IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA v. JERRY BAPTISTE, *et al*.	Criminal Action No. 1:20-CR-296-JPB-CMS-13

DEFENDANT BAPTISTE'S MOTION TO SUPPRESS EVIDENCE AND FRUITS SEIZED PURSUANT TO THE SEARCH WARRANT DIRECTED TO GOOGLE FOR NETBASEDSTUDIOS@GMAIL.COM AND MEMORANDUM OF LAW IN SUPPORT

EXHIBIT ONE

U.S.D.C ATLANTA
Date: Aug 18 2020
JAMES N. HATTEN, Clerk
By: s/B. Evans
Deputy Clerk

(Rev. 4/30/2014 Search Warrant

United States District Court

Northern District of Georgia

In the Matter of the Search of:

Information associated with the email addresses DARRELL.THOMAS1986@GMAIL.COM; GRESERVETRAVEL@GMAIL.COM; BERNBENOIT23@GMAIL.COM; TRANSPORTMANAGEMENTINC@GMAIL.COM; NETBASEDSTUDIOS@GMAIL.COM; CHARLESWILLIAMKNIGHT7@GMAIL.COM; and CREATEIMPACT75@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 1:20-mc-1472

I, Joseph D. Stites, being duly sworn, depose and says:

I am a(n) Special Agent of the FBI, and have reason to believe that, on the property or premises known as

Information associated with the email addresses DARRELL.THOMAS1986@GMAIL.COM; GRESERVETRAVEL@GMAIL.COM; BERNBENOIT23@GMAIL.COM; TRANSPORTMANAGEMENTINC@GMAIL.COM; NETBASEDSTUDIOS@GMAIL.COM; CHARLESWILLIAMKNIGHT7@GMAIL.COM; and CREATEIMPACT75@GMAIL.COM, as further described in Attachment A.

There is now concealed certain property, certain data, and certain information, namely,

See Attachment B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a criminal offense, concerning violations of Title 18, United States Code, Sections 1343, 1344, 1349, 1014, 1956, and/or 1957, over which the United States District Court for the Northern District of Georgia has jurisdiction. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. ☒Yes ☐No

Joseph D. Stites
Signature of Affiant
Joseph D. Stites

Sworn to me by telephone pursuant to Federal Rule of Criminal Procedure 4.1

August 18, 2020 at Atlanta, Georgia
Date City and State

JUSTIN S. ANAND
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA Tal C. Chaiken / 404-581-6069

AFFIDAVIT

I, JOSEPH D. STITES, hereby depose and state under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since July 2004. I am currently assigned to the Atlanta Division investigating financial crimes, including identity theft, wire, mail, and bank fraud. I am also trained as a Certified Public Accountant (CPA) and Certified Fraud Examiner (CFE). I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

2. I submit this Affidavit in support of an Application for a search warrant for information associated with the email accounts

- **DARRELL.THOMAS1986@GMAIL.COM;**
- **GRESERVETRAVEL@GMAIL.COM;**
- **BERNBENOIT23@GMAIL.COM;**
- **TRANSPORTMANAGEMENTINC@GMAIL.COM;**
- **NETBASEDSTUDIOS@GMAIL.COM;**

- **CHARLESWILLIAMKNIGHT7@GMAIL.COM;** and
- **CREATEIMPACT75@GMAIL.COM,**

that is stored at premises controlled by Google LLC ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043; and the email account **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM** that is stored at premises controlled by GoDaddy.com ("GoDaddy"), a service provider headquartered at 14455 N. Hayden Road, Suite 219, Scottsdale, AZ 85260 (collectively, the "**SUBJECT EMAIL ADDRESSES**"). 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), and 2703(c)(1)(A) to require Google 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 the information to locate the items described in Section II of Attachment B.

Jurisdiction

3. 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 a district court of the United States that has jurisdiction over the offenses being investigated.

4. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant because, as described in Attachment A and Attachment B, the email provider will execute the seizure and provide the information to law enforcement. For this same reason, I request that this search warrant be executable at any time, day or night.

Applicable Criminal Laws

5. The wire fraud statute, 18 U.S.C. § 1343, makes it a federal crime for anyone, having devised or intending to devise any scheme and artifice to defraud by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

6. The bank fraud statute, 18 U.S.C. § 1344, makes it a federal crime to execute or attempt to execute a scheme or artifice to defraud a financial institution or to obtain any of the moneys, funds, credits, assets,

securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretenses, representations, or promises.

7. 18 U.S.C. § 1349 makes it a federal crime to conspire to commit wire fraud or bank fraud.

8. Pursuant to 18 U.S.C. § 1014, it is a federal crime to, among other things, knowingly make a false statement or report for the purpose of influencing any institution the accounts of which are insured by the Federal Deposit Insurance Corporation, regarding any application or loan.

9. Pursuant to 18 U.S.C. § 1956(a)(1)(B)(i), it is a federal crime to engage in a financial transaction, knowing that it involves funds that are the proceeds of some unlawful activity, including wire fraud, if those funds were in fact the proceeds of unlawful activity, including wire fraud, and if the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the unlawful activity.

10. Pursuant to 18 U.S.C. § 1957, it is a federal crime to knowingly engage or attempt to engage in a monetary transaction, knowing that the transaction involved property or funds that were the proceeds of some criminal activity, including wire fraud, if the property had a value of more

than $10,000, the property was in fact proceeds of that specified unlawful activity, and the transaction took place in the United States.

PROBABLE CAUSE

11. As explained in more detail below, the government is investigating alleged fraud and money laundering committed by several individuals who obtained Paycheck Protection Program ("PPP") loans for their businesses.

12. On August 4, 2020, a grand jury sitting in the Northern District of Georgia returned a 30-count indictment against DARRELL THOMAS, ANDRE LEE GAINES, KAHLIL GIBRAN GREEN, SR., BERN BENOIT, and CARLA JACKSON, charging them with violations of 18 U.S.C. § 1344 (bank fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (conspiracy to commit bank fraud and wire fraud); 18 U.S.C. § 1014 (false statement to a federally insured financial institution); and/or 18 U.S.C. §§ 1956 and 1957 (money laundering).

13. As explained further below, I respectfully submit that there is probable cause to believe that DARRELL THOMAS and his associates used, and are using, the **SUBJECT EMAIL ADDRESSES** to carry out and facilitate the above-described violations.

The Paycheck Protection Program

14. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act is a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to $349 billion in forgivable loans to small businesses for job retention and certain other expenses, through a program referred to as the PPP. In or around April 2020, Congress authorized over $300 billion in additional PPP funding.

15. In order to obtain a PPP loan, a qualifying business must submit a PPP loan application, which must be signed by an authorized representative of the business. The PPP loan application requires the business (through its authorized representative) to acknowledge the program rules and make certain affirmative representations and certifications in order to be eligible to obtain the PPP loan. In the PPP loan application, the small business (through its authorized representative) must state, among other things, its: (a) average monthly payroll expenses; and (b) number of employees. These figures are used to calculate the amount of money the small business is eligible to receive under the PPP. In

addition, businesses applying for a PPP loan must provide documentation showing their payroll expenses.

16. A PPP loan application must be processed by a participating financial institution (the lender). If a PPP loan application is approved, the participating financial institution funds the PPP loan using its own monies, which are 100% guaranteed by the Small Business Administration ("SBA"). Data from the application, including information about the borrower, the total amount of the loan, and the listed number of employees, is transmitted by the lender to the SBA in the course of processing the loan.

17. PPP loan proceeds must be used by the business on certain permissible expenses: payroll costs, interest on mortgages, rent, and utilities. The PPP allows the interest and principal on the PPP loan to be entirely forgiven if the business spends the loan proceeds on these expense items within a designated period of time and uses a designated percentage of the proceeds on payroll expenses.

18. The PPP is overseen by the SBA, which is headquartered at 409 3rd Street SW, Washington, DC 20416, and has authority over all loans. Individual PPP loans, however, are issued by private approved lenders (most commonly, banks and credit unions), which receive and process PPP applications and supporting documentation, and then make loans using

the lenders' own funds. To date, over 4,900 lending institutions have participated in the PPP.

19. Cross River Bank and Celtic Bank are FDIC-insured, SBA Approved Lenders and have participated as PPP lenders to small businesses.

20. Harvest Small Business Finance LLC ("Harvest") is an SBA Approved Lender and has participated as a PPP lender to small businesses. Harvest is not an FDIC-insured financial institution.

21. BlueVine Capital Inc. ("BlueVine") is an agent that pairs PPP applicants with lenders. BlueVine collects applications and does the underwriting and processing for lenders. BlueVine then submits the loans to the lenders, such as Cross River Bank and Celtic Bank, for funding.

Overview of the Investigation

22. In or around April 2020 and May 2020, at least four individuals—DARRELL THOMAS, ANDRE LEE GAINES, KAHLIL GIBRAN GREEN SR., and BERN BENOIT—applied for, or assisted in submitting an application for, PPP loans on behalf of five businesses – Bellator Phront Group Inc. ("Bellator"), Gaines Reservation and Travel LLC ("Gaines R&T"), Impact Creations LLC ("Impact"), Transportation Management Services Inc. ("Transportation Management"), and Lee

Operations LLC ("Lee Operations"). Each loan was valued at approximately $800,000, and the total amount obtained was approximately $4.1 million. The applications contained false representations and certifications and included substantively identical purported IRS Form 941s reflecting false payroll data for the businesses. Four of the five applications also included a false bank statement for the business. Once the loans were approved, the individuals identified above disbursed the loan funds to entities that do not appear to be employees of their businesses and do not otherwise constitute permissible uses for PPP loan funds.

23. To support the requested loan amount, each applicant supplied BlueVine and/or its respective lender with what were purportedly the business's IRS Form 941s (Employer's Quarterly Federal Tax Return) for January–December 2019. The 941s that the applicants submitted listed the exact same number of employees and amount paid for wages, tips, and other compensation for each quarter of 2019, except that Bellator reported different figures for the third quarter of 2019. Specifically, the 941s that the applicants submitted indicated, among other information, that the businesses had the following number of employees

and amount paid for wages, tips, and other compensation for each of the four quarters in 2019:

Business	Q1 2019 Jan - Mar	Q2 2019 Apr – Jun	Q3 2019 Jul - Sept	Q4 2019 Oct - Dec
Impact	57 employees $815,954.00	59 employees $865,954.00	63 employees $905,132.00	63 employees $905,132.00
Gaines R&T	57 employees $815,954.00	59 employees $865,954.00	63 employees $905,132.00	63 employees $905,132.00
Transportation Management	57 employees $815,954.00	59 employees $865,954.00	63 employees $905,132.00	63 employees $905,132.00
Lee Operations	57 employees $815,954.00	59 employees $865,954.00	63 employees $905,132.00	63 employees $905,132.00
Bellator	57 employees $815,954.00	59 employees $865,954.00	61 employees $895,923.00	63 employees $905,132.00

24. Based on a search of available IRS records related to the employer identification numbers associated with each business, there were no filings of Forms 941 for the first quarter of tax year 2020 or for any of the four quarters of tax year 2019. In addition, there were no records located for the filing of a Form 940 (Employer's Annual Federal Unemployment Tax Return) for tax year 2019.

25. The PPP loan applications for Impact, Gaines R&T, Transportation Management, and Lee Operations also included fraudulent bank statements. Specifically, the loan applications for Impact, Gaines R&T, and Transportation Management included a purported bank statement for their respective bank accounts for the period from February

1, 2020 to February 28, 2020. The bank statements were substantively identical, except for differing business information and account numbers. Each bank statement purports to show that the business's bank account had a beginning balance of $674,776.42 and ending balance of $790,576.16, respectively, during the specified time period. JPMC confirmed that all three February 2020 bank account statements were fake. In fact, Impact opened its account on April 3, 2020 and therefore did not have a statement for February 2020. Transportation Management opened its account on April 21, 2020 and therefore did not have a statement for February 2020. For Gaines R&T's account, JPMC records show that the actual February 2020 beginning and ending balances were both $190.

26. DARRELL THOMAS submitted a purported bank statement from Fifth Third Bank for Lee Operations for the period from February 1, 2020 through February 29, 2020.[1] The bank statement reflects a starting balance of $646,674.16 and an ending balance of $437,207.05, including two payments for $206,114.21 for "Payroll Services." Fifth Third Bank

[1] DARRELL THOMAS does not own Lee Operations. However, based on information developed in the investigation, DARRELL THOMAS used the business and personal information of Lee Operations and its owner to submit a PPP loan application on behalf of Lee Operations. On the same date that Lee Operations' loan was funded, Lee Operations transferred all but $2,000 of the PPP loan amount to a bank account controlled by DARRELL THOMAS.

provided the actual bank statement for Lee Operations' account for the period from February 1, 2020 and February 29, 2020. That bank statement reflects a beginning balance of $50 and an ending balance of $392.92, with no payments for payroll services.

PPP Loan Applications and Use of the SUBJECT EMAIL ADDRESSES

DARRELL THOMAS/Bellator Phront Group Inc.

27. DARRELL THOMAS is a citizen of the United States who claims sole ownership of Bellator Phront Group Inc. ("Bellator"), located at 11285 Elkins Road, Suite H6, Roswell, Georgia 30076. He is listed as the Chief Financial Officer of Bellator according to records obtained from the Georgia Secretary of State.

28. According to records provided by Harvest, on or about April 21, 2020, DARRELL THOMAS digitally signed an application in support of a $799,955.35 PPP loan for Bellator and submitted it to Harvest for funding. The email address that DARRELL THOMAS listed on Bellator's PPP loan application was **DARRELL.THOMAS@BELLATORPHRONTGROUP .COM**. Based on an open source query, the domain bellatorphrontgroup.com and the email address **DARRELL.THOMAS@ BELLATORPHRONTGROUP.COM** are hosted by GoDaddy.

29. After submitting Bellator's PPP loan application, DARRELL THOMAS used the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM** to communicate with Harvest regarding Bellator's PPP loan application and to submit fraudulent documentation associated with Bellator's PPP loan. For example, on April 30, 2020, DARRELL THOMAS, using the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM**, sent an email to Harvest attaching an IRS Form 941 for the first quarter of 2020, and stating: "Thank you! I've attached our most recent 941 the nearest office to file has been closed so I submitted this via fax." As explained above, a search of IRS records revealed that Bellator did not file an IRS Form 941 for the first quarter of 2020. On May 5, 2020, DARRELL THOMAS, using the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM**, sent an email to pppnotes@harvestcref.com attaching a voided check and notarized documents required to receive the PPP loan proceeds.

30. Based on DARRELL THOMAS's untrue statements, Bellator's loan application was approved. On or about May 19, 2020, approximately $799,955.35 in PPP loan funds was distributed to Bellator through a wire transfer to Bank of America account number 334060043940 ("Account

3940"), which is one of Bellator's bank accounts. Between May 22, 2020 and June 15, 2020, approximately $542,200 of proceeds from three other fraudulently obtained loans (discussed further below) were transferred to Account 3940. Bank of America records list DARRELL THOMAS and his wife, Meghan Thomas, as authorized signers for Account 3940.

31. DARRELL THOMAS and Meghan Thomas are also authorized signers for Bank of America bank account number 334060044823 ("Account 4823"), which is held in the business name of Elite Executive Services Inc. ("Elite"). Between May 21, 2020 and June 16, 2020, approximately $1,525,850.15 of proceeds from four other fraudulently obtained loans (discussed further below) were transferred to Account 4823.

BERN BENOIT / Transportation Management Services Inc.

32. BENOIT is a citizen of the United States who claims sole ownership of Transportation Management Services Inc. ("Transportation Management"), located at 2216 Kings Drive, Woodbury, Minnesota 55125. He is listed as the Chief Executive Officer of Transportation Management according to records obtained from the Minnesota Secretary of State.

33. According to records provided by Cross River Bank, on or about May 20, 2020, an application in support of an $830,417 PPP loan for Transportation Management was submitted to BlueVine. The email

address listed for Transportation Management on its PPP loan application is **TRANSPORTMANAGEMENTINC@GMAIL.COM.**

34. Based on documentation provided by BERN BENOIT on behalf of Transportation Management, BERN BENOIT used the email address **BERNBENOIT23@GMAIL.COM** to communicate with others regarding Transportation Management's fraudulent PPP loan application. For example, on May 29, 2020, the email address **CHARLESWILLIAMKNIGHT7@GMAIL.COM** sent an email to CJ Baptiste, using the email address **NETBASEDSTUDIOS@GMAIL.COM**, which CJ Baptiste then forwarded to **BERNBENOIT23@GMAIL.COM**. The subject line of the email was "Expenses for Transportation Management Services" and included an itemized list of purported "expenses" for Transportation Management. Based on text messages and other information provided by BERN BENOIT on behalf of Transportation Management, both CJ Baptiste and a person identified as "Charles," who used the email address **CHARLESWILLIAMKNIGHT7@GMAIL.COM**, were involved in the preparation and submission of Transportation Management's fraudulent PPP loan application. According to records provided by Google, the email address **CHARLESWILLIAMKNIGHT7@**

GMAIL.COM was deleted on July 7, 2020, hours after I called BERN BENOIT to discuss Transportation Management's fraudulent PPP loan.[2]

35. Once BlueVine processed the application, it was submitted to Cross River Bank for funding. Based on the application's untrue statements, Transportation Management's loan was approved. On or about May 18, 2020, approximately $830,417 in PPP loan funds was distributed to Transportation Management's bank account.

ANDRE LEE GAINES/Gaines Reservation and Travel LLC

36. GAINES is a citizen of the United States who claims sole ownership of Gaines Reservation and Travel LLC ("Gaines R&T"), located at 85 Rosemont Court, Hiram, Georgia 30141. He is listed as the registered agent of Gaines R&T according to records obtained from the Georgia Secretary of State.

37. According to records provided by Cross River Bank, on or about May 18, 2020, an application in support of an $806,710 PPP loan for

[2] I sent a preservation request for the **CHARLESWILLIAMKNIGHT7@GMAIL.COM** account on or about July 29, 2020. Google provided information, including email headers, related to the email address **CHARLESWILLIAMKNIGHT7@GMAIL.COM** on or about August 3, 2020. Because Google retained and was able to provide that information after the account was deleted, there is probable cause to believe that Google has retained the information this warrant seeks despite the account deletion.

Gaines R&T was submitted to BlueVine. The email address listed for Gaines R&T on its PPP loan application is **GRESERVETRAVEL@GMAIL.COM**. Based on information provided by Google, on May 18, 2020 – the same day that Gaines R&T submitted its fraudulent PPP loan application – the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM** sent an email to **GRESERVETRAVEL@GMAIL.COM.**

38. Once BlueVine processed the application, it was submitted to Cross River Bank for funding. Based on the application's untrue statements, Gaines R&T's loan was approved. On or about May 18, 2020, approximately $806,710 in PPP loan funds was distributed to Gaines R&T through wire transfer to Gaines R&T's bank account.

KAHLIL GIBRAN GREEN SR./Impact Creations LLC

39. KAHLIL GIBRAN GREEN SR. is a citizen of the United States who claims sole ownership of Impact Creations LLC ("Impact"), located at 600 Superior Avenue East, Fifth Third Center 1300, Cleveland, Ohio 44114. He is listed as the registered agent of Impact according to records obtained from the Ohio Secretary of State.

40. According to records provided by Cross River Bank, on or about May 17, 2020, an application in support of an $830,000 PPP loan for Impact was submitted to BlueVine. Impact's PPP loan application lists

CREATEIMPACT75@GMAIL.COM as the email address for Impact. The application misrepresented critical information, including Impact's average monthly payroll and number of employees. The application was digitally signed in Green's name and certified that the application and the information he provided in all supporting documents and forms was true and accurate.

41. After BlueVine processed the application, it was submitted to Cross River Bank for funding. Based on the application's untrue statements, Impact's loan was approved. On or about May 19, 2020, approximately $830,000 in PPP loan funds was distributed to Impact's bank account.

The Business Email Addresses Associated With Transportation Management, Gaines R&T, and Impact

42. As discussed above, the business email addresses listed on the PPP loan applications for Transportation Management, Gaines R&T, and Impact Creations were **TRANSPORTMANAGEMENTINC@GMAIL.COM, GRESERVETRAVEL@GMAIL.COM,** and **CREATEIMPACT75@GMAIL.COM,** respectively. Based on information provided by Google, there is probable cause to believe that these email addresses were created and used for the sole or primary purpose of carrying out and facilitating the violations being investigated.

43. First, each account was created shortly before the business's PPP loan application was submitted. **TRANSPORTMANAGEMENTINC@GMAIL.COM** was created on May 19, 2020, **GRESERVETRAVEL@GMAIL.COM** was created on May 3, 2020, and **CREATEIMPACT75@GMAIL.COM** was created on April 24, 2020.

44. Second, each account is linked to DARRELL THOMAS. The phone number associated with both **GRESERVETRAVEL@GMAIL.COM** and **CREATEIMPACT75@GMAIL.COM** is +14048205260. Based on public source research, that phone number is registered to DARRELL THOMAS. The recovery phone number associated with **TRANSPORTMANAGEMENTINC@GMAIL.COM** is +17705685744, which based on publicly available information is registered to Meghan Thomas, DARRELL THOMAS's wife. In addition, the email address **GRESERVETRAVEL@GMAIL.COM** is linked by cookies to the email address **DARRELL.THOMAS1986@GMAIL.COM**, which is DARRELL THOMAS's personal email address. Moreover, the email addresses **GRESERVETRAVEL@GMAIL.COM, CREATEIMPACT75@GMAIL.COM,** and **TRANSPORTMANAGEMENTINC@GMAIL.COM** are all linked by

cookies with Meghan Thomas's personal email address, megthom1021@gmail.com.

45. Third, based on email header information provided by Google, each account appears to have been used to communicate with BlueVine, but engaged in few other communications. For example, on or about May 19, 2020, the email address **TRANSPORTMANAGEMENTINC@GMAIL.COM** received an email from noreply@pdffiller.com. According to the website www.pdffiller.com, the website allows users to, among other things, "Edit, annotate and blackout PDFs" and to "Get documents e-signed." The very next email that **TRANSPORTMANAGEMENTINC@GMAIL.COM** received was from service@bluevine.com. Between on or about May 19, 2020 and May 20, 2020, **TRANSPORTMANAGEMENTINC@GMAIL.COM** received approximately six emails from email addresses associated with BlueVine, of a total of only approximately 18 emails sent or received by the email address between May 19, 2020 and July 23, 2020.

46. Similarly, on May 18, 2020, the email address **GRESERVETRAVEL@GMAIL.COM** received several emails from service@bluevine.com and cares@bluevine.com, which are email addresses associated with BlueVine, the company to which Gaines R&T submitted its

PPP loan application. The email address **GRESERVETRAVEL@GMAIL.COM** sent or received only approximately 16 emails between May 3, 2020 and June 24, 2020.

47. Finally, between May 16, 2020 and May 18, 2020, the email address **CREATEIMPACT75@GMAIL.COM** received several emails from service@bluevine.com and cares@bluevine.com. The email address **CREATEIMPACT75@GMAIL.COM** sent or received only approximately 25 emails between April 24, 2020 and June 23, 2020.

Transfers of Fraudulent PPP Loan Proceeds and Use of the SUBJECT EMAIL ADDRESSES

Transfers to DARRELL THOMAS's Companies

48. After receiving their PPP loan proceeds, Impact, Transportation Management, Gaines R&T, and Lee Operations made large payments to DARRELL THOMAS's companies, Bellator and Elite.

49. The total amount deposited into Account 3940 between on or about May 19, 2020 and on or about June 15, 2020 that is traceable to fraudulently obtained PPP loan proceeds is approximately $1,342,155.35. On or about June 5, 2020, approximately $620,000 was transferred from Account 3940 to another Bellator bank account via wire.

50. The total amount traceable to fraudulently obtained PPP loans that was deposited into Account 4823 between May 21, 2020 and June 16,

2020 is approximately $1,525,850.15. On or about June 8, 2020, approximately $100,000 was transferred from Account 4823 to another Bellator bank account.

51. Documents produced by Transportation Management and information provided by Google show that there is probable cause to believe that the email addresses **BERNBENOIT23@GMAIL.COM, NETBASEDSTUDIOS@GMAIL.COM,** and **CHARLESWILLIAMKNIGHT7@GMAIL.COM** were used to facilitate and carry out the money laundering of fraudulent PPP loan proceeds deposited into Transportation Management's account. Specifically, on June 15, 2020, CJ Baptiste, using the email address Jerry@NetbasedStudios.com, sent an email to **BERNBENOIT23@GMAIL.COM** with the subject line "disbursement time." The email said:

> Ok it's disbursement time. Important…remember and remind Bern that he will be getting about 322k out of this deal for free. And everything done is for the purpose of keeping him legal and safe. So…no angst, questioning, 3 way calls or other drama allowed. This is the way it goes, no objection. Let's make this easy and just do what's necessary. The split is 40% Bern and 60% processor/doc people/cpa/taxes etc
>
> 1) We need him to do another cashier check for 100K make it out to warehouse rent same company name (he will get 50k of this back)
>
> 2) Payroll wire to Elite Executive Services Inc

7200 Grandview Overlook
Duluth, Ga 30097
Account: xxxxxxx44823
Routing: xxxxx9593

Total wire amount: $169,998.72

In memo line for wire put payroll business management services

Bern will get a big chunk of this back via wire/payroll cards

There will be a second payroll run in about a week and a 1/2 for 169,998.72

And then a final payroll run two weeks after that for whatever the balance is.

Need this done today. No conference call needed its easy. Thanks.

52. On June 15, 2020, the same day as the email quoted above, Transportation Management wired $169,998.72 to Elite and purchased a $100,000 cashier's check made out to Bellator.

53. Header information provided by Google shows that Bern Benoit, using the email address **BERNBENOIT23@GMAIL.COM,** received an email from CJ Baptiste, using the email address **NETBASEDSTUDIOS@GMAIL.COM** on June 2, 2020, the same day that Transportation Management made a $12,000 online ACH payment to J Anthony Properties, a company affiliated with CJ Baptiste. The header information also shows that the email addresses

BERNBENOIT23@GMAIL.COM and **NETBASEDSTUDIOS@GMAIL.COM** exchanged several emails in May and June 2020, including the email quoted above regarding Transportation Management's purported "expenses." In addition, bank records show that Transportation Management transferred at least $51,000 of the fraudulent PPP loan proceeds to CJ Baptiste or his company, J Anthony Properties, in May and June 2020.

54. Moreover, header information provided by Google shows that CJ Baptiste, using the email address **NETBASEDSTUDIOS@GMAIL.COM**, exchanged many emails with **CHARLESWILLIAMKNIGHT7@GMAIL.COM** in May and June 2020, including exchanging approximately 19 emails on or about June 15, 2020, the same date as the "disbursement time" email discussed above.

Purchases of Luxury Vehicles

55. Bank of America records show that, on or about June 9, 2020, Bellator sent a $137,953.00 wire transfer from Account 3940 to "Jakes Motorcars." Records produced by Jakes Motorcars show that this wire transfer represented payment for DARRELL THOMAS's purchase of a 2018 Mercedes-Benz S-Class S65 AMG ("2018 Mercedes"), which was delivered to DARRELL THOMAS's residence on or about June 18, 2020.

56. Bank of America records show that, on or about June 15, 2020, Bellator sent a $126,441.00 wire transfer from Account 3940 to "CMD, LLC DBA MCLAREN CHARL." Records provided by McLaren Charlotte establish that this wire transfer represented payment for DARRELL THOMAS's purchase of a 2018 Land Rover Range Rover ("2018 Land Rover"), which was delivered to DARRELL THOMAS at his residence or about June 27, 2020. The 2018 Land Rover has since been seized pursuant to a seizure warrant signed by United States Magistrate Judge Alan J. Baverman.

57. Records provided by McLaren Charlotte show that DARRRELL THOMAS used the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM** in connection with his purchase of the 2018 Land Rover. On June 11, 2020, McLaren sales representative Kyle Slawter, using the email address kslawter@charlottemclaren.com, sent an email to DARRELL THOMAS, using the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM**, and said, in part: "Thank you for your interest in my 2018 Land Rover Range Rover SVAUTOBIOGRAPHY. This vehicle is still in my inventory at the moment. How may I assist you?" DARRELL THOMAS, using the email

address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM**, responded that he was "looking to purchase immediately," and later that day stated that "I'll be doing cash no financing needed." On June 15, 2020, Kyle Slawter emailed DARRELL THOMAS, using the email address **DARRELL.THOMAS@BELLATORPHRONTGROUP.COM**, to confirm that McLaren had received the wire payment and that the vehicle would be detailed before being transported.

58. The records provided by McLaren also show that DARRELL THOMAS used the email address **DARRELL.THOMAS1986@GMAIL.COM** to carry out and facilitate his money laundering. On June 11, 2020, Kyle Slawter, using the email address kslawter@charlottemclaren.com, asked DARRELL THOMAS if he had a "Gmail account." The same day, DARRELL THOMAS responded that his email address is **DARRELL.THOMAS1986@GMAIL.COM**. Based on header information provided by Google, on June 11, 2020, DARRELL THOMAS, using the email address **DARRELL.THOMAS1986@GMAIL.COM**, received an email from kslawter@gmail.com, which appears to be a Google email address used by Kyle Slawter.

BACKGROUND CONCERNING EMAIL

59. In my training and experience, I have learned that Google and GoDaddy provide a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name www.gmail.com, like the email accounts listed in Attachment A. GoDaddy allows subscribers to obtain email accounts using custom domain names created by the subscriber. Subscribers obtain an account by registering with Google and GoDaddy. During the registration process, Google and GoDaddy ask subscribers to provide basic personal information. Therefore, the computers of Google and GoDaddy are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail and GoDaddy subscribers) and information concerning subscribers and their use of Gmail and GoDaddy services, such as account access information, email transaction information, and account application information. 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.

60. A Gmail and GoDaddy subscriber can also store with the provider files in addition to emails, such as address books, contact or

buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google and GoDaddy. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

61. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). 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. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

62. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. 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. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular 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 computers or other devices were used to access the email account.

63. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as 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.

64. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email 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, email 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 the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of

the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. 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 email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner'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).

65. Based on my training and experience, user attribution evidence can be found anywhere within the records associated with an email account, including within records that were generated years prior to criminal activity. Because this investigation involves a group of criminals who are believed to be controlling the accounts sought in the warrant, it is necessary to request records starting from March 31, 2020, when the PPP loan program was announced, to the present.

66. Moreover, the stored communications and files connected to the target accounts may provide direct evidence of the offenses under investigation.

67. Google also maintains records for online (internet/web) and application activity associated with a particular Google account, such as the search history associated with the accounts listed in Attachment A. Google retains a user's search history whether the search is executed from a mobile device or from a traditional computer. This history includes the searched-for terms, the date and time of the search, and the user-selected results. Furthermore, Google retains records about the specific type of search a user performed, including general web searches and specialty searches where the results are focused in a particular group such as images, news, videos, and shopping. Based on my training and experience, I believe that a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it.

68. According to representatives from Google and GoDaddy, the companies keep records that can reveal other accounts accessed from the same electronic device (i.e. computer or mobile phone) as a known account, including accounts linked by "cookies," which are small pieces of

text sent to the user's Internet browser when visiting websites. Therefore, Google and GoDaddy can identify any other accounts accessed by the same device(s) that accessed the account(s) described in Attachment A, including accounts linked by cookies, creation IP address, recovery email address, or telephone number.

69. Therefore, Google's and GoDaddy's servers are likely to contain stored electronic communications and other information concerning subscribers and their use of email services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

70. Based on my training, experience, and knowledge of law enforcement guidelines for Google and GoDaddy, I know that these email providers can conduct searches based on objective criteria like date ranges, but they are unfamiliar with this investigation and cannot filter content for subjective criteria based on the subject matter of communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

71. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google

and GoDaddy to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly 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.

CONCLUSION

72. As explained in this Affidavit, there is probable cause to believe that DARRELL THOMAS and his co-conspirators used the **SUBJECT EMAIL ADDRESSES** to carry out and facilitate the offenses being investigated.

73. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email accounts **DARRELL.THOMAS1986@GMAIL.COM, GRESERVETRAVEL@GMAIL.COM, BERNBENOIT23@GMAIL.COM, TRANSPORTMANAGEMENTINC@GMAIL.COM, NETBASEDSTUDIOS@GMAIL.COM, CHARLESWILLIAMKNIGHT7@GMAIL.COM,** and **CREATEIMPACT75@GMAIL.COM,** that is stored at premises owned, maintained, controlled, or operated by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period March 31, 2020 through the present**:

a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the account, draft emails, 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;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on

which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. A list of the types of Google service utilized by each account in Attachment A and any dates associated with the commencement or termination of that use;

g. All records pertaining to devices from which the account accessed any Google service or to which any Google service is synced, to include device serial numbers, model type/number, IMEI, phone numbers, and MAC Addresses; and

h. All search history and internet browsing history associated with each account in Attachment A;

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1343, 1344, 1349, 1014, 1956, and/or 1957 involving the target and/or any associates or accomplices, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the email account(s), including records that help reveal the whereabouts of such person(s) and their employer;

b. Evidence relating to the Paycheck Protection Program, including any Paycheck Protection Program loan submitted by any business, any communications with individuals or entities regarding Paycheck Protection Program loan applications, and any documentation or information submitted in connection with any Paycheck Protection Program loan;

c. Evidence relating to any fraudulent loan application;

d. Evidence relating to the incorporation, ownership, or control of Bellator Phront Group Inc., Elite Executive Services Inc., Gaines Reservation and Travel LLC, Impact Creations LLC, Lee Operations LLC, Transportation Management Services Inc., Management Resource Services Inc., and 365 Enterprise LLC;

e. Evidence relating to the use or expenditure of proceeds from any Paycheck Protection Program loan;

f. Evidence indicating the user agent strings used to access the services;

g. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

h. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

i. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

j. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

(Rev. 4/30/2014) Search Warrant

United States District Court

Northern District of Georgia

In the Matter of the Search of:

Information associated with the email addresses DARRELL.THOMAS1986@GMAIL.COM; GRESERVETRAVEL@GMAIL.COM; BERNBENOIT23@GMAIL.COM; TRANSPORTMANAGEMENTINC@GMAIL.COM; NETBASEDSTUDIOS@GMAIL.COM; CHARLESWILLIAMKNIGHT7@GMAIL.COM; and CREATEIMPACT75@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

SEARCH WARRANT

CASE NUMBER: 1:20-mc-1472

TO: FBI Special Agent Joseph D. Stites and any Authorized Officer of the United States:

An affidavit having been made before me by Special Agent Joseph D. Stites, who has reason to believe that, on the property or premises known as

Information associated with the email addresses DARRELL.THOMAS1986@GMAIL.COM; GRESERVETRAVEL@GMAIL.COM; BERNBENOIT23@GMAIL.COM; TRANSPORTMANAGEMENTINC@GMAIL.COM; NETBASEDSTUDIOS@GMAIL.COM; CHARLESWILLIAMKNIGHT7@GMAIL.COM; and CREATEIMPACT75@GMAIL.COM, as further described in Attachment A.

There is now concealed certain property, certain data, and certain information, namely,

See Attachment B

which constitutes evidence of the commission of a criminal offense and property which has been used as the means of committing a criminal offense, concerning violations of Title 18, United States Code, Sections 1343, 1344, 1349, 1014, 1956, and/or 1957, over which the United States District Court for the Northern District of Georgia has jurisdiction. I find that the affidavit establishes probable cause to search and seize the person or property from the person or premises described above.

YOU ARE HEREBY COMMANDED to execute this warrant on or before Sept. 1, 2020
Date

(not to exceed 14 days) AT ANY TIME IN THE DAY OR NIGHT AS I FIND GOOD CAUSE HAS BEEN ESTABLISHED. 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 a copy of the warrant and receipt at the place where the property was taken. The officer executing the 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 United States Magistrate Judge Justin S. Anand.

August 18, 2020 at 2:30 pm
Date and Time

at Atlanta, Georgia
City and State

JUSTIN S. ANAND
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

AUSA Tal C. Chaiken /404-581-6069

Issued pursuant to Federal Rule of Criminal Procedure 4.1

RETURN

Case No: 1:20-mc-1472	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of		
A list of property/information/data/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 associated with the email accounts **DARRELL.THOMAS1986@GMAIL.COM, GRESERVETRAVEL@GMAIL.COM, BERNBENOIT23@GMAIL.COM, TRANSPORTMANAGEMENTINC@GMAIL.COM, NETBASEDSTUDIOS@GMAIL.COM, CHARLESWILLIAMKNIGHT7@GMAIL.COM,** and **CREATEIMPACT75@GMAIL.COM,** that is stored at premises owned, maintained, controlled, or operated by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("the Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period March 31, 2020 through the present**:

a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the account, draft emails, 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;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on

which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. A list of the types of Google service utilized by each account in Attachment A and any dates associated with the commencement or termination of that use;

g. All records pertaining to devices from which the account accessed any Google service or to which any Google service is synced, to include device serial numbers, model type/number, IMEI, phone numbers, and MAC Addresses; and

h. All search history and internet browsing history associated with each account in Attachment A;

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §§ 1343, 1344, 1349, 1014, 1956, and/or 1957 involving the target and/or any associates or accomplices, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the email account(s), including records that help reveal the whereabouts of such person(s) and their employer;

b. Evidence relating to the Paycheck Protection Program, including any Paycheck Protection Program loan submitted by any business, any communications with individuals or entities regarding Paycheck Protection Program loan applications, and any documentation or information submitted in connection with any Paycheck Protection Program loan;

c. Evidence relating to any fraudulent loan application;

d. Evidence relating to the incorporation, ownership, or control of Bellator Phront Group Inc., Elite Executive Services Inc., Gaines Reservation and Travel LLC, Impact Creations LLC, Lee Operations LLC, Transportation Management Services Inc., Management Resource Services Inc., and 365 Enterprise LLC;

e. Evidence relating to the use or expenditure of proceeds from any Paycheck Protection Program loan;

f. Evidence indicating the user agent strings used to access the services;

g. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

h. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

i. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

j. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature