# 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)*

SEARCH OF [redacted] WASHINGTON, DC UNDER RULE 41

Case No. 20-sw-187

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEARCH OF [redacted] WASHINGTON, DC UNDER RULE 41) (as further described in Attachment A)

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

evidence of violations of 18 U.S.C. §§ 641 (Theft of Government Property), 1343 (Wire Fraud), 1344 (Bank Fraud) and 1956 (Money Laundering) (as further described in Attachment B)

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* |
|---|---|
| 18 U.S.C. § 641 | Theft of Government Property |
| **§ 1343** | Wire Fraud |
| **§ 1344** | Bank Fraud |
| **§ 1956** | Money Laundering |

The application is based on these facts:

Please see attached Affidavit

- ☑ 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.

DRzepecki

*Applicant's signature*

Daniel Rzepecki, Special Agent, FBI

*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 08/10/2020

2020.08.10 18:44:32 -04'00'

*Judge's signature*

City and state: Washington, D.C.

G. Michael Harvey, U.S. Magistrate Judge

*Printed name and title*

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

# UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
SEARCH OF [redacted] WASHINGTON, DC
UNDER RULE 41

Case No. 20-sw-187

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

Search of [redacted] Washington, DC for investigation of violations of 18 U.S.C. §§ 641 (Theft of Government Property), 1341 (Wire Fraud), 1344 (Bank Fraud) and 1956 (Money Laundering) (as further described in the attached affidavit in support of search warrant, incorporated fully herein, including Attachment A)

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)*:

Evidence, fruits, and instrumentalities evidence of violations of 18 U.S.C. §§ 641 (Theft of Government Property), 1341 (Wire Fraud), 1344 (Bank Fraud) and 1956 (Money Laundering) (as further described in the attached affidavit in support of search warrant, incorporated fully herein, including Attachment B)

**YOU ARE COMMANDED** to execute this warrant on or before August 24, 2020 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Honorable G. Michael Harvey .
*(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: 08/10/2020 2020.08.10 18:45:20 -04'00'
*Judge's signature*

City and state: Washington, DC G. Michael Harvey, U.S. Magistrate Judge
*Printed name and title*

## Return

| Case No.: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|
| 20-sw-187 | | |

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

## Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

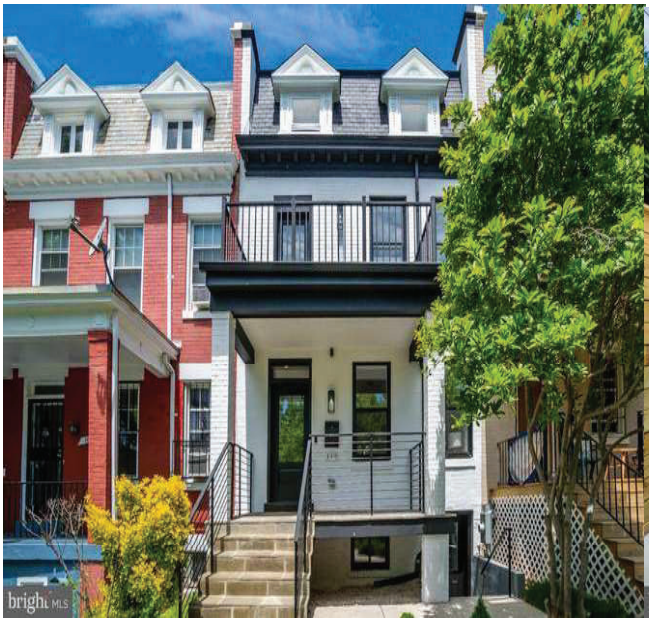
_____
*Executing officer's signature*

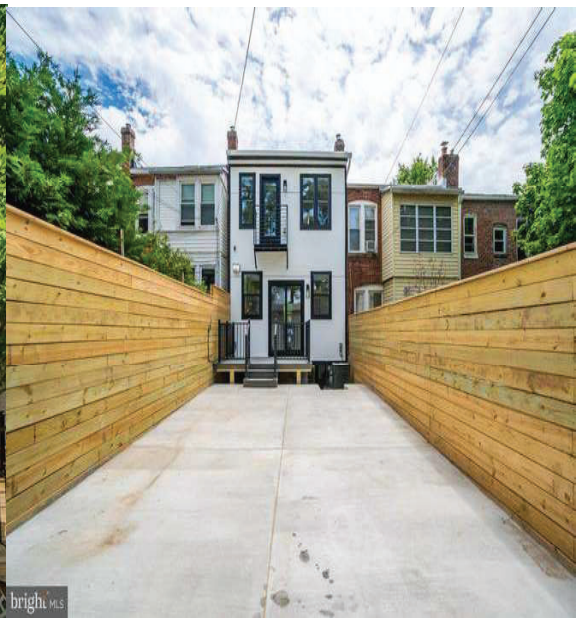
_____
*Printed name and title*

**ATTACHMENT A**

*Property to be searched*

The property to be searched is [redacted] Washington, DC, [redacted], including the English basement and curtilage (the "PREMISES"), further described as a light gray brick multi-story row home. Images of the front and back of the property, respectively, are below:





**ATTACHMENT B**

*Property to be seized*

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. §§ 1344 (bank fraud), 641 (theft of government money or property), 1343 (wire fraud), and 1956 (money laundering), as described in the search warrant affidavit, including, but not limited to:

a. Any and all records and correspondence related to Kenneth Patrick Gaughan, [redacted]Person 1, Richard Strauski, Serving Animals of America Incorporated, Service Dog of America Incorporated, Certapet Incorporated, Official Service Dogs Incorporated, Therapetic Solutions Incorporated, Therapy Dog Incorporated, Therapy Dog International Incorporated, ESA Registry International Incorporated, Service Dog Directory, US Service Dog Registry, ESA Registry, ESA Directory, Therapy Pet Dog;

b. Any and all records related to the use of United Parcel Service ("UPS") and GoDaddy LLC in connection with the entities or persons described in Paragraph (a);

c. Any and all records related to seeking funds from Small Business Administration ("SBA"), CARES Act, Payment Protection Program ("PPP"), the Economic Injury Disaster Loan ("EIDL") program, Fund-Ex Solutions Group LLC, Celtic Bank Corporation, Radius Bank, First Bank of the Lake, Northeast Bank, Bank of America, PNC Bank, and Kabbage Incorporated;

d. Any and all records related to the registration, maintenance, termination, or use of websites or email addresses for the entities or persons described in Paragraph (a), including IP addresses used to access any such email addresses;

e. Any and all financial records—including but not limited to bank statements, checks, loan records, credit card records, ledgers, check registers, credit cards, lines of credit, deposit records, wire transfer detail, money transfer records, faxes, memoranda, correspondence, and applications—for the entities or persons described in Paragraph (a);

f. Any and all documents relating to financial transactions for the entities or persons described in Paragraph (a);

g. Any and all business records for the entities listed in Paragraph (a);

h. Personnel listings, employee files, or other documents of any kind that identify the name, address, telephone number and social security numbers of any current or former employees and independent contractors who performed any work for the entities listed in Paragraph (a);

i. Any and all tax documents, including forms W-2, W-4, W-9, 1040, 1120, and 1099, for the entities or persons described in Paragraph (a);

j. Any and all documents detailing or summarizing annual, quarterly, monthly, weekly, or daily financial performance pertaining to the entities listed in Paragraph (a);

k. Any and all passwords, instructions, and manuals for software programs used in the computer for maintaining billing records and invoices, appointment

information, and any other client information related to the entities described in Paragraph (a);

l. Cash, checks, prepaid cards, debit cards, money orders, and other financial cards and instruments;

m. Any locked or closed containers capable of containing any of the above-listed evidence;

n. Any and all records that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1344 (bank fraud), 641 (theft of government money or property), 1343 (wire fraud), and/or 1956 (money laundering), or the use of the proceeds derived from the violations of these statutes, as described elsewhere in the affidavit;

o. Records and information relating to any of the following e-mail accounts:

i. serviceanimalsofamerica@gmail.com;

ii. [redacted]@gmail.com;

iii. [redacted]@gmail.com;

iv. certapet@gmail.com;

v. madams6119@gmail.com;

vi. certifytherapydog@gmail.com;

vii. esaregistryinternational@gmail.com;

viii. richard.s.vost@gmail.com;

ix. kengaughan@gmail.com;

x. intlserviceanimal@gmail.com; and

xi. rstrauski@gmail.com;

p. Records and information relating to the identity or location of perpetrators and any aiders and abettors, coconspirators, and/or accessories after the fact;

q. Records and information that constitute evidence of use, control, ownership, or occupancy of the PREMISES and things therein;

r. Records and information that constitute evidence of the state of mind of Kenneth Patrick Gaughan, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

s. Records and information that constitute 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 Kenneth Patrick Gaughan about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Digital devices used in the commission of, or to facilitate, the above described offenses, including preparing and submitting applications for the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) programs.

3. For any digital device that is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":

a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry

entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

e. evidence of the times the Device(s) was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

h. records of or information about Internet Protocol addresses used by the Device(s);

i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. Routers, modems, and network equipment used to connect computers to the Internet.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from Kenneth Patrick Gaughan (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the Device(s) found at the PREMISES,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offenses as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)' security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric

characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital devices" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters,

monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); security devices; and any other type of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions.

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | |
|---|---|
| **IN THE MATTER OF THE SEARCH OF [redacted] WASHINGTON, DC UNDER RULE 41** | **SW No. 20-SW-187** |

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Daniel Rzepecki, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [redacted] Washington, DC, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been in this position since October 2008. I am currently assigned to the Baltimore Field Office where I conduct complex financial crime investigations. I have duties that include investigations of, among other things, bank fraud, mail fraud, wire fraud, health care fraud, and money laundering. Through my twenty-one (21) weeks of training at the FBI Academy and my participation in searches and arrests conducted by my squad and other squads, I have assisted and/or participated in the preparation and/or execution of multiple search and arrest warrants. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. 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.

4. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1344 (bank fraud), 641 (theft of government money or property), 1343 (wire fraud), and 1956 (money laundering) have been committed by **Kenneth Patrick Gaughan**, who also goes by the alias **"Richard Strauski"** (hereinafter **"Gaughan"**). There is also probable cause to search the PREMISES, further described in Attachment A, for the things described in Attachment B.

## PAYCHECK PROTECTION PROGRAM

5. As discussed in this affidavit, **Gaughan** is actively defrauding the federal Payment Protection Program, which this section briefly describes.

6. 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 Paycheck Protection Program ("PPP"). In April 2020, Congress authorized over $300 billion in additional PPP funding.[1]

[1] All dates and amounts are approximations. The words "on or about" and "approximately" are omitted for clarity.

7. In order to obtain a PPP loan, a qualifying business must submit a PPP loan application, which is 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 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 average monthly payroll expenses and number of employees. These figures are used to calculate the amount of money the small business is eligible to receive under the program. In addition, businesses applying for a PPP loan must provide documentation showing their payroll expenses.

8. A PPP loan application must be processed by a participating lender. If a PPP loan application is approved, the participating lender funds the PPP loan using its own money, which is 100 percent guaranteed by 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.

9. The small business must use the PPP loan proceeds on certain permissible expenses, specifically, payroll costs, interest on mortgages, rent, and utilities. The program allows the interest and principal on the PPP loan to be entirely forgiven if the business spends the loan proceeds on the allowable expenses within a designated period of time after receiving the proceeds and uses a certain amount of the PPP loan proceeds on payroll expenses.

## ECONOMIC INJURY DISASTER LOANS

10. As discussed in this affidavit, **Gaughan** is actively defrauding the federal Economic Injury Disaster Loan ("EIDL") program, which this section briefly describes.

11. In response to the COVID-19 pandemic, small business owners and non-profit organizations in all U.S. states, Washington DC, and territories are able to apply for an EIDL. EIDL is an existing SBA program designed to provide economic relief to businesses that are currently experiencing a temporary loss of revenue. EIDL provides loan assistance, including up to $10,000 advances, for small businesses and other eligible entities for loans up to $2 million. The EIDL proceeds can be used to pay fixed debts, payroll, accounts payable and other bills that could have been paid had the disaster not occurred; however, such loan proceeds are not intended to replace lost sales or profits or for expansion of a business. Unlike certain other types of SBA-guaranteed loans, EIDL funds are issued directly from the United States Treasury and applicants apply through the SBA via an online portal and application. The EIDL application process, which also uses certain outside contractors for system support, collects information concerning the business and the business owner, including: information as to the gross revenues for the business prior to January 31, 2020; the cost of goods sold; and information as to any criminal history of the business owner. Applicants electronically certify that the information provided is accurate and are warned that any false statement or misrepresentation to SBA or any misapplication of loan proceeds may result in sanctions, including criminal penalties.

**PROBABLE CAUSE**

12. For more than seven years, **Kenneth Patrick Gaughan** ("**Gaughan**"), a long-time employee of the Catholic Archdiocese of Washington, DC ("ADW" or "the archdiocese"), fraudulently diverted money from ADW to contractors **Gaughan** surreptitiously owned and that provided virtually no legitimate services to ADW. In late 2018, a federal grand jury in the District of Maryland charged **Gaughan** with mail fraud. In December 2019, that indictment was

dismissed for lack of venue. However, in July 2020, based on the fraud **Gaughan** executed against ADW, a grand jury in the District of Columbia indicted **Gaughan** with mail fraud, wire fraud, and money laundering.

13. During the investigation of the fraud that **Gaughan** committed against ADW, your affiant identified **Person 1** as **Gaughan**'s cohabitant in **Gaughan**'s former residence and as the joint account holder on several of **Gaughan**'s bank accounts and credit cards. That is, your affiant learned that **Person 1** resided with **Gaughan** at **Gaughan**'s U Street residence in the [redacted] neighborhood. In May 2018, your affiant obtained a copy of a [redacted] article about **Person 1** stating that **Person 1** "owns a house in [redacted] with his friend **Ken Gaughan**." Further, bank records for bank and credit card accounts on which **Gaughan** and **Person 1** were joint accountholders show that **Gaughan** and **Person 1** were joint accountholders for BB&T accounts ending in 7875, 0952, and 2616. In addition, **Gaughan** and **Person 1** were cardholders and authorized users on a US Bank credit card ending in 4376, which was opened in January 2013, and Barclays Bank credit cards ending in 2023 and 2024, opened in November 2013.[2]

14. On July 17, 2020, your affiant discovered that **Gaughan** was attempting to commit fraud on the EIDL and PPP programs. Specifically, your affiant was informed that **Gaughan** and **Person 1** fraudulently applied for 11 PPP loans to SBA lenders. Records show that **Gaughan** and **Person 1** submitted those PPP loan applications using the business names of

---

[2] According to law enforcement databases, **Person 1** currently resides at an address different from the U Street address and [redacted] Washington, DC. Thus, your affiant believes that **Gaughan** and **Person 1** no longer reside together.

at least eight bogus emotional support animal companies, including Service Animals of America Incorporated, Service Dog of America Incorporated, Certapet Incorporated, Official Service Dogs Incorporated, Therapetic Solutions Incorporated, Therapy Dog Incorporated, Therapy Dog International Incorporated, and ESA Registry International Incorporated.[3]

15. Further, according to the PPP loan applications, **Gaughan** and **Person 1**'s purported service animal companies each have twenty-five (25) employees and are located at a single private mailbox in the UPS Store at 1030 15th Street, NW, Suite 170-B1, Washington, DC ("the 15th Street UPS box").

16. Records from UPS show that **Gaughan** applied for and rents the 15th Street UPS box. The evidence detailed in this affidavit otherwise shows that **Gaughan** made extensive use of the 15th Street UPS box when defrauding ADW.

17. **Gaughan** also fraudulently applied for 12 EIDLs. Records show that **Gaughan** applied for these loans utilizing nine of the above-mentioned suspected bogus service animal-related businesses. The twelve (12) businesses used to submit EIDL applications are Therapetic Solutions Incorporated, Anything Pawsable Incorporated, Therapy Pet Inc, Therapy Dog International, ESA Registry International, Official Service Dogs, Service Dog of America, Certapet Incorporated, Service Animals of America, International Service Animals, Therapy Dog Inc, and US Therapy Dog.

---

[3] **Person 1** also submitted a loan application under the business name [redacted] a food science and nutrition consulting firm. According to **Person 1**'s biography posted on the website of [redacted] where **Person 1** is an [redacted] **Person 1** is the [redacted] of [redacted]

18. **Gaughan's** name and Social Security Number is the business listed contact for all 12 of the EIDL applications. The business addresses provided are variations of the 15th Street UPS box provided for PPP applications. All applications shared a common business phone number of [redacted]-4390, mobile phone contact number of [redacted] 2357, and contact address of [redacted] NE, Washington, DC, 20002.

19. Nine of the 12 entities used to apply for EIDLs shared the same Taxpayer Identification Number (TIN) and business name as entities used to apply for PPP loans. The number of employees per each respective application contradicted each other. The PPP loan applications claimed these entities each had twenty-five (25) employees while the EIDL application stated three (3) employees per entity. Additionally, see below for a summary of the applicant for PPP loans and EIDLs between the like entities:

| PPP | | | EIDL | | |
|---|---|---|---|---|---|
| **Borrower TIN** | **Borrower** | **Applicant** | **Borrower TIN** | **Borrower** | **Applicant** |
| [redacted]3968 | THERAPETIC SOLUTIONS | [redacted] | [redacted]968 | Therapetic Solutions Inc | Kenneth Gaughan |
| [redacted]2437 | Service Animals of America | Kenneth Gaughan | [redacted]437 | Service Animals of America | Kenneth Gaughan |
| [redacted]1136 | ESA Registry International | ESA Registry International | [redacted]136 | ESA Registry International | Kenneth Gaughan |
| [redacted]1218 | Certapet Inc | Kenneth Gaughan | [redacted]218 | Certapet Inc | Kenneth Gaughan |
| [redacted]1090 | Therapy Dog Inc | [redacted] | [redacted]090 | Therapy Dog Inc | Kenneth Gaughan |
| [redacted]0847 | THERAPY DOG INTERNATIONAL | [redacted] | [redacted]847 | Therapy Dog International | Kenneth Gaughan |
| [redacted]2288 | Service Dog of America | Kenneth Gaughan | [redacted]288 | Service Dog of America | Kenneth Gaughan |
| [redacted]1364 | Therapy Pet Inc | [redacted] | [redacted]364 | Therapy Pet Inc | Kenneth Gaughan |
| [redacted]7450 | Official Service Dogs | [redacted] | [redacted]450 | Official Service Dogs | Kenneth Gaughan |

20. **Gaughan** provided Bank of America account number [redacted]9804 for the proceeds for nine (9) of twelve (12) EIDLs. He provided the same account for proceeds of at least one PPP loan, for Service Animals of America. **Gaughan** provided Bank of America account number [redacted]6270 for proceeds on two (2) EIDLs, the same account provided for proceeds of at least one (1) PPP loan for Certapet Incorporated.

## *I. SCHEME TO DEFRAUD ARCHDIOCESE OF WASHINGTON*

21. The scheme to defraud ADW is described in detail in the above-referenced indictment, filed as D.D.C. Case No. 20-cr-128, incorporated herein by reference. For ease of reference, the scheme is also summarized here. ADW is a religious organization that covers the District of Columbia and parts of Maryland. ADW operates schools and provides counseling, shelter, adoption and foster care, health care, immigration and legal aid, and affordable housing to its parishioners.

22. In 2008, ADW hired **Gaughan** as its Director of Counseling, and in July 2013 made **Gaughan** the archdiocese's Assistant Superintendent, a position **Gaughan** held until he formally resigned in April 2018. In those capacities, **Gaughan** was responsible for recruiting and acting as the point of contact for ADW's contractors, particularly those that instituted anti-bullying and crisis intervention programs for the archdiocese.

23. As alleged in the indictment and found in the earlier investigation, **Gaughan** devised and executed a scheme to defraud ADW by, among other things, causing ADW to make payments to purported companies that were actually payments to **Gaughan**. For example, **Gaughan** caused ADW to issue a check to Company 2, which was deposited into an account controlled by **Gaughan**. **Gaughan** also caused ADW to pay two other illegitimate companies, Company 1 and Soulutions Counseling for Youth ("SCY"), more than $450,000 from ADW bank accounts, and **Gaughan** falsely represented to ADW officials that Co.1 and SCY implemented social programs for the benefit of ADW. **Gaughan** then used that money on personal expenditures and to extricate himself from personal debt. The following sections describe **Gaughan**'s fraud on ADW in greater detail.

24. Company 2. In 2018, in connection with the Co.2 entity, **Gaughan** used the alias **Richard Strauski** ("**Strauski**") to open a virtual mailbox through which **Gaughan** defrauded and/or attempted to defraud ADW. The application for this mailbox listed the applicant's home address as the 15th Street UPS box, and, in connection with this application, **Gaughan** also provided a bogus residential lease agreement purportedly showing **Strauski**'s rental of this address. On March 15, 2018, **Gaughan** submitted a fraudulent Co.2 invoice for $21,060 to ADW's Finance Office with a request for payment, *i.e.*, a recommendation that ADW pay Co.2 ADW issued a check to Co.2 which was mailed to the virtual mailbox, to pay for the fraudulent invoice. The invoice requested payment from ADW to Co.2 to provide a school messaging service for the 2018 calendar year – a service which ADW was already receiving from a legitimate entity. On April 17, 2018, **Gaughan** deposited the $21,060 Co.2 check into a bank account he controlled. ADW would not have issued the check had ADW realized that **Gaughan** was the beneficiary of that payment.

25. This earlier investigation also showed how **Gaughan**'s use of digital devices to perpetrate the fraud led to evidence of his offenses being stored on digital devices at his workplace and home. For example, a PDF of a lease agreement used in connection with the Co.2 scheme was also found on **Gaughan**'s ADW computer. An edited version of the lease agreement was also later found on **Gaughan**'s personal MacBook. Similarly, a search of the ADW computer assigned to **Gaughan** revealed various forgeries connected to his fraud scheme, including an image of a District of Columbia driver's license that displayed **Gaughan**'s photograph and the name **Richard Strauski** (*i.e.*, **Gaughan**'s real license with the name altered), a forged certificate from the Nebraska Secretary of State purporting that **Gaughan** does business

as [redacted] and a copy of the fraudulent Co.2 invoice **Gaughan** submitted to ADW's Finance Office in Microsoft Word format.

26. Company 1. In June 2011, by falsely representing information about Co.1 including its purported but non-existent previous work with other dioceses and archdioceses, **Gaughan** persuaded ADW to contract with Co.1 to implement web-based anti-bullying modules that were purportedly required under Maryland law. The original contract, which was effective from June 20, 2011 through June 30, 2014, was for $136,701. On **Gaughan**'s recommendation, in June 2011, ADW issued Co.1 a check for $136,701, which **Gaughan** deposited into a Co.1 account he controlled. Thereafter, in 2014 and 2015, **Gaughan** submitted for approval Co.1 invoices for other large payments, which ADW issued and **Gaughan** deposited into the Co.1 account **Gaughan** controlled. The real Co.1 (in the United Kingdom) has no association with **Gaughan** and does no work in the United States.

27. ***Soulutions Counseling for Youth ("SCY").*** In late 2010, by falsely representing information about SCY, including by using **Strauski**'s identity and concealing **Gaughan**'s own involvement, **Gaughan** persuaded ADW to pay SCY for anti-bullying and crisis intervention programs. Bank records show that those payments were deposited into a bank account **Gaughan** opened in the SCY business name and over which **Gaughan** was the sole signer.

28. ADW records show that between May 2010 and April 2018, the archdiocese issued twenty-six (26) checks to Co.2 Co.1 and SCY. The aggregate value of those checks was $472,832. Financial records show that **Gaughan** deposited the twenty-six (26) ADW checks into accounts **Gaughan** controlled as the sole signer, that the company bank accounts were almost entirely funded by ADW's money, and that **Gaughan** used ADW's money for his

personal benefit and not to operate legitimate businesses.[4] For example, financial records show that **Gaughan** spent over $185,000 in fraudulent proceeds from the Co.1 and SCY accounts to pay for debt incurred on fourteen (14) personal credit cards. **Gaughan** also spent the money credited to the company bank accounts on gambling, entertainment, the mortgage on his home, and a boat.

29. Bank records reflect no paychecks issued from the company accounts to any employees or contractors. Records from the IRS also show that neither Co.2 Co.1 nor SCY ever issued Forms W-2 or 1099 to any employees or contractors, and records from the State of Oregon – the state in which **Gaughan** registered Co.1 – show that there were no wage payments to anyone who worked for Co.1 Thus, along with other third-party records, the financial records show that Co.2 Co.1 and SCY were shell companies **Gaughan** used to illegally enrich himself at the expense of ADW, and were not legitimate businesses. Each of the shell companies **Gaughan** used to defraud ADW (*i.e.*, Co.2 Co.1 and SCY) were associated with the 15th Street UPS box. [5]

---

[4] From your affiant's review of the financial records, the only significant payment made for the benefit of ADW was a $10,000 payment to a company called Connect With Kids ("CWK") for an anti-bullying website. **Gaughan** made this payment from the Co.1 bank account. **Gaughan** then converted the $10,000 contract he signed with CWK into the original $136,701 contract Co.1 entered into with ADW, netting himself a 1,200 percent return on investment at ADW's expense.

[5] The address listed on the application for an account with PNC for Co.1 is a UPS box that was located at 1718 M Street NW, Suite 170, Washington, DC ("the M Street address"). Records from UPS show that "**Kenneth Gaughan**" of "Soulutions Counseling for Youth" opened the private mailbox on May 20, 2010. According to the UPS Store manager, the UPS Store at the M Street address later moved to 1030 15th Street NW, Washington, DC, and **Gaughan**'s private mailbox was converted into the 15th Street UPS box. According to the manager of that particular UPS Store, once the store moved to 1030 15th Street NW, Washington, DC, mail that

30. ***Search Warrant on Gaughan's U Street Residence.*** On September 25, 2018, your affiant and other agents executed a federal search warrant on **Gaughan**'s U Street residence. While executing the warrant, agents encountered **Gaughan** and [redacted]. Agents interviewed **Gaughan**, who waived his *Miranda* rights and made a number of incriminating statements, including (1) that his (**Gaughan**'s) photograph was depicted on the fraudulent **Strauski** driver's license image found on the ADW computer that had previously been assigned to **Gaughan**, (2) that **Strauski** was fictitious, (3) that **Gaughan** thought the evidence of his guilt was overwhelming, (4) that **Gaughan** was in significant personal debt, and (5) that **Gaughan** was sorry for what he did to ADW.

31. Further, in **Gaughan**'s residence, agents found evidence of his financial fraud scheme, including paper receipts for Co.1 and SCY checks deposited into the fraudulent company bank accounts, statements for those bank accounts, a Form 1099 reflecting the fraudulent payments from ADW to SCY in 2010, and the Co.1 State of Oregon registration form.

32. Agents found two MacBook computers that contained inculpatory evidence, including a .png file of **Strauski**'s signature, emails showing **Gaughan**'s control of the mail boxes used for the fraudulent corporate entities, and a fraudulent Co.2 lease agreement. Agents also found several checks from Therapetic, an entity later used in the loan fraud scheme described below.

---

was sent to the M Street address was forwarded to **Gaughan**'s 15th Street UPS box. In other words, the 15th Street UPS box was effectively the address listed on the Co.1 bank account.

## *II. FRAUD ON THE SBA'S PAYCHECK PROTECTION PROGRAM (PPP)*

33. As described above, in July 2020, your affiant learned that **Gaughan** and **Person 1** submitted eleven (11) loan applications for businesses listing the address as the 15th Street UPS box. Your affiant knows that it is indicative of fraud when multiple businesses are located at a single address, particularly when that address is a private mailbox, and where numerous loan applications were submitted for different companies containing the same or similar information, including the same address and number of employees, and similar average monthly payroll amounts. Furthermore, your affiant knows that those who utilize private mailboxes often use those private boxes to receive mail, but then store that mail in their homes.

34. Even though all of the businesses were purportedly located at the same private UPS mailbox, the loan applications listed each business as having twenty-five (25) employees (for a total of at least 200 employees) and an average monthly payroll exceeding $110,000. The names of each of these businesses indicates they are engaged in similar business activity—registering emotional support animals.

35. **Gaughan** worked full-time for ADW for almost a decade until he resigned in April 2018, and in early 2018, **Gaughan**'s LinkedIn profile does not reflect any involvement with animal support services.

36. Further, your affiant reviewed **Gaughan**'s federal income tax returns for the tax years 2011 through 2018. In doing so, your affiant found no indication that **Gaughan** operated or worked with any animal support companies, or that **Gaughan** paid employees to work for animal support companies.

37. SBA and Bank of America records reflect that seven (7) of the eleven (11) loans have been disbursed, with a total disbursed amount of $2,179,465.00. All disbursed funds were deposited into two accounts at Bank of America in the names of Therapy Dog International or Therapetic Solutions Inc.

38. Specifically, according to SBA records, **Gaughan** submitted applications for the following four (4) PPP loans for businesses located at the 15th Street UPS box; three (3) of these loans were disbursed:

> **Loan Number [redacted]7206**: **Gaughan** applied for Loan Number [redacted]7206 through the lender Fund-Ex Solutions Group LLC under the business name Service Animals of America, and listed the business address for Service Animals of America as the 15th Street UPS box. According to the loan application documents, Service Animals of America has twenty-five (25) employees and an average monthly payroll of $121,215. **Gaughan**'s address listed on this loan application is [redacted] NE, Washington, DC. The loan was approved in the amount of $303,000, and the outstanding balance is $303,000. As of June 6, 2020, the loan status was "past due disbursed" according to SBA records. The email address listed on the application is serviceanimalsofamerica@gmail.com.
>
> **Loan Number [redacted]7308**: **Gaughan** applied for Loan Number [redacted]7308 through Celtic Bank Corporation under the business name Service Dog of America, and listed the business address for Service Dog of America as the 15th Street UPS box. According to the loan application documents, Service Dog of America has twenty-five (25) employees and an average monthly payroll of $121,215. **Gaughan**'s address listed on this loan is the [redacted] NE, Washington, DC. According to SBA records, Celtic Bank cancelled this loan in May 2020. The email address listed on the PPP loan application is kengaughan@gmail.com.
>
> **Loan Number [redacted]7409**: **Gaughan** applied for Loan Number [redacted]7409 through Radius Bank under the business name Certapet Incorporated, and listed the business address for Certapet Incorporated as the 15th Street UPS box. According to the loan application documents, Certapet Incorporated had twenty-five (25) employees and an average monthly payroll of $121,215. **Gaughan**'s address listed on this loan is listed as the 15th Street UPS box. The loan was approved in the amount of $303,100, and the outstanding balance is $303,038. As of June 5, 2020, the loan status was "disbursed." The email address listed on the PPP loan application is certapet@gmail.com.

**Loan Number** [redacted]**7306**: The application for Loan Number [redacted]7306 was submitted to First Bank of the Lake under the business name ESA Registry International, and listed the business address for ESA Registry International as the 15th Street UPS box. According to the loan application documents, ESA Registry International has twenty-five (25) employees and an average monthly payroll of $151,325. The loan was approved in the amount of $378,310.00, and the outstanding balance is $378,310. As of June 6, 2020, the loan status was "disbursed current." Law enforcement has not yet received information about what email address was listed on the PPP loan application.

39. In addition, according to SBA records, the following seven (7) loans for businesses, all of which are purportedly located at the 15th Street UPS box, were applied for in **Person 1**'s name; at least four (4) of those PPP loans have been disbursed:

**Loan Numbers** [redacted]**7402 &** [redacted]**7807**: Loan Number [redacted]7402 was applied for in **Person 1**'s name through Northeast Bank under the business name Official Service Dogs. The business address for Official Service Dogs listed on the PPP loan application is the 15th Street UPS box. According to the loan application documents, Official Service Dogs has twenty-five (25) employees and an average monthly payroll of $121,215. Loan Number [redacted]7402 was cancelled.

According to information Northeast Bank provided, after Loan Number [redacted]7402 was cancelled, the borrower provided information that had been requested by the bank. As a result, Northeast Bank approved Loan Number [redacted]7807 for business name Official Service Dogs, with the address listed as the 15th Street UPS box, in the amount of $303,000. According to the loan application documents, Official Service Dogs has twenty-five (25) employees and an average monthly payroll of $121,200. Additional documentation provided included a bogus residential lease agreement signed by tenant [redacted]Person 1 on behalf of Official Service Dogs and landlord [redacted]. This lease agreement was a version of the same fraudulent lease documents mentioned above found on **Gaughan**'s ADW computer and personally owned MacBook. As of June 5, 2020, this loan status was "active but undisbursed" according to SBA records. According to information received from Northeast Bank, this loan was closed and funded on June 9, 2020. The email address listed on the PPP loan application is [redacted]@gmail.com.

**Loan Number** [redacted]**7709**: Loan Number [redacted]7709 was applied for in **Person 1**'s name through Bank of America under the business name Therapetic Solutions. The business address for Therapetic Solutions listed on the loan application is the 15th Street UPS box. According to the loan application documents, Therapetic Solutions has twenty-five (25) employees and an average monthly payroll of $122,937. The loan was approved in the amount of $307,342 and, according to Bank of America, was disbursed on May 4,

2020. Bank of America's PPP loan application did not ask applicants to list an email address, and none was listed on this application.

**Loan Number [redacted]7303**: Loan Number [redacted]7303 was applied for in **Person 1**'s name through Kabbage Incorporated under the business name Therapy Dog Incorporated. The business address for Therapy Dog Incorporated listed on the loan application is the 15th Street UPS box. According to the loan application documents, Therapy Dog Incorporated has twenty-five (25) employees and an average monthly payroll of $110,973. The loan was approved in the amount of $277,432, and the outstanding balance is $277,432. As of June 9, 2020, the loan status was "disbursed" according to SBA records. The email address listed on the PPP loan application is richard.s.vost@gmail.com.

**Loan Number [redacted]7708**: Loan Number [redacted]7708 was applied for in **Person 1**'s name through Bank of America under the business name Therapy Dog International. The business address for Therapy Dog International listed on the loan application is the 15th Street UPS box. According to the loan application documents, Therapy Dog International has twenty-five (25) employees and an average monthly payroll of $122,937. The loan was approved in the amount of $307,343.00 and, according to Bank of America, the loan was "disbursed" on May 4, 2020. Bank of America's PPP loan application did not ask applicants to list an email address, and none was listed on this application.

**Loan Number [redacted]7901**: Loan Number [redacted]7901 was applied for in **Person 1**'s name through Northeast Bank under the business name Therapy Pet Incorporated. The business address for Therapy Pet Incorporated listed on the loan application is the 15th Street UPS box. According to the loan application documents, Therapy Dog Incorporated has twenty-five (25) employees and an average monthly payroll of $121,215. The loan was approved in the amount of $303,000. According to information received from Northeast Bank, the loan was cancelled on July 10, 2020. The email address listed on the PPP loan application is atdugbartey@gmail.com. Google has informed law enforcement that it has no record of this email address, so it is not included among those requested in this search warrant application.

**Loan Number [redacted]7800**: Loan Number [redacted]7800 was applied for in **Person 1**'s name through Fund-Ex Solutions Group LLC under the business name Therapy Pet Incorporated. According to SBA records, the borrower's street address was [redacted], and the borrower's physical street address was the 15th Street UPS box. According to the loan application documents, Therapy Dog Incorporated has twenty-five (25) employees and an average monthly payroll of $121,215. As of May 30, 2020, the loan status was "fully cancelled." Law enforcement has not yet received information about what email address was listed on the PPP loan application.

**a.** ***SBA PPP Loan Application Documents***

40. In executing an SBA Form 2483, a form required as part of the process to receive PPP funding, each Applicant was required to initial and certify that between February 15 and December 31, 2020, "the Applicant has not and will not receive another loan under the Paycheck Protection Program." Here, by receiving at least multiple PPP loans, the Applicant's signed certification on each application was false. Elsewhere on the Form 2483, applicants certified that the information was accurate and that they knew making false statements subjected them to various criminal penalties.

41. As of July 28, 2020, your affiant has received supporting documentation for loan applications submitted to the following institutions: Bank of America (loan number [redacted]7708); Kabbage Inc. (loan number [redacted]7303); Radius Bank (loan number [redacted]7409); Fund-Ex Solutions Group (loan numbers [redacted]7206 and [redacted]7800); Northeast Bank (loan numbers [redacted]7807 and [redacted]7901); and Celtic Bank Corporation (loan number [redacted]7308). These applications included multiple similar or identical supporting documents used under the names of different entities. For example, the same following twenty-five (25) employees and wage amounts were reported for pay periods January 1, 2020 through January 31, 2020 and February 1, 2020 through February 29, 2020 in connection with each of the eight loan numbers listed above.

| Name | Net Amount | Total Hours | Taxes Withheld | Total Pay | Employer Taxes | Total Cost |
|---|---|---|---|---|---|---|
| [redacted] | $ 3,117.88 | 173.33 | $ 868.71 | $ 3,986.59 | $ 412.62 | $ 4,399.21 |
| | $ 3,433.61 | 173.33 | $ 986.31 | $ 4,419.92 | $ 457.47 | $ 4,877.39 |
| | $ 4,731.67 | 173.33 | $ 1,768.21 | $ 6,499.88 | $ 672.74 | $ 7,172.62 |
| | $ 4,410.06 | 173.33 | $ 1,569.83 | $ 5,979.89 | $ 618.92 | $ 6,598.81 |
| | $ 3,820.42 | 173.33 | $ 1,206.15 | $ 5,026.57 | $ 520.26 | $ 5,546.83 |
| | $ 4,034.85 | 173.33 | $ 1,338.38 | $ 5,373.23 | $ 556.13 | $ 5,929.36 |
| | $ 5,738.24 | 173.33 | $ 1,671.62 | $ 7,409.86 | $ 766.92 | $ 8,176.78 |
| | $ 3,021.88 | 173.33 | $ 834.71 | $ 3,856.59 | $ 399.16 | $ 4,255.75 |
| | $ 5,321.28 | 173.33 | $ 2,131.91 | $ 7,453.19 | $ 570.18 | $ 8,023.37 |
| | $ 3,309.89 | 173.33 | $ 936.70 | $ 4,246.59 | $ 439.53 | $ 4,686.12 |
| | $ 3,599.63 | 173.33 | $ 1,080.28 | $ 4,679.91 | $ 484.37 | $ 5,164.28 |
| | $ 5,160.49 | 173.33 | $ 2,032.71 | $ 7,193.20 | $ 744.50 | $ 7,937.70 |
| | $ 4,624.48 | 173.33 | $ 1,702.07 | $ 6,326.55 | $ 654.80 | $ 6,981.35 |
| | $ 4,838.88 | 173.33 | $ 1,834.33 | $ 6,673.21 | $ 690.68 | $ 7,363.89 |
| | $ 3,765.64 | 173.33 | $ 1,174.27 | $ 4,939.91 | $ 511.28 | $ 5,451.19 |
| | $ 3,514.36 | 173.33 | $ 818.89 | $ 4,333.25 | $ 448.49 | $ 4,781.74 |
| | $ 4,008.05 | 173.33 | $ 1,321.85 | $ 5,329.90 | $ 551.64 | $ 5,881.54 |
| | $ 4,383.26 | 173.33 | $ 1,553.29 | $ 5,936.55 | $ 614.44 | $ 6,550.99 |
| | $ 4,517.27 | 173.33 | $ 1,635.95 | $ 6,153.22 | $ 636.86 | $ 6,790.08 |
| | $ 5,489.15 | 173.33 | $ 1,574.05 | $ 7,063.20 | $ 731.05 | $ 7,794.25 |
| | $ 4,946.09 | 173.33 | $ 1,900.45 | $ 6,846.54 | $ 708.62 | $ 7,555.16 |
| | $ 3,765.64 | 173.33 | $ 1,174.27 | $ 4,939.91 | $ 511.28 | $ 5,451.19 |
| | $ 5,669.71 | 173.33 | $ 2,346.80 | $ 8,016.51 | $ 613.26 | $ 8,629.77 |
| | $ 4,710.80 | 173.33 | $ 1,269.09 | $ 5,979.89 | $ 618.92 | $ 6,598.81 |
| | $ 2,957.89 | 173.33 | $ 812.04 | $ 3,769.93 | $ 390.19 | $ 4,160.12 |
| Totals | **$ 106,891.12** | **4333.25** | **$ 35,542.87** | **$ 142,433.99** | **$ 14,324.31** | **$ 156,758.30** |

42. In addition to the evidence that the applications are fraudulent described above, there is further evidence in the material provided for various of the loan applications. For example:

**Loan Number [redacted]7708**: Documents provided to Bank of America to support payroll obligations for Therapy Dog International (EIN: [redacted]0847) include Payroll Summary Reports as of February 1, 2020 for pay period January 1, 2020 through January 31, 2020, and March 1, 2020 for pay period February 1, 2020 through February 29, 2020. The employees listed and payroll amounts per the reports are identical other than the report and check dates. Payroll Details Reports were also provided for the same period. Similar to the Payroll Summary Reports, the names and numbers on both reports were identical other than report and check dates. Each report showed twenty-five (25) employees, a total monthly pay of $144,817.27, employer taxes of $14,570.99, and total payroll costs of $159,388.26.

**Loan Number [redacted]7303**: Documents provided to Kabbage Inc. to support payroll obligations for Therapy Dog Incorporated (EIN: [redacted]1090) include Payroll Summary Reports as of February 1, 2020 for pay period January 1, 2020 through January 31, 2020,

and March 1, 2020 for pay period February 1, 2020 through February 29, 2020. Each report showed twenty-five (25) employees, a total monthly pay of $144,817.27, employer taxes of $14,570.99, and total payroll costs of $159,388.26. The documents provided were identical to the Payroll Summary and Payroll Details Reports documents provided to Bank of America for [redacted]7708 except for the entity name in the right-hand corner of the document being "Therapy Dog Inc" versus "Therapy Dog International."

**Loan Number [redacted]7409:** Documents provided to Radius Bank included identical Payroll Summary Reports and Payroll Details Reports for January and February 2020 as described above, except that "Certapet Inc." was listed as the entity name in the upper right corner of the documents. Further, the employees claimed are the same twenty-five (25) employees as the other applications listed herein.

**Loan Numbers [redacted]7206 and [redacted]7800:** Applications were submitted to Fund-Ex Solutions by the following entities: Service Animals of America, Certapet Incorporated, and Therapy Pet Incorporated. On June 24, 2020, an employee of Fund-Ex Solutions filed an SBA Hotline compliant. The compliant noted that while the loans for Service Animals of America and Certapet Incorporated were applied for by **Gaughan**, and Therapy Pet Incorporated was filed by **Person 1**, all three claimed the same twenty-five (25) employees. These twenty-five (25) employees are the employees listed above that were utilized on applications across all of the lending institutions. The compliant further stated that all three applications included various tax forms with identical numbers for each entity.

**Loan Numbers [redacted]7807 and [redacted]7901:** Documents provided to Northeast Bank included the same twenty-five (25) employees mentioned above. Additionally, bank statements were provided for two separate entities: Official Service Dogs (Bank of America account [redacted]9804) and Therapy Pet Inc. (Bank of America Account [redacted]6270). Several months of statements were provided. All dollar amounts and transactions within those statements were identical. The only differences were the entity name and account number, suggesting the same statements were likely altered to be provided for two separate entities.

**Loan Number [redacted]7308:** Documents provided to Celtic Bank Corporation include a voided check that states the entity "Service Dog of America" in the upper left corner. But on the subsequent portions of the check, including the payment record, the entity shown on the upper left portion of the two sections states "Therapetic". The check is drawn on Bank of America account [redacted]6270. As exhibited above, during the 2018 search warrant executed on **Gaughan's** U Street Residence, multiple checks were found written to Gaughan from "Therapetic" and drawn on Bank of America account [redacted]6270. Based on this information, it is likely that this voided check was altered to suggest Service Dog of America controlled the bank account. In addition, the same twenty-five (25) employees listed above were utilized in an attempt to obtain loan number [redacted]7308 from Celtic Bank Corporation. Payroll summary reports provided for all

PPP loan documents received to date were identical, except for the entity name of "Service Dog of America" being in the upper right corner of the reports submitted to Celtic Bank Corporation.

***b. Supporting Tax Forms***

43. A variety of federal tax forms were submitted as supporting documents for the following loans: Bank of America (loan number [redacted]7708); Kabbage Inc. (loan number [redacted]7303); Radius Bank (loan number [redacted]7409); Fund-Ex Solutions Group (loan numbers [redacted]7206 and [redacted]7800); Northeast Bank (loan numbers [redacted]7807 and [redacted]7901); and Celtic Bank Corporation (loan number [redacted]7308). These tax forms include Form 990, Return of Organization Exempt from Income Tax (Form 990), Form 940, Employer's Annual Federal Unemployment (FUTA) Tax Return (Form 940), and Form 941, Employer's Quarterly Federal Tax Return (Form 941).

44. Form 990's are filed by tax-exempt organizations and are open to public inspection. The application for Loan Number [redacted]7807 included a 2018 Form 990. Forms 990 filed after 2018 are available on IRS.gov through the Tax-Exempt Organization Search function. The Form 990 provided with the loan application is dated March 31, 2019.

45. A search of the Applicant's Employer Identification Number (EIN) ([redacted]7450) yielded no Forms 990. The search did yield a determination letter dated February 25, 2020 determining that the Applicant is a tax-exempt organization. As the below return was not available on IRS.gov, and since the entity was not determined to be tax exempt until 2020, it is likely the Form was never filed with the IRS and is likely fraudulent.

46. Of further note, the principal officer listed on the Form 990 is **Gaughan**. The application lists **Person 1** as the Applicant and principal officer for Official Service Dogs. The

signature on the Form 990 appears to read "**Kenneth Gaughan**" even though the printed name is "Kevin Ganglof". Neither **Gaughan** nor Ganglof is listed as employees on the employee listing provided as supporting documentation.

47. 2019 Forms 940 were provided with at least three (3) applications for Official Service Dogs, Therapy Dog International, and Therapy Dog Incorporated. All three returns were signed on December 30, 2019 by [redacted] Person 1, CFO. Two (2) of the three (3) Forms 940 were identical other than the EIN and Name. Forms 940 submitted for Therapy Dog International (loan number [redacted] 7708) and Therapy Dog Incorporated (loan number [redacted] 7303) have total payments to all employees of $1,709,301.97, FUTA tax before adjustments of $2,563.80, and Total FUTA tax after adjustments of $92,302.31. Based on the training and experience of other federal agents associated with this investigation, it is unlikely that two businesses would have equal payments to employees and FUTA tax balances for the same year. Additionally, it is unlikely that an entity would complete and sign Forms 940 prior to year-end. These irregularities suggest that the Forms are likely fraudulent.

48. 2019 Forms 941 were provided for the first, second, third, and fourth quarters for the following entities: Service Animals of America (EIN [redacted] 2437); Therapy Pet Incorporated (EIN [redacted] 1364); Certapet Incorporated (EIN [redacted] 1218); and Therapy Dog Incorporated [redacted] 1090). These Forms were identical in every way except for EIN, Name, and the signer. Not only were the Forms identical across entities, all numbers on the Forms were identical across months and quarters. Based on typical turnover for businesses employing twenty-five (25) employees, it is unlikely that each entity would consistently employ twenty-five (25) employees

for an entire year with equal and even monthly earnings. It appears as if the Forms 941 were altered and duplicated to use as support for multiple loan applications.

49. Based on the use of seemingly altered, duplicative Federal Tax Forms, it appears as if the Applicant utilized bogus documents to obtain PPP funding.

### *III. FRAUD ON THE SBA'S ECONOMIC INJURY DISASTER (EIDL) PROGRAM*

50. According to SBA records, **Gaughan** submitted applications for the following twelve (12) EIDL loans for businesses, which cited the same business address and purported in several cases to have identical gross revenues and/or costs across different business entities in other EIDL loan applications:

**EIDL Application Number [redacted]4152:** Application Number [redacted]4152 was applied for by **Gaughan** directly with the SBA under the name Therapetic Solutions Incorporated. According to SBA records, the applicant's business address was the 15th Street UPS box and the borrower's physical street address was [redacted] Northeast, Washington, DC. According to the application, Therapetic Solutions Incorporated has three employees, gross revenues of $210,000, and Non-Profit costs of operation of $210,000. **Gaughan** received a $3,000 advance payment as a result of this application. The email address listed on this EIDL application is help@esapet.org.

**EIDL Application Number [redacted]2063:** Application Number [redacted]2063 was applied for by **Gaughan** directly with the SBA using the business name Anything Pawsable Incorporated. SBA records indicate the applicant's business address was the 15th Street UPS box and the borrower's physical street address was [redacted] Northeast, Washington, DC. The application stated Anything Pawsable Incorporated has one employee, $110,000 in revenue, and $110,000 in cost of goods sold. No funds have been disbursed as a result of this application. The email address listed on this EIDL application is paxton7@aol.com.

**EIDL Application Number [redacted]7207:** Application Number [redacted]7207 was applied for by **Gaughan** with the SBA using the business name Therapy Pet Incorporated. SBA records show that the applicant's business address was the 15th Street UPS box and the borrower's physical address was [redacted] Northeast, Washington, DC. The application stated Therapy Pet Incorporated three employees, gross revenues of $210,000, and Non-Profit costs of operation of $210,000. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is madams6119@gmail.com.

**EIDL Application Number [redacted] 8932:** Application Number [redacted] 8932 was applied for by **Gaughan** with the SBA using the business name Therapy Dog International. SBA application data show the applicant's business address was the 15th Street UPS box and the borrower's physical address was [redacted] Northeast, Washington, DC. Therapy Dog International claimed to have three employees and gross revenues of $210,000 and Non-Profit costs of operation of $210,000. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is certifytherapydog@gmail.com.

**EIDL Application Number [redacted] 7566:** Application Number [redacted] 7566 was applied for by **Gaughan** with the SBA using business name ESA Registry International. The applicant's business address was the 15th Street UPS box and the borrower's physical address was [redacted] Northeast, Washington, DC. ESA Registry International claimed to have three employees and provided no revenue or cost information. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is esaregistryinternational@gmail.com.

**EIDL Application Number [redacted] 1428: Gaughan** applied for loan Application Number [redacted] 1428 under the business name Official Service Dogs and listed the business address as the 15th Street UPS Box. The borrower address was [redacted] Northeast, Washington, DC. Official Service Dogs listed three employees and did not provide gross revenue or cost information. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is richard.s.vost@gmail.com.

**EIDL Application Number [redacted] 8301: Gaughan** applied for loan Application Number [redacted] 8301 under the business name Service Dog of America and listed three (3) employees. Per SBA application data, the business address provided was the 15th Street UPS Box, and the borrower's address was [redacted] Northeast, Washington, DC. Service Dog of America did not provide gross revenue or cost numbers. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is kengaughan@gmail.com.

**EIDL Application Number [redacted] 4874: Gaughan** applied for Application Number [redacted] 4874 under the business name Certapet Inc and listed three (3) employees. The application stated gross revenue of $210,000 and cost of goods sold totaling $210,000. The business address provided was the 15th Street UPS Box and the borrower's address was [redacted] Northeast, Washington, DC. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is certapet@gmail.com.

**EIDL Application Number [redacted] 1397:** Application Number [redacted] 1397 was applied for by **Gaughan** using the business name Service Animals of America. Service Animals

of America claimed to have three (3) employees and did not provide revenue or cost information. The business address provided was the 15th Street UPS Box and the applicant's address was [redacted] Northeast, Washington, DC. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is intlserviceanimal@gmail.com.

**EIDL Application Number [redacted]9829: Gaughan** applied for Application Number [redacted]9829 under the business name International Service Animals. International Service Animals provided the business address of the 15th Street UPS box and claimed to have three (3) employees. The borrower's address was [redacted] Northeast. International Service Animals did not provide revenue or cost numbers. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is serviceanimalsofamerica@gmail.com.

**EIDL Application Number [redacted]3683: Gaughan** applied for loan Application Number [redacted]3683 using business name Therapy Dog Incorporated claiming to have three (3) employees. Therapy Dog Incorporated's business address was the 15th Street UPS Box and the applicant's address was [redacted] Northeast, Washington, DC. There were no revenue or cost numbers provided. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is atdugbartey@gmail.com. As stated above, Google has informed law enforcement that it has no record of this email address.

**EIDL Application Number [redacted]2533: Gaughan** applied for loan Application Number [redacted]2533 using business name US Therapy Dog. US Therapy Dog claimed three (3) employees and did not provide revenue or cost information. The business address provided was the 15th Street UPS Box and the applicant's address was [redacted] Northeast, Washington, DC. As of July 22, 2020, no funds were disbursed as a result of this application. The email address listed on the EIDL application is rstrauski@gmail.com. As stated above, Gaughan is known to go by the alias of **Richard Strauski**, and this email address was used to register the website for SCY in **Gaughan**'s scheme against ADW.

51. In addition to the loans described in this affidavit, SBA records reflect that **Person 1** applied for a PPP loan in the name [redacted], with the address [redacted]. In contrast with the businesses associated with the 15th Street UPS box, the loan application for [redacted] shows that [redacted] has only a single employee and an average monthly payroll of $7,818. This loan has been disbursed and the outstanding balance is $19,545. The email associated with this application was

[redacted].com. **Person 1**'s LinkedIn profile reflects that he currently has two jobs—as the [redacted] of [redacted] (a position **Person 1** has held since January 2016), and as an [redacted] at [redacted] **Person 1**'s LinkedIn profiles does not reflect any involvement with animal support services.

### *IV. EVIDENCE OF FRAUDULENT DOCUMENTATION RELATED TO THE PURPORTED BUSINESS USED TO OBTAIN PPP AND EIDL LOANS*

52. Records obtained from the internet domain registrar and web hosting company GoDaddy LLC show that an account with the login name "**kennethpgaughan**" reserved numerous internet domains similar to the businesses used to obtain the PPP loans, including:

- servicedogdirectory.com
- usservicedogregistry.net
- certapet.net
- certapets.com
- certapet.org
- certapets.org
- esaregistry.net
- esadirectory.com
- esadogregistry.org
- esadirectory.org
- therapetic.org
- therapetic.us
- therapypetdog.com
- therapypetdog.org

53. The GoDaddy account used to register the foregoing domains listed the customer name as **Richard Strauski**, the company name as SCY, and the customer address as 1718 M Street NW, Suite 170, Washington, DC ("the M Street address"), which converted into the 15th Street UPS box.

54. A search of electronic media seized from **Gaughan**'s U Street Residence revealed numerous service or support animal certificates purportedly signed by "**Richard Strauski**"

certifying an animal as a service or emotional support animal that appeared to be issued by Therapetic. For example, a fraudulent support animal registration certificate that was purportedly signed by "**Richard Strauski**" listed the address of the 15th Street UPS box and stated that a dog "Tex" was "registered with TheraPetic's National Registry." The email address on the certification has the domain esadirectory.org, which **Gaughan** registered. Similarly, your affiant discovered another fraudulent animal support certification, signed by **Strauski**, for a squirrel named Elly May. The certificate displayed the email address contact@therapetic.org and a logo for Therapetic Solutions. Based on this, your affiant believes that **Gaughan** prepared the fraudulent certificates using the alias **Richard Strauski** in order to conceal his involvement.

55. Similarly, while conducting a review of the electronic media seized from **Gaughan**, your affiant found an email letter from "**Richard Strauski**, Senior Legal Advisor" of Therapetic Solutions to an attorney at the law firm Wilson Sonsini Goodrich & Rosati confirming that Therapetic Solutions would voluntarily remove the logo of Hawaiian Airlines Incorporated from its website. Your affiant is aware that those who commit service animal fraud often represent that their certifications can be used to bring animals onto airplanes. Your affiant found similar email letters from "**Richard Strauski**, Senior Legal Advisor" of Therapetic Solutions to JetBlue Airways Corporation and Alaska Airlines.

## *V. USE OF SBA PPP AND EIDL FUNDS*

56. Based on a review of records to date, your affiant suspects that **Gaughan** received a total of $2,182,465.00 in combined PPP and EIDL funds. Based on information received from Bank of America, **Gaughan** received the funds in two accounts in the name of Therapetic

Solutions Incorporated and Therapy Dog International between May 4, 2020 and May 26, 2020. As of July 27, 2020, the balance in the two accounts totaled approximately $200,000.

57. Your affiant is aware of at least the following purchases and transfers out of the aforementioned accounts:

- On May 27, 2020, a cashier's check for $1,130,000 to Allied Title and Escrow LLC was purchased at Bank of America by Therapy Dog International to fund the purchase of [redacted] Washington, DC.
- On May 27, 2020, Therapetic Solutions Incorporated sent a wire to AYS Marine Enterprise LLC for $295,550. The wire funded the purchase of a 2020 Cruisers Yachts 338 CX 33-foot watercraft.
- Between May 16, 2020 and July 15, 2020, at least $42,869.71 in likely proceeds were transferred to pay a Capital One credit card balance.

58. Form 2483 explicitly states that by signing, the Applicant represents that "[t]he funds will be used to retain workers and maintain payroll or make mortgage interest payments, lease payments, and utility payments, as specified under the Paycheck Protection Program Rule: I understand that if the funds are knowingly used for unauthorized purposes, the federal government may hold me legally liable, such as for charges of fraud." The above-mentioned use of PPP funds to purchase a residence, watercraft, and make personal credit card payments does not meet the certified use of funds requirements specified under the PPP Rule.

***VI. TARGET RESIDENCE***

59. Evidence shows that **Gaughan** is currently residing at [redacted] Washington, DC.

60. **Gaughan** lived at [redacted], Washington, DC prior to June 5, 2020. Based on evidence stated below, **Gaughan** purchased and closed on [redacted] Washington, DC on June 5, 2020. Surveillance and drive-bys of [redacted] Washington, DC, detailed below, suggest that **Gaughan** has been residing there since at least July 20, 2020. Further, **Gaughan** updated his billing address with Capital One to [redacted] Washington, DC on July, 15, 2020.

61. Information was received on July 20, 2020 from Capital One that **Gaughan** recently changed the billing address for a credit card account at their institution to [redacted] Washington, DC. A black Kia Forte baring Maryland license plate [redacted] was observed parked on the street in front of [redacted] Washington, DC on July 20, 2020.

62. Internet searches of [redacted] Washington, DC indicate that the property was sold on June 5, 2020 for $1,089,000. Public deed records show that the home was purchased by [redacted] Trust and the sale was executed with Allied Title and Escrow LLC. Bank of America stated that Bank of America account number [redacted] 9804 in the name of Therapy Dog International ordered a cashier's check on May 27, 2020 payable to Allied Title and Escrow LLC for $1,130,000.

63. Allied Title and Escrow LLC provided a copy of the cashier's check used to purchase [redacted] Washington, DC. The Remitter (Purchaser) of the Bank of America cashier check (number [redacted] 4879) is Therapy Dog International. Allied Title and Escrow LLC provided a copy of the Land Trust Agreement for [redacted] Trust. [redacted] has a 100% beneficial ownership interest in the land trust and has a listed address of [redacted] Washington, DC in the trust agreement. **Gaughan** was residing at this same address prior to

the purchase of [redacted] Washington, DC. Based on information received as part of the search warrant executed on September 25, 2018, on **Gaughan**'s U Street residence, **Gaughan** and [redacted] were involved in a romantic relationship. Further, [redacted] appears in corporate documents as an officer for multiple entities utilized for SBA PPP funding.

64. Surveillance was performed at [redacted] Washington, DC on the following dates: Thursday, July 23, 2020; Friday, July 24, 2020; and Monday, July 27, 2020.

65. On Thursday, July 23, 2020 at approximately 2:24PM, a white male, matching **Gaughan**'s description exited [redacted] Washington, DC to retrieve mail on the front porch of the home. The unidentified male retrieved the mail and went back into the residence. A black Kia Forte baring Maryland license plate [redacted] was observed parked on the street in front of the house.

66. On Friday, July 24, 2020 at approximately 12:40PM a white male, appearing to be aged in late 30's, early 40's with a light beard and baseball hat emerged from [redacted] Washington, DC. The unidentified male was approximately six feet tall with a trim build, matching **Gaughan**'s description. This person looked around the porch, exited towards the street, and entered a black Kia Forte bearing Maryland license plate [redacted] and drove away from the residence.

67. The black Kia Forte baring Maryland license plate [redacted] was registered by King Volkswagen. King Volkswagen is part of the King Auto, including a group of dealerships located in Gaithersburg, MD. This group includes King Kia. The aforementioned Kia Forte had a front paper license plate baring "King Kia".

68. **Gaughan** registered a 2020 Kia Stinger AWD (VIN: [redacted]0651) on June 8, 2020 with the District of Columbia. The vehicle was assigned DC plate [redacted]. A drive-by was performed at approximately 4:20PM on Friday July 24, 2020 at King Kia at 953 North Frederick Ave., Gaithersburg, MD, 20879. **Gaughan**'s Kia Stinger with DC tag [redacted] was observed in the dealer's service lot with a placard hanging from the rearview mirror, likely indicating the vehicle was awaiting service.

69. At approximately 5:50PM on July 24, 2020, the aforementioned Kia Forte was observed parked on the curb outside of [redacted] Washington, DC.

70. On Monday, July 27, 2020 at approximately 12:45PM, an individual matching the description of **Gaughan** exited a black Kia Forte bearing Maryland license plate [redacted] in front of [redacted] Washington, DC. The individual walked up the front outdoor stairway onto the porch and entered [redacted] Washington, DC.

71. The Manager of King Kia in Gaithersburg, MD confirmed that **Gaughan**'s Kia Stinger was serviced by King Kia and that **Gaughan** was in possession of King Kia's Black Kia Forte license plate [redacted] from July 17, 2020 until July 27, 2020 at approximately 6:30PM.

72. On Tuesday, July 28, 2020 at approximately 7:30AM, the Kia Stinger bearing Washington, DC plate [redacted], registered by **Gaughan**, was observed parked on [redacted] Washington, DC outside of [redacted].

73. [redacted] Washington, DC is a multi-level home, including an English basement that appears to have a separate entrance. During the surveillance of the address described above, no individuals were seen approaching or exiting the English basement of the home. There is no indication that any separate residents reside in the basement. Rental units in

Washington, DC are required to have a business license, and no such license exists for [redacted].

74. In your affiant's training and experience, those involved in financial frauds of the type under investigation here often maintain records, receipts, notes, ledgers, bank deposit receipts, money transfer receipts, credit card receipts, money order receipts, and other papers relating to bank fraud, wire fraud and money laundering, and that those records are maintained where they are readily accessible, including in places controlled by the criminals (such as their residences and automobiles). Those involved in fraudulent activities often hide the proceeds of bank transactions and records of fraudulent transactions in secure locations within their residences, automobiles, businesses and storage facilities for their ready access and to conceal them from law enforcement. They also often conceal in their residences, automobiles, businesses, and storage facilities, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value or proceeds of fraudulent activities and evidence of financial transactions relating to obtaining, transferring, concealing, or the spending of large sums of money made from engaging in fraudulent activities.

75. In addition, I know that some of the information related to the fraud is often stored on digital devices/computers – in part because such computers are integral to producing and maintaining the records (including fraudulent and/or manipulated/doctored records) essential to perpetrating the fraud scheme. Those who execute fraudulent schemes (such as the scheme described in this affidavit) use cell phones and other electronic digital devices to communicate with other individuals associated with the schemes about their fraudulent activity. In your affiant's training and experience, such subjects typical keep these devices/computers at their

residence for convenience. This is particularly so now, during the ongoing COVID-19 pandemic. Because **Gaughan** appears to be residing in [redacted] Washington, DC, investigators have reason to believe that the Devices are currently located there. The property to be searched includes laptop computers, mobile phones, and/or tablets owned, used, or controlled by Kenneth Patrick Gaughan, hereinafter the "Devices."

## TECHNICAL TERMS

76. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not

limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files;

storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its

client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A

P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

i. When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-

hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

**COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS**

77. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers;

personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including bank fraud, theft of government money, and money laundering, use digital devices, like the Devices, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Devices, documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers of

other individuals; and records of illegal transactions using stolen financial and personal identification data, to, among other things, (1) keep track of co-conspirator's contact information; (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds for purposes of, among other things, splitting those proceeds with co-conspirators; and (4) store stolen data for future exploitation. Additionally, in this case, the Devices could be used to store and create the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) applications and related documentation, including rosters of purported employees and their salary information.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage

space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

78. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital devices were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Devices at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs,

applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Devices, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated

with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

f. I know that when an individual uses a digital device to commit fraud, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is

also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

**METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

79. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially-trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden,"

erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby

thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating

system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

80. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Devices), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden

files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

**BIOMETRIC ACCESS TO DEVICE(S)**

81. This warrant permits law enforcement agents to obtain from the person of Kenneth Patrick Gaughan (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometic access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

82. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device

through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

83. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

84. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

85. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this

feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

86. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

87. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. During the September 28, 2018 search of **Gaughan**'s U Street residence, law enforcement seized two (2) MacBook computers and an Apple iPhone 11, which was the most current model at the time. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

88. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric

features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

89. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

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

## CONCLUSION

91. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

Daniel Rzepecki
Special Agent
Federal Bureau of Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on August 10, 2020

2020.08.10 18:46:16
-04'00'

G. Michael Harvey
UNITED STATES MAGISTRATE JUDGE