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	9:56 a.m.
Date Issued	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 Account [redacted]@projectveritas.com, Maintained at Premises Controlled by Microsoft Corporation, USA, USAO Reference No. 2020R001153

21 Mag. 992

§ 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 Warrant and Order 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 or otherwise seriously jeopardizing an investigation.

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 Warrant and Order, to the listed subscriber of the account referenced in the Warrant and Order or to any other person, except that the Provider may disclose the attached Warrant and Order 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

January 13, 2022

THE HON. DEBRA FREEMAN
UNITED STATES MAGISTRATE JUDGE
UNITED STATES DISTRICT COURT

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	9:56 a.m.
Date Issued	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.