Account  
[REDACTED]@projectveritas.com, Maintained  
at Premises Controlled by Microsoft  
Corporation, USA, USAO Reference  
No. 2020R001153

**SEARCH WARRANT AND NON-DISCLOSURE ORDER**

TO: Microsoft Corporation, USA (“Provider”)

Federal Bureau of Investigation (“Investigative Agency”)

**1. Warrant.** Upon an affidavit of Special Agent John Vourderis of the Federal Bureau of Investigation, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account [REDACTED]@projectveritas.com, maintained at premises controlled by Microsoft Corporation, USA, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within one day of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of one year from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

4/9/2021  
Date Issued

7:17 a.m.  
Time Issued



UNITED STATES MAGISTRATE JUDGE  
Southern District of New York

## **Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Microsoft Corporation, USA (the “Provider”), which is headquartered at 1 Microsoft Way, Redmond, Washington 98052, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email account [REDACTED]@projectveritas.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email) limited to items sent, received, or created between September 1, 2020, and December 1, 2020, inclusive;

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone



number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise, including those preserved pursuant to requests that were assigned Apple Reference ID 21396344.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. §§ 371 (conspiracy to transport stolen property across state lines and conspiracy to possess stolen goods), 2314 (interstate transportation of stolen property), and 2315 (possession of stolen goods) (the “Subject Offenses”), including the following:

a. Evidence sufficient to establish the user of the Subject Account at times relevant to the Subject Offenses, such as subscriber information, customer correspondence, access logs, device information, photographs, communications with other individuals or entities that reveal the true identity of the user such as their name, address, telephone number, email address, payment information, and other personally identifiable information.