UNITED STATES DISTRICT COURT

for the

Southern District of Florida

United States of America v. JEAN RENALD FLEURIDOR and HASAN BROWN,	))))))	Case No. 20-mj-03472-AOR

Dejenda111(s)

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant **in** this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of ___ ....;;2;;.:;0;..;1...;..7_-:..:A=u..gu=s;:..:t=2 5i...:2;=0=2=0_ in the county of Miami-Dade and Broward in the Southern District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1344 and 1349	Conspiracy to commit bank fraud

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

rif Continued on the attached sheet.

David P. Brant

Complainant's signature

Special Agent David Brant, FDIC-OIG

Printed name and title

Attested to by tJ1e Applicant in accordance with the requirements ofFed.R.Crim.P. 4.1by Face Time

Date: 8/25/20

Alicia M. Otazo-Reyes

Judge's signature

City and state: Miami Florida Alicia M. Otazo-Reyes, US Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, David Brant, being first duly sworn, state:

AGENT BACKGROUND AND INTRODUCTION

1. I am a Special Agent with the Federal Deposit Insurance Corporation Office of Inspector General ("FDIC-OIG") and have been so since September 2019. Prior to that, I was a Special Agent with the Internal Revenue Service - Criminal Investigation ("IRS-CI") for approximately ten years. Throughout the course of my career, I have participated and directed numerous criminal investigations involving identity theft, fraud against the government, bank fraud, and many other illegal schemes affecting the government and financial institutions. Through my training and experience, I am familiar with the tactics, methods, and techniques individuals use to commit various types of fraud and money laundering schemes.

2. This affidavit is made **in** support of a criminal complaint charging **JEAN RENALD FLEURIDORand HASAN BROWN** with conspiracy to commit bank fraud, in violation of Title 18, United States Code, Sections 1344 and 1349.

3. The facts set forth in this affidavit are based on information obtained from other individuals in this investigation, including other law enforcement officers and cooperating witnesses, as well as review of documents and records related to this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant; as such, it does not set forth all of my knowledge about this matter.

OVERVIEW OF CRIMINAL CONDUCT

4. This investigation involves two separate, but related, fraud schemes. Law enforcement learned that beginning in or around 2017, **JEAN RENALD FLEURIDOR ,**

HASAN BROWN, and their co-conspirators were involved in a scheme to defraud a bank located in San Antonio, Texas (the "Victim Bank"), which is insured by the Federal Insurance Deposit Corporation ("FDIC"), by creating bank accounts and shell companies with stolen identities and synthetic or manufactured identifies, as described in further detail below.

5. Then, **in** or around March 2020, the Coronavirus Aid, Relief, and Economic Security ("CARES") Act was enacted. It was designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. In or around April through July of 2020, members of this conspiracy utilized the already established shell/ front companies and established or reestablished new shell/front companies, to falsely and fraudulently apply for financial assistance under the Paycheck Protection Program ("PPP"), as described in further detail below.

Defendants and Relevant Entities

PPP Loan Fraud Entities

6. B.V. is a company based in Redwood City, California that processes small business loans. B.V. participated in the PPP by acting as a service provider between small businesses and certain banks, including Bank 1. Small businesses seeking PPP loans could apply through B.V. for PPP loans. B.V. would review the loan application and, if approved, a partner bank disbursed the loan funds to the applicant. The following banks, among others, processed PPP loans:

a. Bank 1 is a bank based in Salt Lake City, Utah, and is insured by the FDIC.

b. Bank 2 is a bank based in Teaneck, New Jersey, and is insured by the FDIC.

c. Bank 3 is a bank based in Charlotte, North Carolina and is insured by the FDIC.

d. Bank 4 bank based in Charlotte, North Carolina, and is insured by the FDIC.

e. Bank 5 is a bank based in Birmingham, Alabama, and is insured by the FDIC.

FLEURIDOR

7. **FLEURIDOR** resides at 228 La Costa Way, Weston, Florida 33326, ("TARGET LOCATION 1").

8. **FLEURIDOR** is the sole registered agent of Skyline Development & Construction LLC, ("Skyline"), a Florida corporation with a principal place of business listed as TARGET LOCATION 1.

9. **FLEURIDOR** 1s the sole signatory on the Bank 4 account for Skyline Development.

10. Law enforcement obtained records from Comcast which revealed that the Internet Protocol Address ("IP Address")[1] 108.207.136.149 (the "TARGET LOCATION **1** IP") is a static IP Address[2] assigned to TARGET LOCATION 1.

11. Law enforcement confirmed that as of August 24, 2020, the TARGET LOCATION IP was registered to TARGET LOCATION 1.

BROWN

12. **BROWN** resides at 3030 NE 188th Street Apt 405, Aventura, FL 33180 ("TARGET LOCATION 2").

13. **BROWN** is the president, owner, and officer of the Florida corporation, Tech Savvy Holding Corp. ("Tech Savvy").

---

[1] An IP Address is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

[2] A static IP address is an IP address that doesn't change. Once a device is assigned a static IP address, that number typically stays the same until the device is decommissioned or the device's network architecture changes.

14. Tech Savvy Holding's principle address is TARGET LOCATION 2.

15. Law enforcement confirmed that as of the week of August 17, 2020, **BROWN** was receiving mail at TARGET LOCATION 2.

Overview of the Paycheck Protection Program

16. As noted above, the CARES Act is a federal law enacted in or around March 2020 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 the PPP. In or around April 2020, Congress authorized over $300 billion in additional PPP funding.

17. 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: (a) average monthly payroll expenses; and (b) number of employees. These figures are used to calculate the amount of money the small business is eligible to receive under the PPP. In addition, businesses applying for a PPP loan must provide documentation to the lending institution showing their payroll expenses; typically, businesses would supply documents showing the amount of payroll taxes reported to the Internal Revenue Service ("IRS").

18. 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 monies, which are 100% guaranteed by the 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.

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

Overview Synthetic Identification Fraud

20. Synthetic Identification ("ID") Fraud is a type of fraud in which a criminal combines real information) such as stolen social security numbers ("SSNs") and false and fraudulent information (such as fake names) dates of birth) etc.) to create a new identity) which is used to open fraudulent credit card accounts and make fraudulent purchases.

21. Based on my training and experience) I am aware that individuals engaged in Synthetic ID fraud often steal SSNs from specific groups of individuals) such as children or prisoners) because those individuals do not have direct access to their credit histories or credit reports. This allows individuals engaged in Synthetic ID fraud to utilize Synthetic IDs for long periods of time withoutdetection.

22. Based on my training and experience) I know that individuals engaged in Synthetic ID fraud can create Synthetic IDs by combining a stolen SSN) fictitious information) and legitimate information. For instance) individuals engaged in Synthetic ID fraud may create a Synthetic ID by combining a legitimate name) with a fictitious date of birth) an illegally obtained SSN) a fictitious mailing address) and an e-mail address created specifically for the Synthetic ID.

23. Based on my training and experience, I know that many credit agencies do not verify SSNs on credit card applications with the SSA; rather, credit agencies use other identifiers to verify if a SSN on a credit application matches an existing profile with someone who already has a credit line.

24. For example, if a SSN on a credit application does not match to anyone in particular, a credit card agencies' system may believe it is encountering a new individual with no credit history, such as a young adult getting their first credit card.

25. Thus, if an individual engaged in Synthetic ID fraud applies for a credit card with a Synthetic ID, they may be able to obtain a credit card. The credit card issued to a Synthetic ID generally has a small amount of available credit, due to the fact the Synthetic ID has no credit history.

26. Based on my training and experience, I know that fraudsters are able to use Synthetic IDs in a number of ways, such as opening bank accounts, obtaining loans, and applying for certain benefits.

ID Theft and Mail Forwarding

27. As noted above, fraudsters create Synthetic IDs by combing real identification information, such as a social security number, with false and fraudulent identification information, such as a fake name.

28. Based on my training and experience, I know that the social security numbers, dates of birth, and other personal identification information ("PII") are often stolen from unwitting victims. Fraudsters have numerous ways of obtaining stolen PII including, but not limited to, purchasing PII from illicit websites, stealing PII from businesses such as hospitals,

banks, or schools, or by fraudulently accessing lawful websites that maintain personal identification information for illicit purposes.

29. In order to evade detection, fraudsters sometimes set up mail forwarding services for accounts they have created (Synthetic IDs) or accounts they have taken over (Identity Theft).

30. Mail forwarding is a service that arranges for mail and packages sent to one address to be forwarded on to a second address.

31. Fraudsters use mail forwarding in a number of ways, including by tricking legitimate companies into sending correspondence to a victim's true address. However, once a company has mailed the correspondence to a victim's true address, fraudsters use mail forwarding to divert the correspondence from the intended address to an address controlled by the fraudsters.

THE SCHEME

32. Beginning in or around January 2019, the Victim Bank identified suspicious Victim Bank accounts which they later determined were opened in the name of incarcerated inmates. As the Victim Bank continued its investigation, it identified approximately 700 suspicious accounts which were opened in the names of suspected identity theft victims and opened in the names of Synthetic IDs (the "VB Fraud Accounts"). The accounts were being used to defraud the Victim Bank. The Victim Bank believed that the accounts were part of one scheme, because among other things, money was wired between various VB Fraud Accounts. Specifically, the VB Fraud Accounts were used to conduct various transactions

that included payments to different entities by credit card and convenience checks[3] beginning in or about January 2017.

Use of Synthetic IDs

33. Law enforcement learned that VB Fraud Accounts were being controlled by **FLEURIDOR** and his co-conspirators who, for the most part, reside in the Southern District of Florida. Law enforcement further learned that **FLEURIDOR** and/ or his co-conspirators registered several shell companies to the stolen identities and Synthetic IDs and opened bank accounts for the shell companies registered to the stolen identifies and Synthetic IDs.

34. For example, during the course of this investigation, law enforcement learned that the Florida corporation Carter Landscaping Services Inc. ("Carter Landscapint') is registered to "Nicholas Carter" at an address in Naples, Florida. In addition to registering a company in the name "Nicholas Carter," member of this conspiracy also opened bank accounts in the name of "Nicholas Carter." The Social Security Administration confirmed that the Social Security number listed for "Nicholas Carter" was assigned to an individual in 2003 with a different name and date of birth than the purported "Nicholas Carter." Therefore, based on my training and experience, I know that "Nicholas Carter" (SID-1) is a Synthetic ID created using a false and fraudulent name, along with a social security number registered to an unrelated individual.

35. Additionally, during the course of this investigation, law enforcement learned that Florida corporation Debs Housekeeping Services Inc. ("Debs") is registered to "Deborah Brown" at an address in Miami, Florida. The Social Security Administration

---

[3] Convenience checks are blank checks that lenders, usually credit card issuers, offer to their customers. The borrowers can use these checks to pay offbalances on other cards, make new purchases, or to secure a cash advance.

confirmed that the Social Security number listed for "Deborah Brown" was assigned to an individual in 2002 with a different name and date of birth than the purported "Deborah Brown". Therefore, based on my training and experience, I know that "Deborah Brown" (SID-2) is a Synthetic ID created using a false and fraudulent name, along with a social security number registered to an unrelated individual.

36. Below are just a few of the Synthetic IDs utilized by members of this conspiracy:

VB Fraud Account Name	SID-#	Status ofIdentity
N.C.	SID-1	The Social Security Administration confirmed that the Social Security number listed for SID-1 was assigned to an individual with a different name and DOB. SID-1 was born in 2003.
D.B.	SID-2	The Social Security Administration confirmed that the Social Security number listed for SID-2 was assigned to an individual with a different name and DOB. SID-2 was born in 2002.
D.C.	SID-3	SSN belongs to inmate sentenced to life imprisonment. SID-3 has been in custody since May 2008.
B.H.	SID-4	The Social Security Administration confirmed that the Social Security number listed for SID-4 was assigned to an individual with a different name and D OB. SID-4 was born in 2010.
D.S.	SID-5	The Social Security Administration confirmed that the Social Security number listed for SID-5 was assigned to an individual with a different name and DOB. SID-5 was born in 2002.
M.P.	SID-6	The Social Security Administration confirmed that the Social Security number listed for SID-6 was assigned to an individual with a different name and DOB. SID-6 was born in 2010.
D.B.	SID-7	The Social Security Administration confirmed that the Social Security number listed for SID-7 was assigned to an individual with a different name and D OB. SID-7 was born in 2006.
J.B. 1	SID-8	The Social Security Administration confirmed that the Social Security number listed for SID-8 was assigned to an individual with a different name and DOB. SID-8 was born in 2010.

FLEURIDOR AND IDENTITY FRAUD

37. During the course of this investigation) law enforcement identified multiple payments from VB Fraud Accounts to **FLEURIDOR's** Skyline Development account.

38. For example) law enforcement identified credit card payments from VB Fraud Accounts in the names of SID-3 and SID-4 to **FLEURIDOR's** Skyline Development account.

39. Furthermore) law enforcement determined that on or about April 20) 2019) VB Fraud Accounts opened in the names of SID-3 and SID-4 were accessed from TARGET IP 1.

40. Between on or about December 12) 2018) and on or about December 25) 2019) TARGET IP 1 was utilized to log into a Victim Bank account in the name **ofFLEURIDOR** who resides at TARGET LOCATION 1.

FLEURIDOR AND PPP LOAN FRAUD

41. Continuing through on or about April 4, 2020, Bank 5 received a PPP loan application for **FLEURIDOR's** company, Skyline Development, seeking $60,000. **FLEURIDOR** was listed as the primary contact in the application, and TARGET LOCATION **1** was listed as the address for Skyline Development on the application.

42. In the loan application, **FLEURIDOR** provided Bank 5 with a purported IRS Form 941 (employer's quarterly federal tax return) for the first quarter of 2019. Employers use this form to report payroll taxes- such as income tax, social security tax, or Medicare tax- withheld from employees' paychecks. The Form 941 provided stated that Skyline Development had 11 employees and had paid approximately $25,000 in wages and withheld no federal income taxes during the first quarter of 2019.

43. In the loan application, **FLEURIDOR** provided Bank 5 with a purported list of employees. This list included approximately nine employees including **FLEURIDOR.** SIDs 4 and 5 were listed as Skyline Development employees.

44. Approximately seven payments were made between October 12, 2018, and February 6, 2019, from the VB Fraud Accounts for SID-4 and SID-5 to the Skyline account owned by **FLEURIDOR.**

45. The Florida Department of Revenue ("FLDOR") maintains records of wages paid to employees by corporations **in** Florida. The FLDOR has no record of any wages paid to employees of Skyline in Florida.

46. As part of his application, on or about April 28, 2020, **FLEURIDOR** digitally signed the SBA Form 2483. In that form, **FLEURIDOR** indicated that Skyline Development had an average monthly payroll of $25,000 and sought a loan amount of $60,000. **FLEURIDOR** initialed by electronic signature a representation that the information in the application was "true and accurate in all material respects." **FLEURIDOR** acknowledged that "knowingly making a false statement to obtain a guaranteed loan from SBA is punishable under the law, including ... under 18 USC 1014 by imprisonment of not more than thirty years." Based on the submission, the SBA provided a guarantee on this loan.

47. On or about May 1, 2020, as a result of the loan application for Skyline Development and SBA guarantee, Bank 5 wired $60,000 to the account of Skyline Development at Regions.

48. On or about June 16, 2020, the Skyline Development Bank 4 account was accessed by the TARGET 1P 1.

49. Based on my training and experience, I believe that **FLEURIDOR** submitted a false and fraudulent PPP loan application.

BROWN AND IDENTITY FRAUD

50. As law enforcement continued to investigate fraud against the Victim Bank, law enforcement discovered a Victim Bank account in the name of **BROWN** with a listed address of TARGET LOCATION 2.

51. Law enforcement also discovered that approximately ten of the VB Fraud Accounts were also registered to TARGET LOCATION 2.

52. A further review of the VB Fraud Accounts that listed TARGET LOCATION 2 as an address revealed fraudulent activity. For example, law enforcement located fraudulent Victim Bank Account convenience check payments from SID-6 to **BROWN's** company, Tech Savvy on or about March 20, 2019 and September 18, 2019.

53. Law enforcement also located a VB Fraud Account in the name of SID-2, with a listed address of TARGET LOCATION 2.

BROWN and PPP LOAN FRAUD

54. A further review of VB Fraud accounts assigned to TARGET LOCATION 2 revealed that on or about May 9, 2020, B.V. received a loan application from Debs Housekeeping in the name of SID-2 seeking a loan of $1,413,157.

55. Law enforcement observed that the address on the PPP loan application for Debs Housekeeping did not list TARGET LOCATION 2. However, law enforcement learned that a mail forwarding request was submitted electronically with the United States Postal Service for SID-2. The mail forwarding request was for mail to be forwarded from the address listed on Debs Housekeeping PPP application to TARGETLOCATION 2.

56. Law enforcement learned that multiple other mail forwarding requests directing mail to the TARGET LOCATION 2 address were submitted electronically.

57. In the Debs Housekeeping loan application, an unknown co-conspirator provided B.V. with purpo1ted IRS Forms 941 for the first through fourth quarter of 2019. The Forms 941 stated that Debs Housekeeping Service had 72 employees and had paid approximately $6,783,164 in wages and withheld approximately $1,424,464.44 in federal income taxes during the first through fourth quarters of 2019.

58. A review of the quarterly Forms 941 for Ql 2019 through Q4 2019 contained identical information for each quarterly statement. More specifically, each listed 72 employees, wages paid of $1,695,791 and federal income taxes withheld of $356,116.11. Law enforcement reviewed the metadata document properties for each document, and learned that the documents each had a creation date of February 12, 2019 and modification of May 8,2020.

59. Based on my training and experience, I know that this means that all of the documents in the application were created on the same date rather than completed and submitted quarterly to the Internal Revenue Service in accordance with published deadlines.

60. Debs Housekeeping had no reported employees or payroll. The FLDOR has no record of any wages paid to employees of Debs Housekeeping in Florida.

61. On or about May 9, 2020, someone purporting to be SID-2 digitally signed an SBA Form 2483. In this form, SID-2 indicated that Debs Housekeeping had an average monthly payroll of $565,263 for 72 employees and sought a loan amount of $1,413,157. SID-2 initialed by electronic signature a representation that the information in the application was "true and accurate in all material respects." SID-2 acknowledged that "knowingly making a false statement to obtain a guaranteed loan from SBA is punishable under the law, including ... under 18 USC

1014 by imprisonment of not more than thirty years." Based on the submission, the SBA provided a guarantee on this loan.

62. On or about May 12, 2020, as a result of the loan application for Debs Housekeeping and SBA guarantee, Bank 2 Bank wired $1,413,157to an account of Debs Housekeeping at Bank 3.

63. Subsequent to the funding in the Debs Housekeeping Bank 3 account, multiple payments out of the account occurred including payments to Skyline Development, Tech Savvy, and other entities known to be part of the conspiracy. For example:

a. On or about June 16, 2020, a check in the amount of $200,000 issued from Debs Housekeeping Service was deposited into the Bank 4 account for **FLEURIDOR's** company, Skyline Development.

64. Based on my training and experience, I know that the Debs Housekeeping account was created in the name of a Synthetic ID. I also know that when the fraudulent PPP loan for Debs Housekeeping was dispersed, funds were distributed to **FLEURIDOR** and to **BROWN.**

65. During this investigation, law enforcement also learned that **BROWN** applied for a PPP loan for his company Tech Savvy.

66. On or about May 6, 2020, B.V. received a PPP loan application for **BROWN's** company, Tech Savvy, seeking $544,650. **BROWN** was listed as the primary contact in the application and TARGET LOCATION 2 was listed as the address for Tech Savvy on the application.

67. On that same date, May 6, 2020, TARGET LOCATION 1 IP accessed the Tech Savvy application three times.

68. In the loan application, **BROWN** provided B.V. with purported IRS Forms 941 (employer's quarterly federal tax return) for the first through fourth quarters of 2019. The Forms 941 provided stated that Tech Savvy had 33 employees and had paid approximately $2,614,321.60 in wages, and federal income taxes withheld of $65,358.

69. Additionally, in the loan application, **BROWN** provided B.V. a copy of a Florida Driver's License displaying the TARGET LOCATION 2 address. Law enforcement reviewed information obtained by the State of Florida Department of Highway Safety and Motor Vehicles noting the license provided matched.

70. A review of the quarterly Forms 941 for Ql 2019 through Q4 2019 contained identical information for each quarterly statement. More specifically, each listed 33 employees, wages paid of $653,580.40 and federal income taxes withheld of $16,339.50. Law enforcement reviewed the metadata document properties for each document, and learned that the documents each had a creation date of February 12, 2019 and modification of May 6, 2020.

71. Based on my training and experience, I know that this means that all of the documents in the application were created on the same date rather than completed and submitted quarterly to the Internal Revenue Service in accordance with published deadlines.

72. According to the FLDOR, Tech Savvy became active/ required to file for re-employment assistance tax on May 16, 2020, but had not received a report for the second quarter of 2020.

73. On or about May 6, 2020, **BROWN** digitally signed an SBA Form 2483. In this form, **BROWN** indicated that Tech Savvy had an average monthly payroll of $217,860 for 33 employees and sought a loan amount of $544,650. **BROWN** initialed by electronic signature a representation that the information in the application was "true and accurate in all material respects." **BROWN** acknowledged that "knowingly making a false statement to obtain a guaranteed loan from SBA is punishable under the law, including ... under 18 USC 1014 by imprisonment of not more than thirty years." Based on the submission, the SBA provided a guarantee on this loan.

74. Therefore, based on my training and experience, I believe that **BROWN** is using Electronics and obtaining mailed documents located within TARGET LOCATION 2 to conduct identity and Synthetic ID Fraud and to commit CARES Act fraud.

ADDITIONAL FRAUD MONEY PAID TO FLEURIDOR AND BROWN

75. During the course of this investigation, law enforcement identified another individual, ("TARGET 3"), who resides at an address in Miami, Florida ("TARGET LOCATION 3").

76. Law enforcement learned that at various times during the conspiracy, multiple IP addresses (the "TARGET LOCATION 3 IPs") assigned to TARGET LOCATION 3 were used to further the conspiracy.

TARGET LOCATION 3 AND IDENTITY FRAUD

77. A review ofIP activity from TARGET LOCATION 3 revealed that electronic devices within TARGET LOCATION 3 directed several fraudulent payments from VB Fraud Accounts by credit card and convenience check to **FLEURIDOR's** company, Skyline

Development. The payments included payments from accounts opened in the names of SID-3 and SID-4.

78. Additionally, one of the IPs associated with TARGET LOCATION 3 was utilized to access the VB Fraud Account for SID-6. On or about November 26, 2019, a purchase was made at Best Buy Store #559 located in Pembroke Pines, Florida. The purchase was made with a VB Fraud Account credit card in the name of SID-6. Documents obtained from Best Buy determined the purchase made for various electronics was associated with a Best Buy membership account registered to **FLEURIDOR,** with a listed address of TARGET LOCATION 1.

79. Additionally, one of the IPs associated with TARGET LOCATION 3 was utilized to access the VB Fraud Accounts for SID-7 and SID-8. On or about October 12, 2019, through October 17, 2019, purchases were made at Best Buy Store #559 in Pembroke Pines, Florida. The purchases were made with VB Fraud Account credit cards in the names of SID-7 and SID-8. Documents obtained from Best Buy determined the purchase made for various electronics was associated with a Best Buy membership account for a known co-conspirator.

80. Law enforcement also learned that approximately five payments were made between September 2, 2019, and October 15, 2019, from the VB Fraud Accounts in the names SID-7 and SID-8 to **FLEURIDOR's** company, Skyline Development.

81. Law enforcement also learned that PPP Loan applications were made from TARGET LOCATION 3 IPs, including the application for Debs Housekeeping.

TARGET LOCATION 3 AND PPP LOANS

82. In addition to the false and fraudulent loan application made for Debs Housekeeping, TARGET LOCATION 3 IPs also applied for a false and fraudulent PPP loan for Cater Landscaping.

83. On or about May 11, 2020, B.V received a loan application from Carter Landscaping, Inc. in the name of SID-1, seeking a loan of $1,707,120.

84. On that same date, May 11, 2020, an IP address registered to TARGET ADDRESS 3, accessed the Carter Landscaping application three times.

85. In the loan application, Carter Landscaping provided B.V. with purported IRS Forms 941 (employer's quarterly federal tax return) for the first through fourth quarters of 2019. The Forms 941 stated that Carter Landscaping had 200 employees; had paid approximately $8,194,180 in wages; and withheld approximately $175,791in federal income taxes during the first through fourth quarters of2019.

86. A review of the quarterly Forms 941 for Ql 2019 through Q4 2019 contained identical information for each quarter reflected in the Forms 941. More specifically, each listed 200 employees, wages paid of $2,048,545, and federal income taxes withheld of $43,947.75. Law enforcement reviewed the metadata document properties for each document, and learned that the documents each had a creation date of February 12, 2019 and modification of May 11, 2020. Based on my training and experience, I know that this means that all of the documents in the application were created on the same date rather than completed and submitted quarterly to the Internal Revenue Service in accordance with published deadlines.

87. The Florida Department of Revenue ("FLDOR") maintains records of wages paid to employees by corporations in Florida. The FLDOR has no record of any wages paid to employees of Carter Landscaping in Florida.

88. On or about May 11, 2020, someone purporting to be SD-1 digitally signed an SBA Form 2483. In this form, SD-1 indicated that Carter Landscaping had an average monthly payroll of $682,848 and sought a loan amount of $1,707,120. SD-1 initialed by electronic signature a representation that the information **in** the application was "true and accurate **in** all material respects." SD-1 acknowledged that "knowingly making a false statement to obtain a guaranteed loan from SBA is punishable under the law, including ... under 18 USC 1014 by imprisonment of not more than thirty years." Based on the submission, the SBA provided a guarantee on this loan.

89. On or about May 12, 2020, as a result of the loan application for Carter Landscaping and SBA guarantee, Bank 1 wired $1,707,120 to the account of Carter Landscaping at Bank 3.

90. Subsequent to the funding in the Carter Landscaping Bank 3 accoun,t multiple payments out of the account occurred including payments to Skyline Developmen,t Tech Savvy, and other entities known to be part of the conspiracy.

91. For example, on or about June 10, 2020, Bank 4 surveillance captured **FLEURIDOR** depositing check number 1208 issued from Carter Landscaping in the amount of $100,000 into the Skyline Development account with Bank 4.

92. On or about June 10, 2020, the Skyline Developm ent Bank 4 account was accessed by the TARGET IP 1.

93. Based on my training and experience, I know that *the* Carter Landscaping account was created in the name of a Synthetic ID. I also know that on the same date the Carter Landscaping applied for a fraudulent PPP loan, an IP address assigned to TAR GET LOCATION 3 accessed the loan application.

94. Finally, I know that when the fraudulent PPP loan for Ca1ter Landscaping was dispersed, funds were distributed to entities controlled by **FLEURIDOR, BROWN,** and other co-conspirators.

CONCLUSION

95. Based on my training and experience, and the infonnation provided in this affidavit, I respectfully submit that there is probable cause to believe that **JEAN RENALD FLEURIDOR** and **HASAN BROWN** participated in a conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1344 and 1349.

FURTHER YOUR AFFIANT SAYETH NAUGHT.

t'.

Special Agent David Brant
Federal Deposit Insurance Corporation
Office ofinspector General

Attested to in accordance with the requirements
of Fed. R. Crim. P. 4.1 by FaceTime this 25thday of August, 2020.

Hon. Alicia M. Otazo-Reyes
United States Magistrate Judge