AO 106 (Rev. 06/09) Application for a Search Warrant

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)* Information associated with the e-mail account felixglobex@yahoo.com that is stored at premises controlled by Oath Holdings, Inc.	)	Case No. 18-ml-874

APPLICATION FOR A SEARCH WARRANT

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, incorporated herein by reference.

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

See Attachment B, incorporated herein 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*
See Attached Affidavit in Support of Search Warrant	

The application is based on these facts:

See Attached Affidavit in Support of Search Warrant

- ☑ 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

Carlos A. Tomala, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/13/2018

Judge's signature

City and state: Washington, D.C.

Robin M. Meriweather United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant

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)*	)	
Information associated with the e-mail account felixglobex@yahoo.com that is stored at premises controlled by Oath Holdings, Inc.	)	Case No. 18-ml-874

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

See Attachment A, hereby incorporated by reference.

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, hereby incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before December 27, 2018 *(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 Robin M. Meriweather, United States Magistrate Judge .
(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: 12/13/2018 0:00 am

Judge's signature

City and state: Washington, D.C. Robin M. Meriweather, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 18-ml-874	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 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

This warrant applies to information that is associated with the Oath account identified by **felixglobex@yahoo.com** and is stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California.

ATTACHMENT B

Particular Things to be Seized and Procedures to Facilitate Execution of the Warrant

I. Information to be disclosed by Oath Holdings, Inc. ("PROVIDER") to facilitate execution of the warrant

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, regardless of whether such information is located within or outside of the United States, including any records that have been deleted but are still available to PROVIDER, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), PROVIDER is required to disclose the following information to the government for each account or identifier listed in Attachment A ("Account"):

a. For the time period September 1, 2013 to December 31, 2016: The contents of all communications and related transactional records for all PROVIDER services used by an Account subscriber/user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, instant messaging or chat services, voice call services, or remote computing services), including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating Internet Protocol ("IP") addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

b. For the time period September 1, 2013 to December 31, 2016: The contents of all other data and related transactional records for all PROVIDER services used by an Account user (such as e-mail services, calendar services, file sharing or storage services, photo sharing or

storage services, remote computing services, instant messaging or chat services, voice call services, or remote computing services), including any information generated, modified, or stored by user(s) or PROVIDER in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, and any other saved information);

c. For the time period September 1, 2013 to December 31, 2016: All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

d. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, and server log files;

e. All records pertaining to devices associated with the Account and software used to create and access the Account, including device serial numbers, instrument numbers, model types/numbers, International Mobile Equipment Identities ("IMEI"), Mobile Equipment Identifiers ("MEID"), Global Unique Identifiers ("GUID"), Electronic Serial Numbers ("ESN"),

Android Device IDs, phone numbers, Media Access Control ("MAC") addresses, operating system information, browser information, mobile network information, information regarding cookies and similar technologies, and any other unique identifiers that would assist in identifying any such device(s);

f. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment information) concerning any PROVIDER account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

g. For the time period September 1, 2013 to December 31, 2016: All records of communications between PROVIDER and any person regarding the Account, including contacts with support services and records of actions taken; and

h. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel).

Within 14 days of the service of this warrant, PROVIDER shall deliver the information set forth above via United States mail or courier to: Acting Unit Chief Robert C. Basáñez, Federal Bureau of Investigation, J. Edgar Hoover Building, MLAT Unit, Room 7848, 935

Pennsylvania Avenue, NW, Washington D.C. 20535-0001 or email to

HQ_ISP_MLAT_Returns@FBI.gov.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of the criminal laws of Belgium, specifically, Sections 193, 196, 314, 504*bis*, and 505*ter* of the Belgian Criminal Code, regarding public contract fraud/bid-rigging and bribery, including, for each Account, information pertaining to the following matters:

(a) Information that constitutes evidence of the identification or location of the user(s) of the Account;

(b) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

(c) Information that constitutes evidence indicating the Account user's state of mind, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, related to the criminal activity under investigation;

(d) Information that constitutes evidence concerning how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Account user;

(e) Information that constitutes evidence concerning fraud, bid-rigging, and bribery with respect to public contracts and collusion and conspiracy of the same;

(f) Information regarding any communication:

a. between or among the individuals named in this affidavit, and/or other individuals associated with the companies WWDC, USK Most, NV DEME, Belfort Ltd., SM-Ltd., Porteco, Newcomb Ltd., KV-M, and Sevmorgeologia;

b. regarding consultancy agreements occurring or existing between 2013 and 2017 and related to any individual or company described in this affidavit,

c. regarding dredging or port development in Russia;

d. regarding invoices or payment instructions involving any company, individual, or for any activity described in this affidavit; and

e. regarding any attempt to conceal the identity, location, or activity of any individual, company, or transfer of funds or otherwise regarding the concealment evidence of wrongdoing.

III. Government procedures for warrant execution

The United States government will conduct a search of the information produced by the PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States and shared with appropriate foreign authorities.

Law enforcement personnel will then seal any information from PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ONE ACCOUNT STORED AT PREMISES CONTROLLED BY OATH HOLDINGS, INC., PURSUANT TO 18 U.S.C. 2703 AND 3512	**ML No. 18-874**

Reference: ***DOJ Ref. # CRM-182-59483; Subject Account: felixglobex@yahoo.com***

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Carlos A. Tomala, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information which is associated with one account – that is, felixglobex@yahoo.com– which is stored at premises controlled by Oath Holdings, Inc. ("PROVIDER"), an electronic communications services provider and/or remote computing services provider, which accepts service at 701 First Avenue, Sunnyvale, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A), and 3512(a), to require PROVIDER to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of Attachment B.

2. The information requested in this search warrant is being sought pursuant to a request for assistance ("Request") from the Federal Public Service Justice in the Kingdom of Belgium ("Belgium"), transmitted to Washington, D.C. Authorities in Belgium are investigating Sofia Mirtcheva-Neirynck ("Sofia"), the Belgian company NV DEME, and other known and unknown individuals for public contract fraud and bribery offenses, which began on or before October 2013, in violation of the criminal law of Belgium, specifically, Sections 193, 196, 314, 504*bis*, and 505*ter* of the Belgian Criminal Code. A copy of the applicable laws is appended to this application. This Request is made pursuant to the Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance Between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty Between the United States of America and the Kingdom of Belgium on Mutual Legal Assistance in Criminal Matters signed 28 January 1988, Belg.-U.S., Dec. 16, 2004, S. TREATY DOC. NO. 109-13 (2006) (hereinafter, the "Instrument"). Under the Instrument, the United States is obligated to render assistance in response to the Request.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 1997. I am currently assigned to the International Operations Division, Mutual Legal Assistance Treaty Unit, in Washington, D.C. My current duties include responding to requests from foreign governments pursuant to mutual legal assistance treaties, including serving as the affiant on search warrant affidavits, serving search warrants, and reviewing the data received in response thereto for relevance in compliance with the parameters of the search warrants. During my employment with the FBI, I have conducted investigations related to high technology and cybercrimes, cyber intrusions, remote delivery of exploits, and cyber offensive attacks. I have also worked on numerous criminal and counterintelligence investigations. I have experience in

the execution of search warrants and the analysis of collected evidence. Additionally, I have received training in the operation of computers and the collection and handling of digital evidence. I have been trained by the FBI as a Digital Extraction Technician ("DExT") and received specialized training in several forensic software programs, such as Forensic Toolkit ("FTK"), EnCase, and X-Ways Forensics.

4. The facts set forth in this affidavit are based upon information conveyed to the United States via the Request made pursuant to the Instrument by authorities in Belgium and upon my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

5. 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 the criminal laws of Belgium have been committed by Sofia Mirtcheva-Neirynck ("Sofia"), executives of the Belgian company NV DEME, and other known and unknown individuals. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

6. Pursuant to the applicable treaty, this Court has jurisdiction to issue the proposed Order. *See* Instrument Annex art. 16(1) (authorizing courts to issue orders necessary to execute the request). In addition, 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. *See* 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court "is acting on a request for foreign assistance pursuant to [18 U.S.C.] section 3512 . . . ." 18 U.S.C. § 2711(3)(A)(iii); *see also* 18 U.S.C.

§ 3512(a)(2)(B) (court may issue "a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703"), § 3512(c)(3) ("application for execution of a request from a foreign authority under this section may be filed . . . in the District of Columbia").

7. This application to execute Belgium's request has been approved and duly authorized by an appropriate official of the Department of Justice, through the Criminal Division, Office of International Affairs ("OIA").[1] *See* 18 U.S.C. § 3512(a). An OIA attorney has authorized the undersigned to file this application.

PROBABLE CAUSE

8. Authorities in Belgium are investigating Sofia, executives of the Belgian company NV DEME, and other known and unknown individuals (collectively, "the suspects") for fraud (i.e. bid-rigging) and bribery in obtaining a public contract to conduct dredging in the Russian port of Sabetta on the Yamal peninsula. According to Belgian authorities, NV DEME, through its agent, Sofia, bribed its way into winning the lucrative dredging contract for the Russian port and used a series of shell companies to launder the bribe money. Evidence gathered by Belgian authorities establishes that NV DEME's Chief Executive Officer ("CEO") Alain Bernard ("Bernard"), Group Finance Manager for International Dredging Bart Vandemeulebroucke ("Vandemeulebroucke"), Manager of Estimates Girard "Gerd" Moyson ("Moyson"), and Area Director for Russia and Eastern Europe Dirk Poppe ("Poppe") were directly involved in the criminal activity.

[1] The Attorney General, through regulations and Department of Justice directives, has delegated to the Office of International Affairs the authority to serve as the "Central Authority" under treaties and executive agreements between the United States and other countries pertaining to mutual assistance in criminal matters. *See* 28 C.F.R. §§ 0.64-1, 0.64-4, and Appendix to Subpart K, Directive Nos. 81B and 81C (2018).

The Sabetta Dredging Subcontract

9. A Russian state-owned port company is responsible for the development of an important harbor terminal in Sabetta, Russia on the Yamal peninsula. As part of this development project, the state-owned Russian company selects a managing contractor to design public tenders and allocate various subcontracts for the execution of the project. With respect to the dredging of the harbor, the state-owned company selected the Russian company USK Most as the managing contractor to oversee the public tender. On or about November 6, 2013, USK Most formally announced the public tender for a subcontract to conduct dredging in the Sabetta harbor from 2014 through 2017. The subcontract had an initial estimated value of EUR 4 million (approximately USD 5.4 million). By contract and statute, USK Most and its agents were bound by confidentiality to ensure an open and competitive bidding process for the dredging subcontract and were not permitted to release confidential information regarding competitors' bids and proposals. Two Belgian companies – NV JAN DE NUL ("the Victim Company") and NV DEME submitted competing bids for the contract.

10. Prior to the publication of the public tender, between September 2002 and August 2012, Sofia served as NV DEME's business development and deputy area director for Russia and Eastern Europe. Sofia, who is a naturalized Belgian citizen of Bulgarian origin and speaks fluent Russian, specialized in consulting with regard to the Russian market. On August 31, 2012, Sofia formally left the employment of NV DEME to work as an independent consultant. However, in reality, Sofia continued her role in advancing NV DEME's interests in contracts in Russia and Eastern Europe under the facade of an independent consultancy. For example, despite not formally leaving NV DEME until August 31, 2012, Belgian authorities obtained a "Consultancy and Service Agreement" between NV DEME and Sofia's Belgian consultancy

company, BVBA Porteco ("Porteco"), dated June 18, 2012. Sofia established the company less than a year prior, in October 2011. The agreement outlined Sofia's role in supporting NV DEME's business activities, including dredging, in Russia and the former Soviet Republics.

11. Despite Sofia's official and unofficial relationship with NV DEME, she proceeded to conclude a contemporaneous contract with USK Most in December 2012 with regard to the Sabetta harbor dredging project. According to the contract, Sofia would participate in the development of the public tender and sit on the evaluation board charged with reviewing subcontractor bids and awarding the ultimate subcontract. Thus, from 2012 through 2014, Sofia was simultaneously contracted to assist NV DEME in winning Russian dredging contracts and to serve on the evaluation board of a public tender on which NV DEME was bidding, a clear conflict of interest.

12. This conflict of interest was first discovered in March 2014, when Sofia, together with the chair of the public tender evaluation board, Sergey Komkov ("Komkov"), visited the Victim Company and NV DEME in Belgium to evaluate their respective bids. It was at this time that the Victim Company learned that Sofia – who was already known to the Victim Company due to her longstanding role in business consulting for NV DEME– was on the evaluation board for the public tender. On April 11, 2014, the Victim Company received a letter informing them that they were not selected for the dredging subcontract. The subcontract was instead awarded to NV DEME and its Russian subsidiary.

13. Following their own private investigation, the Victim Company provided Belgian authorities with numerous e-mails between October 2013 and November 2014 between Sofia and the NV DEME leadership. These included e-mails from Sofia to the NV DEME e-mail accounts of Poppe and Bernard requesting personal e-mail addresses Sofia could use to contact them about

the dredging project through unofficial channels. Sofia also e-mailed Bernard, Poppe, and Moyson to discuss updates regarding the dredging project and share confidential competitors' bids including that of the Victim Company.

The Bribe Money

14. A review of business records for Sofia's Belgian company, Porteco, established that in the period from October 1, 2012, through November 30, 2013, NV DEME made payments to Porteco totaling EUR 175,340 (approximately USD 236,569) pursuant to their official consultancy agreement. According to Belgian authorities, this amount represented a reasonable market price for the type of official consultancy services outlined in the contract. Business records also established that Porteco likewise received payment from USK Most for the consultancy services outlined in Sofia's official contract with the company related to the public tender. Despite official business records showing that Sofia, through her firm Porteco, was fully compensated for her official services for both contracts, Belgian authorities subsequently uncovered evidence that, following the awarding of the dredging contract to NV DEME, Sofia and Komkov—her counterpart at USK Most— were each paid an additional EUR 4,188,000 (approximately USD 5,650,450) through a series of shell companies with links to NV DEME.

15. Following their loss of the subcontract and their own independent investigation, the Victim Company reported the suspected public contracting fraud to Belgian authorities on September 8, 2016. As part of their complaint, the Victim Company provided authorities with a variety of records they had privately obtained, including copies of e-mail communication between NV DEME leadership and Sofia as well as the consultancy contracts between NV DEME and Sofia. Belgian authorities subsequently conducted searches of the suspects' homes and obtained records from Belgian banks and e-mail providers. These materials evidenced a

scheme by which NV DEME laundered money through companies registered in Cyprus and Panama in order to bribe Komkov (of USK Most) and Sofia to obtain the dredging subcontract.

16. Based on these records, Belgian authorities determined that, between June 2014 and February 2018, Sofia was scheduled to receive EUR 4,188,000 in monthly payments made to two Bulgarian companies registered in her name: Belfort LTD ("Belfort") and Sofia Mirtcheva LTD ("SM-Ltd."). The payments were to be made according to "local consultancy agreements" between Sofia's two Bulgarian companies and a company named World Wide Dredging Corporation ("WWDC"). WWDC is registered in Cyprus, and further information about its activities is currently the subject of a pending mutual legal assistance request by Belgium to Cyprus. Pursuant to these agreements, Sofia would provide generic consulting services to WWDC amounting to a total of EUR 4,188,000. The respective agreements provided that Sofia's Bulgarian companies, Belfort and SM-Ltd., would submit periodic invoices to WWDC pursuant to a schedule of payments between June 2014 and February 2018. However, based on e-mails provided by the Victim Company and obtained from providers, the consultancy agreements, invoices, and payment schedule were all transmitted by e-mail between Sofia and the leadership of NV DEME, in particular its Group Finance Manager Vandemeulebroucke.

17. Simultaneously, Belgian authorities uncovered evidence of a local consultancy agreement between WWDC and an unknown Panamanian company KV-M Ltd. ("KV-M"). Based on e-mail records and a copy of the agreement obtained by Belgian authorities, Sofia provided the consultancy contract, invoices, and payment schedule for KV-M to WWDC, while an individual named Felix Vakhovsky ("Vakhovsky") served as the official agent of KV-M. Like the agreements between WWDC and Sofia's two Bulgarian firms, WWDC agreed to pay KV-M EUR 4,188,000 in monthly installments between June 2014 and May 2018. Pursuant to

the agreement, Sofia would routinely submit invoices on behalf of KV-M to WWDC. In turn, WWDC would send payments to KV-M; however, Belgian authorities determined through bank records that those payments were ultimately routed through a series of banks before ending in a Swiss bank account registered to the unknown company, Newcomb Ltd. ("Newcomb"). Notably, Komkov, using the alias "Vasya Vasechkin," was blind-carbon-copied on e-mails between Sofia and Vakhovsky regarding KV-M invoices and payments.

18. Based on these records, Belgian authorities believe that Vakhovsky served as a straw man, and that KV-M served as a pass-through company to conceal payments that actually originated with NV DEME and ended with Komkov. This conclusion is supported by the fact that the contracts between WWDC and Belfort and SM-Ltd. on one hand, and between WWDC and KV-M, on the other, were agreed contemporaneously with each other and with the April 2014 award of the dredging contract to NV DEME. The contracts between WWDC, KV-M, and Sofia's Bulgarian companies provided for the payment of identical amounts of EUR 4,188,000 in nearly identical installments over the time period of 2014 through the spring of 2018, a time period coinciding with the anticipated duration of the Russian dredging contract awarded to NV DEME (anticipated to be performed from 2014 through at least December 2017). Finally, all recovered communication regarding the local consultancy agreements, invoices, and payment schedules was conducted between Sofia, Komkov, Vakhovsky, and the NV DEME leadership.

19. Belgian authorities believe that WWDC, KV-M, and Newcomb are shell companies established by or at the direction of NV DEME and Sofia to launder bribe money to Sofia, Komkov, and possibly others in order to unlawfully obtain lucrative dredging contracts in Russia. Authorities have more recently identified another shell company, Sevmorgeologia, which is associated with Andrei Ovsyannikov. E-mail records obtained from NV DEME Group

Finance Manager Vandemeulebroucke's account confirmed that this company was receiving money from NV DEME-*cum*-WWDC during the same time period as KV-M, Belfort, and SM-Ltd. E-mail records obtained from Google LLC ("Google LLC") further confirmed that Ovsyannikov, via his Russian e-mail account Sivers1@yandex.ru, was in regular contact with Sofia and Vandemeulebroucke during the time period contemporaneous with the payments to Komkov and Sofia, that is, from October 2014 through June 2016.

20. As part of their investigation, Belgian authorities uncovered evidence that at least nine e-mail accounts hosted with U.S. providers were used by the respective suspects to communicate regarding the dredging project and subsequent payments to Sofia and Komkov. Belgian authorities are now seeking records for the following e-mail accounts belonging to the suspects to gather additional evidence, determine the scope of the criminal conduct, and identify accomplices[2]:

a. **Porteco.sofia@gmail.com**[3] is the official e-mail account for Sofia's Belgian consulting company, **Porteco**, with which NV DEME concluded a contract for consulting services beginning on June 18, 2012. The Victim Company provided authorities with copies of e-mails it had obtained between the account, Komkov, and other accounts belonging to USK Most or Sofia in April and July 2014. Notably, despite the fact that this account uses the name of the Belgian company with which NV DEME concluded its consultancy agreement, this account appears

[2] The United States previously obtained court orders issued pursuant to 18 U.S.C. §2703(d) for these accounts. *See In re Application of USA Pursuant to 18 U.S.C. 3512 for 2703(d) Order for Eight E-mail Accounts Serviced by Google LLC*, No. 1:18-ml-00722 (D.D.C. October 11, 2018); *In re Application of USA Pursuant to 18 U.S.C. 3512 for 2703(d) Order for One E-mail Account Serviced by Oath Holdings, Inc.*, No. 1:18-ml-00723 (D.D.C. October 24, 2018).

[3] These Gmail accounts are the subject of an application for a search warrant filed contemporaneously with the instant application in case number 18-ml-873.

to have been used almost exclusively to communicate with Komkov and others at USK Most, as well as with Sofia's other accounts. E-mails obtained by Belgian authorities included a discussion of Sofia and Komkov's collaboration on the Russian dredging project and consultancy agreements with WWDC. For example, on April 5, 2014, Komkov sent Sofia an e-mail at this account with the subject line "DEME vs. JDN" and an attachment containing an evaluation of the competing offers. On April 26, 2014, Komkov e-mailed Sofia congratulating her on the victory of DEME in the public tender. In her response, Sofia promises Komkov that he and his wife deserve a VIP holiday for their work. Sofia forwarded herself an e-mail from NV DEME's Group Finance Manager Vandemeulebroucke providing the value-added-tax (VAT) and billing information for WWDC to be used in the invoices for agreements with Belfort, SM-Ltd., and KV-M. Records from Google also established that the account was created on November 4, 2013 and was used to communicate regularly with Komkov and with other e-mail accounts with USK Most's official domain between November 2013 and September 2016. The records evidence that this account was created and used to be Sofia's primary mechanism of communication with USK Most regarding the dredging project.

b. **sofianeirynck@gmail.com** is Sofia's personal e-mail account. The Victim Company provided Belgian authorities with several e-mails from November 2012 through May 2016 between this account and NV DEME leadership and Komkov. For example, in November 2012, Sofia used this account to exchange a series of e-mails with Bernard and Poppe regarding the Russian dredging project. In the e-

mail communication, Sofia informs them that she will be working with USK Most on the dredging project and that this presented a "very good opportunity for all" that she would like to discuss in person. A month later, on December 2, 2012, Sofia used this account to transmit to Bernard and Poppe partial submissions of subcontract bids from various competitors. In response, Bernard inquired as to the status of the bid of their Belgian competitor, the Victim Company. Belgian authorities also recovered a May 6, 2016, e-mail to Komkov in which Sofia provides confirmation of a series of 2016 invoice payments made by WWDC to KV-M. Attached to that e-mail was a spreadsheet showing payments and invoices involving "Felix," (presumably Vakhovsky) and a "Mister X."

c. **Belfortltd@gmail.com** is associated with one of Sofia's two Bulgarian consultancy companies, Belfort. Despite NV DEME having no formal relationship with Sofia's Bulgarian companies, the Victim Company provided Belgian authorities with numerous e-mails between October 2013 and November 2014 between this account and NV DEME leadership. These included e-mails from Sofia to the NV DEME e-mail accounts of Poppe and Bernard requesting personal e-mail addresses Sofia could use to contact them about the dredging project through unofficial channels. Sofia also used this account throughout 2014 to discuss with NV DEME leadership, including Moyson and Vandemeulebroucke, updates regarding the dredging project, share confidential competitors' bids, and subsequently to exchange agency agreements and invoices for WWDC. For example, on February 6, 2014, a few months prior to the award of the subcontract, Poppe sent an e-mail to Sofia at this address directing her to

remove a reference to her prior position with NV DEME from her LinkedIn account. This account was also used to communicate with Komkov, then using the alias "Vasya Vasechkin," regarding the contracts and payments between WWDC and KV-M and to provide Komkov with copies of invoices "already sent to the client." Non-content records obtained pursuant to a prior court order confirmed that Sofia used this count to communicate with Moyson in the months leading up to the award of the subcontract; with Poppe between October 5, 2013 and May 18, 2016; with Bernard between at least October 15, 2013, and Vandemeulebroucke between May 20, 2014 and May 14, 2016. Sofia also used this account to communicate regularly with Komkov and Vasechkin between May 2014 and September 2016. Sofia also repeatedly sent e-mails from this account to other e-mail accounts owned by her, including **eoodsm@gmail.com**, sofia.detelina@gmail.com, **porteco.sofia@gmail.com**, **sofianeirynck@gmail.com**, and **sabeta03250@gmail.com**.

d. **eoodsm@gmail.com** is an account associated with Sofia's second Bulgarian company, SM-Ltd; the e-mail name derives from the Bulgarian name for the company, as the Bulgarian version of "Ltd." is "EOOD." Additionally, subscriber records obtained from Google established that this account was first created on May 16, 2014; the same day Sofia immediately received e-mails from her other accounts **belfortltd@gmail.com**, **sabeta03250@gmail.com**, **sofiamircheva@gmail.com**, and on May 19, sent an e-mail to Vandemeulebroucke at **debouwer2014@gmail.com**. The timing of the registration and immediate use to communicate primarily with herself and with

Vandemeulebroucke strongly suggests the account was set up for the purpose of facilitating the payments between WWDC and SM-Ltd. Belgian authorities obtained a June 6, 2014, e-mail in which Sofia used this account to forward an e-mail to herself at **belfortltd@gmail.com** containing the payment schedule for the consultancy agreements with WWDC. Moreover, in a May 16, 2014, e-mail from her personal account to Vandemeulebroucke, Sofia provided the payment schedule for WWDC to Sofia's Bulgarian companies, proposed to Vandemeulebroucke that they "communicate via separate mails," and promised that she would send him the "e-mail address for [SM-Ltd]," understood to be this account. Non-content records established that Sofia used this account between May 2014 and May 2016 to communicate with Vandemeulebroucke at **debouwer2014@gmail.com** monthly, corresponding to the schedule of periodic invoices for the bribe payments.

e. **Sabeta03250@gmail.com** is an account bearing a name derived from the Russian dredging project in the port of Sabetta and recovered e-mails are signed by "Olga Pankratova." However, evidence indicates that this account belongs to Sofia. Belgian authorities obtained a March 20, 2014, e-mail from Google to Sofia's e-mail **belfortltd@gmail.com**. The e-mail header information indicated that **belfortltd@gmail.com** had itself been configured to appear as though it was from "Olga Pankratova," with the "To" line reading "Olga Pankratova <belfortltd@gmail.com>." The message from Google confirmed the creation of the new e-mail account **sabeta03520@gmail.com**. The same day, Sofia, using **belfortltd@gmail.com**, forwarded the e-mail in which Bernard had provided his

personal address to this account (**sabeta03250@gmail.com**). Additionally, on July 1, 2014, this account was used to forward an e-mail from Vandemeulebroucke to Sofia's account **porteco.sofia@gmail.com.** That e-mail contained the VAT and billing information for WWDC for Sofia to use in the invoices for agreements with Belfort, SM-Ltd, and KV-M. Non-content records obtained from Google confirmed that this account was registered with **belfortltd@gmail.com** under the alias Olga Pankratova. This account appears to have been used to communicate almost exclusively with NV DEME leadership, including Vandemeulebroucke, Ovsyannikov at **sivers1@yandex.ru**, and periodically with Sofia's other e-mail accounts.

f. **Bernard.alain65@gmail.com** is the personal account of NV DEME CEO Alain Bernard. Following direct e-mail communication between Sofia and Bernard's official NV DEME e-mail account regarding the Russian dredging subcontract in 2012 and 2013, Sofia began requesting that Bernard and other NV DEME officials begin communicating with her through personal e-mail accounts in 2014, coinciding with the award of the subcontract to NV DEME and conclusion of WWDC consultancy agreements. For example, Belgian authorities were provided with a copy of a March 15, 2014, e-mail from Sofia to Bernard using Bernard's official NV DEME e-mail account. The subject line was "PLS send me your private mail address, tnks." Bernard replied, providing Sofia with this account and copied **sabet03250@gmail.com**. Non-content records obtained from Google established that Bernard used this account to communicate repeatedly

with Sofia at **belfortltd@gmail.com** from August 2014 through April 2016, and with **sabeta03250@gmail.com** between at least June 2014 and July 2016.

g. **Gerd.moyson@gmail.com** is the personal account of Moyson, Manager of the Estimates Department at NV DEME. Authorities obtained e-mails from November 25, 2013, and February 20, 2014, in which Sofia transmitted confidential information regarding competing bids for the dredging project to this account, and Moyson responded providing his analysis and directions for how to proceed.

h. **Debouwer2014@gmail.com** is believed to be the personal account of Vandemeulebroucke, NV DEME's Group Finance Manager of International Operations. Subscriber records obtained from Google established that the account was created on May 9, 2014, and linked to the account bvm2000@gmail.com, "bvm" likely corresponding to Bart Vandemeulebroucke. In 2014, Belgian authorities recovered e-mails to this account from Sofia regarding the consultancy agreements and payment invoices between WWDC and KV-M, Belfort, and SM-Ltd. The e-mails established that Sofia transmitted the invoices meant for WWDC to Vandemeulebroucke at this account. For example, on May 16, 2014, Sofia transmitted the "financial schedule for the contracts in Bulgaria" to this account. This account was subsequently used to provide Sofia the VAT and billing information to be included in the WWDC consultancy agreements and invoices on July 1, 2014. An in a November 14, 2014, e-mail provided to Belgian authorities, Sofia e-mailed October and November invoices for WWDC to this account. Non-content records for the account establish the account was created

just after the award of the subcontract and was used to communicate almost exclusively with Sofia, NV DEME leadership, and **sivers1@yandex.ru**. The timing and use of the account, as well as the registration of the account under an alias, evidence that the account was created for the purpose coordinating the bribery payments between NV DEME, Sofia, and Komkov. Google records established that the account was used routinely to contact Sofia at numerous of her accounts between May 2014 and September 2016, as well as to contact Ovsyannikov between at least June 2014 and June 2016.

i. **felixglobex@yahoo.com** is a personal account belonging to Felix Vakhovsky. Vakhovsky is believed to be the strawman for KV-M, the pass-through company through which payments from WWDC flow to Newcomb/Komkov. In September 2014, e-mails were recovered showing that Sofia transmitted the WWDC—KV-M consultancy agreement and invoices to Vakhovsky. On November 30, 2014, an e-mail from an as yet unidentified individual sent an e-mail to this account with the subject line "consulting agreement KVM-Newcomb" and an attachment of the ostensible consulting agreement. The e-mail also contained directions for Vakhovsky to draw up an agreement between KV-M and Newcomb and an explanation of the payment schedule. According to records obtained from Google, Sofia, using **belfortltd@gmail.com**, contacted this account in monthly intervals corresponding to the schedule of invoice payments between at least September 2014 and April 2016. In her e-mails to Vakhovsky, Sofia routinely blind-carbon-copied Komkov's e-mail jam2014-17@yandex.ru.

21. The e-mail account **felixglobex@yahoo.com** is hosted by PROVIDER.

BACKGROUND CONCERNING PROVIDER'S ACCOUNTS

22. PROVIDER is the provider of the internet-based accounts identified by felixglobex@yahoo.com.

23. PROVIDER provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. PROVIDER accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other PROVIDER services, such as instant messages and remote photo or file storage.

24. Based on my training and experience, I know that PROVIDER allows subscribers to obtain accounts by registering with PROVIDER. During the registration process, PROVIDER asks subscribers to create a username and password, and to provide basic personal information, such as a name, an alternate e-mail address for backup purposes, a phone number, and in some cases, a means of payment. PROVIDER typically does not verify subscriber names. However, PROVIDER does verify the e-mail address or phone number provided.

25. Once a subscriber has registered an account, PROVIDER provides e-mail services that typically include folders, such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. PROVIDER subscribers can also use that same username or account in connection with other services provided by PROVIDER.

26. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a PROVIDER account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete

an e-mail, the e-mail can remain on PROVIDER's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on PROVIDER's servers for a certain period of time.

27. A subscriber's PROVIDER account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on PROVIDER's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on PROVIDER's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on PROVIDER's servers for a certain period of time. Furthermore, a PROVIDER subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on PROVIDER's servers. Based on my training and experience, I understand that evidence of who controlled, used, and/or created a PROVIDER account may be found within such computer files and other information created or stored by the PROVIDER subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

28. Based on my training and experience, I know that providers such as PROVIDER also collect and maintain information about their subscribers, including information about their use of PROVIDER services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as PROVIDER also

commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as PROVIDER typically collect and maintain location data related to subscriber's use of PROVIDER services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

29. Based on my training and experience, I understand that providers such as PROVIDER also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by PROVIDER in order to track what devices are using PROVIDER's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other PROVIDER accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during the course of the investigation was used to access the PROVIDER account.

30. Based on my training and experience, I understand that providers such as PROVIDER use cookies and similar technologies to track users visiting PROVIDER's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to PROVIDER. More sophisticated cookie technology can be used to identify users across devices and web browsers. From training and experience, I know that cookies and similar technology used by providers such as PROVIDER may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a PROVIDER account and determine the scope of criminal activity.

31. Based on my training and experience, I understand that PROVIDER maintains records that can link different PROVIDER accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple PROVIDER accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular PROVIDER account.

32. Based on my training and experience, I understand that subscribers can communicate directly with PROVIDER about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as PROVIDER

typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

33. In summary, based on my training and experience in this context, I believe that the computers of PROVIDER are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for PROVIDER subscribers), as well as PROVIDER-generated information about its subscribers and their use of PROVIDER services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide PROVIDER with false information about their identities, that false information often provides clues to their identities, locations, or illicit activities.

34. As explained above, information stored in connection with a PROVIDER account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the investigating authorities to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a PROVIDER account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or

controlled the account at a relevant time. Further, information maintained by PROVIDER can show how and when the account was accessed or used. For example, providers such as PROVIDER typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the PROVIDER account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the PROVIDER account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).[4]

CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on PROVIDER who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

---

[4] At times, communication service providers such as PROVIDER can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of PROVIDER's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

Respectfully submitted,

Carlos A. Tomala
Supervisory Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 13, 2018

Robin M. Meriweather
UNITED STATES MAGISTRATE JUDGE

Relevant Provisions of the Belgian Criminal Code

Section 193
Forgery of documents, [computer data], or telegrams with a fraudulent intent or with the intent to harm will be punished in accordance [with the following] sections.

Section 196 Penal Code
Imprisonment from 5 to 10 years will [be the punishment for] persons who commit a forgery of public and official documents, and all those who commit a forgery of commercial, bank, or private documents, whether by false signatures, counterfeiting, altering writing and signatures, or by making agreements, dispositions, obligations, or discharges, or by their insertion after the fact, or by adding or altering clauses, declarations, or facts that these acts were intended to incorporate or to record.

Section 314 Penal Code
A person who, in the award of property, of usufruct, of the rental of real or personal property, of a business, of the supply or the exploitation of any service, obstructed or disturbed the freedom of bidding or tendering, by violence or by threat, by gifts or promises, or by any fraudulent means, will be punished by an imprisonment of 15 days to 6 months and a fine of 100 to 3,000 euro.

Section 504*bis* Penal Code
(1) Passive private bribery is constituted by the fact that a person who is a director or manager of a legal person or trustee or agent of a legal or natural person, solicits, accepts or receives, directly or through intermediaries, an offer, a promise, or an advantage of any kind, for themselves or for a third party, to perform or refrain from performing an act of their office or facilitated by their office, without the knowledge or authorization, as the case may be, of the board of directors, the general assembly, the trustee, or the employer.

(2) Active private bribery is the constituted by the act of proposing, directly or through intermediaries, to a person who is a director or manager of legal person or trustee or agent of a legal or natural person an offer, a promise, or an advantage of any kind, for themselves or for a third party, to do or to refrain from performing an act of their office or facilitated by their office, without the knowledge or authorization, as the case may be, the board of directors, the general assembly, the trustee, or the employer.

Section 504*ter*
(1) In the case of private corruption, the penalty will be imprisonment of six months to two years and a fine of 100 euros to 10,000 euros or one of these penalties.

(2)Where the act referred to in Article 504*bis*(1) is followed by a proposal referred to in Article 504*bis*(2), likewise in the case where the proposal referred to in Article 504*bis*(2) is accepted, the sentence shall be imprisonment from six months to three years and a fine of 100 euros to 50,000 euros or one of these penalties.