AFFIDAVIT OF SPECIAL AGENT JORDAN KNIGHT IN SUPPORT OF APPLICATION FOR A CRIMINAL COMPLAINT AND SEARCH WARRANT

I, Jordan Knight, having been duly sworn, do hereby depose and state as follows:

AGENT BACKGROUND

1. I have been employed with the United States Secret Service ("Secret Service") since 2014, and I am currently assigned as a Special Agent to the New England Cyber Fraud Task Force within the Boston Field Office. My duties include the investigation of federal offenses, to include wire fraud, bank fraud, access device fraud, and identity theft, among other things. In preparation for my employment as a Special Agent with the Secret Service, I completed extensive training at the Secret Service James Rowley Training Center in Beltsville, Maryland, including courses related to constitutional law, criminal investigations and various financial crimes. I hold a B.A. in Criminology from Central Connecticut State University. Prior to becoming a Special Agent, I was a Sergeant with the Uniformed Division of the Secret Service in Washington, D.C.

PURPOSE OF AFFIDAVIT

2. I submit this affidavit in support of an application for a criminal complaint charging Shane SPIERDOWIS (date of birth xx/xx/1990) with wire fraud, in violation of 18 U.S.C. § 1343.

3. I also submit this affidavit in support of an application for a search warrant for 16 Rockland Circle, Hull, Massachusetts, 02045 (the "TARGET PREMISES") as further described in Attachment A. I have probable cause to believe that these premises contain evidence, fruits, and instrumentalities of false claim, in violation of 18 U.S.C. § 287; theft of public money, in violation of 18 U.S.C. § 641; false statement, in violation of 18 U.S.C. § 1001; false statement, in

violation of 18 U.S.C. § 1014; wire fraud, in violation of 18 U.S.C. § 1343; and bank fraud, in violation of 18 U.S.C. § 1344 (the "TARGET OFFENSES"), as described in Attachment B.

4. As set forth in more detail below, an ongoing investigation has connected SPIERDOWIS with certain fraudulent applications for federally-funded U.S. Small Business Administration ("SBA") loans issued in connection with the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act").

5. This affidavit is based on my personal knowledge, information provided by other law enforcement officers and government employees, information provided by bank personnel, and my review of police reports and other records. This affidavit is not intended to set forth all of the information that I have learned during this investigation but includes only the information necessary to establish probable cause for the requested complaint and arrest warrant.

PROBABLE CAUSE

6. As set forth below, there is significant evidence that SPIERDOWIS submitted fraudulent information to the SBA, the Rockland Trust Company ("RTC"), and Northeast Bank in connection with an SBA Economic Injury Disaster loan ("EIDL") issued to Consulting & Administrative LLC – which resulted in the wiring of $89,900 in loan proceeds to an account controlled by SPIERDOWIS – and in connection with an SBA Paycheck Protection Program ("PPP") loan issued to Advisors Club LLC – which resulted in the wiring of $101,517 in loan proceeds to a separate account controlled by SPIERDOWIS. In connection with this fraudulent scheme, SPIERDOWIS appears to have used fraudulent Social Security numbers ("SSNs"), fraudulent tax forms, and a fraudulent Pennsylvania driver's license. SPIERDOWIS also appears to have made fraudulent representations concerning his role as the supposed president of

Consulting & Administrative LLC and Advisors Club LLC, and concerning those companies' employees and payroll, during a timeframe during which SPIERDOWIS was in fact in federal custody.

7. A recent database query indicated that SPIERDOWIS resides at 16 Rockland Circle in Hull (*i.e.,* the TARGET PREMISES), with date of birth xx/xx/1990, a SSN of xxx-xx-9048, and a Massachusetts driver's license with number Sxxxx0474.[1] A criminal history check for SPIERDOWIS indicates that his date of birth is xx/xx/1990, his SSN is xxx-xx-9048, and that he was the defendant in federal criminal case 1:18-cr-20355 in the Southern District of Florida.

8. Law enforcement records reflect that SPIERDOWIS was pulled over on January 31, 2021 driving a car ("Vehicle 1") that was registered to PERSON 1[2] at the TARGET PREMISES. These records reflect SPIERDOWIS's SSN as xxx-xx-9048 and his Massachusetts driver's license as Sxxxx0474.

RTC Records

9. RTC[3] has provided information indicating that a personal account was opened in January 2021 in the name of SPIERDOWIS, with the address of the TARGET PREMISES, date of birth xx/xx/1990, and Massachusetts driver's license Sxxxx0474. RTC records for this account include a photograph of SPIERDOWIS's Massachusetts driver's license, which reflect

[1] All references in this affidavit to "xx/xx/1990" refer to the same date. Similarly, all references to SSN xxx-xx-9048 refer to the same SSN, and all references to driver's license Sxxxx0474 are to the same number.

[2] Person 1 is a male relative of SPIERDOWIS.

[3] I understand from the RTC website and my review of pertinent records that RTC is insured by the Federal Deposit Insurance Corporation ("FDIC") and is headquartered in Massachusetts.

an address of the TARGET PREMISES, date of birth xx/xx/1990, and Massachusetts driver's license Sxxxx0474.

10. RTC has also provided information showing that the following accounts were opened in 2021:

a. Account ending in 9740 in the name of Consulting & Administrative LLC (the "9740 Account"). This account was opened on February 8, 2021 and received an Automated Clearing House ("ACH") credit for $89,900 on February 22, 2021in connection with an SBA EIDL.[4]

b. Account ending in 9583 in the name of Advisors Club LLC (the "9583 Account"). This account was opened on January 21, 2021 and received an ACH credit for $101,517 on February 24, 2021, in connection with an SBA PPP loan via Northeast Bank.[5] Specifically, the February 28, 2021 statement for the 9583 Account reflects the following credit:

Date	Deposits	Activity Description
2/24	101,517.00	NORTHEAST BANK/PPP LOAN Advisors Club LLC

11. The account opening documents for the 9583 Account and the 9740 Account list

[4] I know that SBA EIDLs are directly processed through the SBA that the SBA relies on the applicant's submissions in the application. I also know, via my training and experience, that ACH credits typically involve interstate wires.

[5] I know PPP loans are processed by a third-party lender to which SBA has delegated authority for the underwriting and approval of such loans. I understand from the Northeast Bank website and my review of pertinent records that Northeast Bank is insured by the FDIC and is headquartered in Maine.

SPIERDOWIS as the sole signatory and list his address as the TARGET PREMISES. Both accounts were opened by SPIERDOWIS in person at the RTC Hingham branch located in Hingham, MA. RTC has retained surveillance images of SPIERDOWIS from the dates on which he opened the 9740 Account and the 9583 Account.[6]

12. The account opening documents for the 9583 Account and the 9740 Account list the known date of birth for SPIERDOWIS (xx/xx/1990) and his known MA driver's license number (Sxxxx0474). However, the account opening documents for the 9583 Account and the 9740 Account – as well as the aforementioned personal account – list SPIERDOWIS's SSN as ending -3175, which does not match the known SSN for SPIERDOWIS.

13. After the SBA credits were deposited into the aforementioned accounts, RTC contacted the SBA and learned that SBA records reflected an SSN for SPIERDOWIS ending in -5521. RTC also learned that SBA records associated with a Consulting & Administrative LLC EIDL application included an RTC statement dated January 31, 2021, which predates the opening of the 9740 Account.[7]

Northeast Bank Records

14. Northeast Bank records include a PPP loan application dated February 17, 2021 requesting a loan of $101,517 for Advisors Club LLC. This application– a copy of which is attached as **Exhibit A** to this affidavit and is hereby incorporated by reference – lists the primary contact as SPIERDOWIS (supposed president of Advisors Club LLC), lists his SSN as ending -

[6] I have reviewed the surveillance images and it appears that the individual depicted is the same person who appears in the MA driver's license photograph of SPIERDOWIS.

[7] I am awaiting production of SBA records in connection with the Advisors Club LLC PPP loan and the Consulting & Administrative, LLC EIDL.

5521, and his address as XX W Market St., Mount Union, Pennsylvania.[8] The application bears the electronic signature of SPIERDOWIS, underneath a certification that all information provided is true and that knowingly making a false statement to obtain a guaranteed loan from SBA is punishable by imprisonment under various federal statutes.

15. Northeast Bank records associated with the Advisors Club LLC PPP loan reveal that SPIERDOWIS provided an RTC statement for the 9583 Account in the name of Advisors Club LLC as part of the loan application documentations. This statement – a copy of which is attached as **Exhibit B** to this affidavit and is hereby incorporated by reference – is dated February 29, 2020, well before the 9583 Account was in fact opened. On March 2, 2021, I met with the RTC Director of Financial Crimes, who confirmed that the February 2020 9583 Account statement appears to be fraudulent.

16. Northeast Bank records for the Advisors Club LLC PPP loan also include photographs of a Pennsylvania driver's license bearing the name Shane SPIERDOWIS and date of birth xx/xx/1990. The front of this supposed license is attached as **Exhibit C** to this affidavit and is hereby incorporated by reference. The photograph image on the license does not appear to be SPIERDOWIS. The listed address on the license is XX W Market Street, Mount Union, PA.[9]

17. Northeast Bank records for the Advisors Club LLC PPP loan also include what purports to be a 2019 Schedule C federal tax filing for the business Advisors Club LLC. This

[8] All references to "XX W Market St." in this affidavit are to the same street number address in Mount Union, Pennsylvania.

[9] I conducted several database checks on the PA driver's license number, all of which yielded negative results. Based on my training and experience, and the information developed during this investigation, I believe that the driver's license presented to Northeast Bank in connection with this PPP loan application was fraudulent.

document lists the proprietor as SPIERDOWIS, with SSN ending -5521, and reflects an annual profit exceeding $450,000. This supposed tax filing is attached as **Exhibit D** to this affidavit and is hereby incorporated by reference.

18. Northeast Bank records for the Advisors Club LLC PPP loan also include what purport to be 2019 IRS Form 940 and 941 filings, which reflect that Advisors Club LLC employed between 32 – 37 employees. These filings bear the electronic signature of SPIERDOWIS as President of Advisors Club LLC. Specifically, these filings reflect the following:

Form	Employer	Date	Reported Payroll
2019 940	Advisors Club LLC	1/27/2020	$487,295
2019 Q1 941	Advisors Club LLC	4/23/2019	$110,311 (32 employees)
2019 Q2 941	Advisors Club LLC	7/28/2019	$124,965 (32 employees)
2019 Q3 941	Advisors Club LLC	10/22/2019	$119,450 (32 employees)
2019 Q4 941	Advisors Club LLC	1/29/2020	$132,569 (35 employees)

Communications with RTC Re: Loan Funds

19. SPIERDOWIS has engaged in numerous communications with RTC seeking the

release of and/or access to the SBA loan funds that were received into Account 9583 and Account 9740. On February 24, 2021, during a phone conversation recorded by RTC, SPIERDOWIS provided the last four digits of the SSN ending in 3175 and date of birth xx/xx/1990, and confirmed that he was the signatory for the 9740 Account.[10] During this call, SPIERDOWIS stated in part:

> "Yes, I sent the manager at the branch when I opened my accounts, they all know me there I am sure you already know that. I sent the manager my loan documentation straight from the SBA all signed and completed. I have done everything that I know I can possibly do on my end, I have one hundred percent verified, one hundred percent confirmed all my documents are there, I mean you guys can go to Sunbiz, these are my companies, there's nothing unusual going on in my situation."

RTC asked if SPIERDOWIS was the owner of the business Consulting and Administrative, LLC and SPIERDOWIS stated in part:

> "Yes, one hundred percent owner. I mean this is what I was talking about with the manager at the bank. The SBA isn't going to send the loan to my business if, if it's not my business, I mean it's just not going to happen. So I mean, I've done everything on my end, I even sent you guys the paperwork."

RTC also asked about information about the Advisors Club LLC business and the PPP loan deposit into the 9583 Account, and SPIERDOWIS stated in part:

> "…because of SBA requirements, so me being the owner, I had to amend these things for the SBA…Everything I am going to give you is the same thing the SBA saw is why we got approval, which is why they sent the money…I am one hundred percent the owner of the company so everything has to be under my name."

RTC requested additional supporting documentation from SPIERDOWIS, to include the original documents provided to the SBA and Northeast Bank that resulted in obtaining the SBA and PPP

[10] I have reviewed several recorded phone conversations between RTC and SPIERDOWIS in addition to this one. I have summarized only portions of the February 24, 2021 call, rather than describe it in its entirety. Quoted portions from this call are not from a formal or verbatim transcript, but from my personal listening to the call.

loan. SPIERDOWIS responded that he would email these documents to an RTC employee.

20. On February 24, 2021, RTC received emails from xxxxx@consultingandadministrative.com and xxxxx@advisorsclubllc.com that included various documents relating to Advisors Club LLC and Consulting & Administrative LLC. One such email attached the 2019 IRS Forms 940 and 941 for Advisors Club LLC that are described *supra*.

21. Another such email attached what purport to be 2019 IRS Form 940 and 941 filings for Consulting & Administrative LLC. These filings bear the electronic signature of SPIERDOWIS as President of Consulting & Administrative LLC. Specifically, these filings reflect the following:

Form	Employer	Date	Reported Payroll
2019 940	Consulting & Administrative LLC	1/30/2020	$559,237
2019 Q1 941	Consulting & Administrative LLC	4/27/2019	$134,786 (27 employees)
2019 Q2 941	Consulting & Administrative LLC	7/24/2019	$130,254 (27 employees)
2019 Q3 941	Consulting & Administrative LLC	10/28/2019	$145,654 (30 employees)
2019 Q4 941	Consulting & Administrative LLC	1/25/2020	$148,543 (30 employees)

Information Concerning SPIERDOWIS's Actual Employment Status in 2019

22. According to federal court filings, SPIERDOWIS was previously charged in the

Southern District of Florida (Case No. 18-cr-20355) with conspiracy to commit securities fraud in connection with his role in a million-dollar pump-and-dump stock manipulation scheme. SPIERDOWIS pleaded guilty and, on October 23, 2018, was sentenced to five years of probation.

23. After SPIERDOWIS violated numerous conditions of his probation, the Court held a detention hearing on March 23, 2019, at which SPIERDOWIS's lawyer represented that SPIERDOWIS had been attempting to find work as a personal trainer and that work or school would give him more structure than "doing nothing all day." The transcript of this hearing makes no reference to Advisors Club LLC and Consulting & Administrative LLC, or to SPIERDOWIS serving as president of any company that employs dozens of workers. SPIERDOWIS was detained pending a revocation hearing.

24. In May 2019, SPIERDOWIS submitted a letter to the Court indicating that he was working on building a fitness company called "Muscle Assassin" and would also purse a commercial driver's license. SPIERDOWIS's letter makes no reference to Advisors Club LLC and Consulting & Administrative LLC, or to SPIERDOWIS serving as president of any company that employs dozens of workers.

25. On May 28, 2019, SPIERDOWIS admitted to various probation violations. During this hearing, SPIERDOWIS's lawyer emphasized SPIERDOWIS's efforts to find a job. SPIERDOWIS's lawyer made no reference to Advisors Club LLC or Consulting & Administrative LLC, or to SPIERDOWIS serving as president of any company that employs dozens of workers.

26. On May 28, 2019, the Court revoked SPIERDOWIS's probation and sentenced

him to 18 months imprisonment, with no supervised release to follow. According to the BOP Inmate Locator, SPIERDOWIS was released from federal custody on June 29, 2020.

Indicators of Fraud

27. SBA records reveal that, since approximately July 2020, SPIERDOWIS has attempted to obtain at least one other SBA loan in addition to the loans mentioned *supra*.

28. Based on my training and experience, and this investigation to date, I believe that the SBA loan applications for Advisors Club LLC and Consulting & Administrative LLC were in fact fraudulent. Among the various indicators of fraud are the following:

a. The purported SSN of SPIERDOWIS that was provided to RTC in connection with the Advisors Club LLC and Consulting & Administrative LLC accounts that received the loan proceeds does not appear to be the actual SSN assigned to SPIERDOWIS.

b. The purported SSN of SPIERDOWIS that was provided to the SBA and Northeast Bank in connection with the Advisors Club LLC PPP loan was different that the purported SSN of SPIERDOWIS that was provided to RTC in connection with the Advisors Club LLC account; neither of these SSNs appear to be the actual SSN assigned to SPIERDOWIS.

c. Records associated with the Advisors Club LLC PPP loan include a February 29, 2020 RTC statement for Advisors Club LLC (Exhibit B) that appears fraudulent in that it predates the opening of the Advisors Club LLC account with RTC.

d. Records associated with the Advisors Club LLC PPP loan include what

appears to be a fraudulent Pennsylvania driver's license (Exhibit C).

e. SBA informed RTC that an RTC statement dated January 31, 2021 was submitted in connection with the Consulting & Administrative LLC EIDL application; this statement appears fraudulent in that it predates the opening of the Consulting & Administrative LLC account with RTC.

f. A supposed 2019 Schedule C (Exhibit D) submitted to Northeast Bank in connection with the Advisors Club LLC PPP loan appears fraudulent in that it misrepresents the SSN of SPIERDOWIS.

g. Other supposed tax filings of Advisors Club LLC submitted to Northeast Bank and RTC appear fraudulent in that they indicate that SPIERDOWIS was the president of a company employing dozens of workers and paying significant payroll at various times in 2019 when SPIERDOWIS was in fact in federal custody. Representations made by SPIERDOWIS and his lawyer to the U.S. District Court for the Southern District of Florida during a relevant timeframe in 2019 concerning SPIERDOWIS's employment fail to mention, and are inherently inconsistent with, any notion that SPIERDOWIS was in fact president of such a company at that time.

h. Other supposed tax filings of Consulting & Administrative LLC submitted to RTC appear fraudulent in that they indicate that SPIERDOWIS was the president of a separate company employing dozens of workers and paying significant payroll at various times in 2019 when SPIERDOWIS was in fact in federal custody. Representations made by SPIERDOWIS and his lawyer to the

U.S. District Court for the Southern District of Florida during a relevant timeframe in 2019 concerning SPIERDOWIS's employment fail to mention, and are inherently inconsistent with, any notion that SPIERDOWIS was in fact president of such a company at that time.

29. Based on for foregoing, and my training and experience, I believe that SPIERDOWIS submitted fraudulent information and documentation in connection with the SBA loan applications and/or bank accounts associated with Advisors Club LLC and Consulting & Administrative LLC.

SEARCH OF TARGET PREMISES

30. Based on my training and experience, and the evidence uncovered during this investigation, I believe that SPIERDOWIS is residing at the TARGET PREMISES.

31. On March 2, 2021 at approximately 12:30 P.M. a Detective from the Hull Police Department ("HPD") observed a person they believed to be PERSON 1 exit the TARGET PREMISES, enter Vehicle 1 and depart the area. At approximately 2:30 P.M., PERSON 1 – operating Vehicle 1 – arrived back at the TARGET PREMISES. Upon arrival, an HPD Detective observed an individual wearing a backwards ball cap and chin-strap style beard, believed to be SPIERDOWIS, exit the TARGET PREMISES and depart the area as a sole occupant, operating Vehicle 1.[11]

32. Based on my training and experience, and facts uncovered during this investigation, I believe that SPIERDOWIS is likely to possess records relating to (a) bank

[11] I am aware of phone recorded calls provided by RTC where SPIERDOWIS stated that he recently came up to Massachusetts from Florida to be with his family and that he will be here for approximately six months to twelve months. Based upon the facts discovered during the case, I was unable to locate any other family members within the surrounding area.

accounts that he has opened, or for which he is signatory; and (b) loans for which the proceeds have been routed to such accounts.

33. Based on my training and experience, and facts uncovered during this investigation, I believe that SPIERDOWIS is likely to possess records relating to both his true identity (*i.e.*, that associated with SSN xxx-xx-9048), as well as records relating to other identities and/or SSNs he has used.

34. I know, based on my training and experience, that:

a. Individuals often keep identification documents and financial records in their residence, in part to ensure the security of these documents and in part to allow for access to these documents when needed;

a. It is common for individuals to keep financial documents, loan documents, bank statements, tax records, debit cards, credit cards, or identification documents for extended periods of time, including for numerous years; and

b. It is common for individuals who use fraudulent documents and/or identifications to retain those documents for substantial periods of time so that they can continue to use them in the commissions of their crimes.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

35. I know based on my training and experience, and facts uncovered during this investigation, that SBA loan applications and certain bank applications can be submitted online via an internet-capable device.

36. I know from my communications with RTC and my review of records that SPIERDOWIS has used telephone and email to engage in communications concerning one or more SBA loans.

37. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

38. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

39. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a

desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019.[12]

40. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly create, receive, send, and/or store records included in the types of records described in Attachment B in computer hardware, computer software, smartphones, and/or storage media.

41. Based on the facts reflected above, and my training and experience, I believe that SPIERDOWIS utilized various fraudulent documents and/or fraudulent identification documents in connection with his fraudulent conduct. I know, from my training and experience, that individuals often use computer equipment in connection to produce fraudulent identification documents or to alter or create fictitious documents, to apply for and/or use accounts under fraudulent identities, and to engage in fraudulent loan applications to avoid law enforcement detection.

42. Based on the reflected above, and my training and experience, I believe that SPIERDOWIS used one or more computers in connection with a fraudulent scheme involving the submission of false information to SBA, RTC, and Northeast Bank.

43. Based on my knowledge, training, experience, and information provided to me by

[12] https://www.census.gov/topics/population/computer-internet/library/publications.html and https://www.pewinternet.org/fact-sheet/mobile/.

other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes

automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium 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 traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

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

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium 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, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also

falls within the scope of the warrant.

i. Further, in finding evidence of how a computer 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 a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

44. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the TARGET PREMISES or seize the computer equipment for subsequent processing elsewhere.

45. The TARGET PREMISES may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the TARGET PREMISES during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in

order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

CONCLUSION

46. Based on the foregoing, there is probable cause to believe that, on or about February 24, 2021, Shane SPIERDOWIS, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud – specifically, by causing $101,517 in funds derived from an SBA loan to be wired into RTC Account 9583, all in violation of Title 18, United State Code, Section 1343.

47. Based on the foregoing, there is also probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B, are likely to be found at the TARGET PREMISES, as described in Attachment A.

Sworn to under the pains and penalties of perjury.

Jordan Knight

Jordan Knight
Special Agent

U.S. Secret Service

Subscribed and sworn by telephone in accordance with Fed. R. Crim. P. 4.1

on March 4, 2021.

Honorable Donald L. Cabell
United Sates Magistrate Judge