

UNITED STATES DISTRICT COURT

for the

District of Massachusetts

United States of America

v.

Elijah Majak Buoi

Case No.

20-mj-4143-DHH

Defendant(s)

CRIMINAL COMPLAINT

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 April 2020 - Present in the county of Middlesex in the
District of Massachusetts, the defendant(s) violated:

Code Section

18 U.S.C. § 1343

Offense Description

Wire fraud

This criminal complaint is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.

Sheila Magoon / D.H.G.

Complainant's signature

Sheila Magoon, FBI, Special Agent

Printed name and title

Sworn telephonically in accordance with Fed. R. Crim. P. 4.1

Date: Jun 19, 2020

City and state: Worcester, Massachusetts

David H. Hennessy

Judge's signature

Hon. David H. Hennessy, U.S. Magistrate Judge

Printed name and title



**AFFIDAVIT OF SPECIAL AGENT SHEILA MAGOON IN SUPPORT OF
COMPLAINT AND AN APPLICATION FOR A SEARCH WARRANT**

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been employed as such since September 2003. I have been assigned to the Economic Crimes Squad of the Boston Field Office since January 2004. I am a certified public accountant. My duties include the investigation of violations of federal criminal laws, and my experience includes investigations of securities fraud, corporate fraud, bank fraud and mortgage fraud.

2. I am currently investigating Elijah Majak Buoi (“Buoi”) for various crimes including wire fraud and bank fraud in violation of 18 U.S.C. §§ 1343 and 1344, respectively (collectively, the “Target Offenses”).

3. This affidavit is being submitted in support of a criminal complaint against Buoi, charging him with wire fraud in connection with the submission of fraudulent loan applications.

4. This affidavit is also being submitted in support of an application for a warrant to search Buoi’s residence, located at 303 Cross Street, Winchester, Massachusetts (the “Subject Premises”), as described in Attachment A, because there is probable cause to believe that it contains evidence, fruits, and instrumentalities of the crimes listed in paragraph 2 above, as described in Attachment B.

5. In addition, I submit this affidavit in support of an application for seizure warrants for the following:

- a. Up to \$772,000, currently held by Bank of America in, or on behalf of, checking account 4666702641 in the name of Sosuda Tech LLC (“BOA Account 2641”); and
- b. Up to \$1,200,000, currently held by Bank of America in, or on behalf of, savings account 466006700252 in the name of Sosuda Tech LLC (“BOA Account 0252”)

(collectively the “Funds”).¹

6. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses.

7. This affidavit does not set forth all of the facts developed during the course of this investigation and does not set forth all of my knowledge about this matter. This affidavit is intended to show that there is probable cause to believe that Buoi has committed the above-described offense, that evidence, fruits, and instrumentalities of the offense will be found at the Subject Premises, and that the Funds are subject to forfeiture to the United States as the Funds represent proceeds traceable to the offenses set forth above.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

Overview of the Paycheck Protection Program

8. 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 or around April 2020, Congress authorized over \$300 billion in additional PPP funding.

9. 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

¹ The Funds are currently being held by Bank of America either in the identified bank accounts or in a separate account on behalf of the identified bank accounts.

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 showing their payroll expenses.

10. A PPP loan application must be processed by an authorized Small Business Administration (“SBA”) 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.

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

Relevant Individual and Entities

12. Buoi is a resident of Winchester, Massachusetts. Buoi is the President and CEO of Sosuda Tech, LLC (“Sosuda”).

13. Sosuda is a Massachusetts company that was registered with the Massachusetts Secretary of State on or about May 1, 2019. The company was initially registered under the name South Sudanese American Technologies, LLC. On or about May 15, 2019, the name was changed from South Sudanese American Technologies, LLC to Sosuda.

14. Sosuda advertises that it provides various technology services to businesses. Sosuda's website states that it is located at the Subject Premises, and that its office phone number is (781) 439-2149.²

15. Bank of America, N.A. ("Bank of America") is a federally insured financial institution and is an approved SBA lender for PPP loans. Bank of America received at least one PPP loan application on behalf of Sosuda. That application was for \$7.5 million.

16. Fountainhead Commercial Capital ("Fountainhead") is a non-bank finance company and is an approved SBA lender for PPP loans. Fountainhead received a PPP loan application on behalf of Sosuda for \$2 million.

17. Fundbox, Inc. ("Fundbox") is a financial technology company and is an approved SBA lender for PPP loans. Fundbox received a PPP loan application on behalf of Sosuda for \$2 million.

18. Newtek Small Business Finance, LLC ("Newtek"), which is owned by Newtek Business Services Corp, an approved SBA lender for PPP loans. Newtek received a PPP loan application on behalf of Sosuda for \$2 million.

Overview of the Scheme

19. Buoi submitted at least four PPP loan applications, via wire communications in interstate commerce, on behalf of Sosuda between April 2020 and June 2020. As set forth above, three of the applications sought loans of \$2 million each, and one sought a loan in the amount of \$7.5 million.

² See <https://www.sosudatech.com/>. Records reveal that the phone number is a mobile device registered to Buoi at the Subject Premises.

20. There are numerous inconsistencies in the representations on the various loan applications and the supporting documentation Buoi provided with the applications. Based on my training and experience in financial fraud investigations, I believe these inconsistencies indicate that Buoi exaggerated or fabricated information about Sosuda's payroll expenses and operations, and falsified documents, in order to obtain a PPP loan.

The PPP Loan Applications

A. The Bank of America PPP Application

21. On or about April 21, 2020, Buoi, on behalf of Sosuda, submitted an application to Bank of America for a PPP loan in the amount of approximately \$7.5 million (the "Bank of America PPP Loan Application").

22. Buoi signed the Bank of America PPP Loan Application. Buoi also lists the Subject Premises as his address.

23. On the Bank of America PPP Loan Application, Buoi claimed that Sosuda had 353 employees with an average monthly payroll of \$3 million. Buoi certified that the United States was the principal place of residence for those employees.³

24. In support of his payroll calculation, Buoi submitted payroll documentation in the form of an Excel spreadsheet. The Excel spreadsheet indicated an average monthly payroll expense of \$3 million based on Sosuda's payroll expenses for the last seven months of 2019.

³ All PPP applicants must complete the "Paycheck Protection Program Borrower Application Form," which requires the applicant to provide basic information about the business and its payroll. All applicants must answer a series of questions in order to confirm they qualify for a PPP loan. One of the questions asks, "Is the United States the principal place of residence for all employees of the Applicant included in the Applicant's payroll calculation above?"

25. Buoi also submitted an IRS Form 941, an Employer's Quarterly Federal Tax Return, purporting to reflect Sosuda's wages and federal payroll tax information for the first quarter of 2020.⁴ According to this document, Sosuda had 353 employees and paid \$9,498,987 in wages, tips, and other compensation in that period. Buoi signed the IRS Form 941 as the President and CEO of Sosuda and provided a date of April 30, 2020. The form listed Sosuda's address as the Subject Premises. Buoi also listed his phone number as (781) 439-2149.⁵

26. Buoi also submitted an IRS Form 940, an Employer's Annual Federal Unemployment Return, purporting to show Sosuda's total payments to employees for 2019.⁶ According to the IRS Form 940, Sosuda made \$34,800,000 in payments to employees in 2019 and did not have employees in any other state except Massachusetts. Buoi signed the IRS Form 940 as the President and CEO of Sosuda and provided a date of January 31, 2020.

27. The Bank of America PPP Loan Application was denied.

B. The Fountainhead PPP Loan Application

28. On or about May 21, 2020, Buoi, on behalf of Sosuda, submitted an application to Fountainhead for approximately \$2 million in PPP loan funds (the "Fountainhead PPP Loan Application").

⁴ IRS Form 941 is an official document that an employer files with the Internal Revenue Service ("IRS") every quarter in order to report income taxes, Social Security taxes and Medicare taxes withheld from employees' paychecks.

⁵ Each of the IRS 941 forms discussed herein list Sosuda's address as the Subject Premises, and Buoi's phone number as (781) 439-2149.

⁶ IRS Form 940 is an official document that an employer files with the IRS to report its annual Federal Unemployment Tax Act ("FUTA") tax. Together with state unemployment tax systems, the FUTA tax provides funds for paying unemployment compensation. Most employers pay both federal and state unemployment tax.

29. Buoi signed the Fountainhead PPP Loan Application as the President and CEO of Sosuda. Buoi also provided a copy of his Massachusetts driver's license listing his address as the Subject Premises. He also listed his email address as Elijah.buoi@sosudatech.com.

30. On the Fountainhead PPP Loan Application, Buoi claimed that Sosuda had 18 employees, and an average monthly payroll of \$150,000. Buoi certified that the United States was the principal place of residence for those 18 employees.

31. Buoi also submitted an IRS Form 940 purporting to show Sosuda's total payments to employees for 2019. According to this document, Sosuda made \$1.8 million in payments to employees in 2019 and did not have employees in any other state except Massachusetts. Buoi signed the IRS Form 940 as the President and CEO of Sosuda and provided a date of January 31, 2020.

32. Buoi also submitted an IRS Form 941 purporting to report Sosuda's wages and federal payroll tax information for the first quarter of 2020. According to this document, Sosuda had 18 employees and paid \$450,000 in wages, tips, and other compensation in the first quarter of 2019. Buoi signed this document as the President and CEO of Sosuda and provided a date of April 30, 2020.

33. The Fountainhead PPP Loan Application was denied.

C. The FundBox PPP Loan Application

34. On or about June 6, 2020, Buoi, on behalf of Sosuda, submitted an application to Fundbox for approximately \$2 million in PPP loan funds (the "Fundbox PPP Loan Application").

35. Buoi signed the Fundbox PPP Loan Application as the Founder and CEO of Sosuda and provided a copy of his Massachusetts driver's license listing his address as the Subject Premises. He also listed his email address as Elijah.buoi@sosudatech.com.

36. On the Fundbox PPP Loan Application, Buoi claimed that Sosuda had 96 employees, with an average monthly payroll of \$800,000. Buoi also certified that the United States was the principal place of residence for those 96 employees.

37. In support of the Fountainhead PPP Application, Buoi submitted an IRS Form 941 purporting to reflect Sosuda's wages and federal payroll tax information for the first quarter of 2020. According to the IRS Form 941, Sosuda had 96 employees and paid \$2,400,000 in wages, tips, and other compensation. Buoi signed the IRS Form 941 as the President and CEO of Sosuda on April 30, 2020.

38. Buoi also submitted an IRS Form 940 purporting to show Sosuda's total payments to employees for 2019. According to this document, Sosuda made \$9,600,000 in payments to employees in 2019 and did not have employees in any other state except Massachusetts. Boui signed the IRS Form 940 as the President and CEO of Sosuda and provided a date of January 31, 2020.

39. The Fundbox PPP Loan Application was approved and approximately \$2,000,000 was disbursed to BOA Account 2641.

D. The Newtek PPP Loan Application

40. On or about June 9, 2020, Buoi, on behalf of Sosuda, submitted an application to Newtek for approximately \$2 million in PPP loan funds (the "Newtek PPP Loan Application").

41. Buoi signed the Newtek PPP Loan Application as the Founder and CEO of Sosuda and provided a copy of his Massachusetts driver's license listing his address as the Subject Premises. He also listed his email address as Elijah.buoi@sosudatech.com.

42. On the Newtek PPP Loan Application, Buoi claimed that Sosuda had 96 employees and an average monthly payroll of \$800,000. Buoi certified that the United States was the principal place of residence for those 96 employees.

43. In support of the Newtek PPP Application, Buoi submitted an IRS Form 941 purporting to reflect Sosuda's wages and federal payroll tax information for the first quarter of 2020. According to this document, Sosuda had 96 employees and paid \$2.4 million in wages, tips, and other compensation during that period. Buoi signed the IRS Form 941 as the President and CEO of Sosuda and provided a date of April 30, 2020.

44. Buoi also submitted an IRS Form 940 purporting to show Sosuda's total payments to employees for 2019. According to the IRS Form 940, Sosuda made \$9.6 million in payments to employees in 2019 and did not have employees in any other state except Massachusetts. Buoi signed the IRS Form 940 as the President and CEO of Sosuda and provided a date of January 31, 2020.

45. The Newtek PPP Loan Application was denied.

Inconsistencies in the PPP Loan Applications

46. Based on my training and experience and review of records in this case, including the inconsistent PPP loan applications described above, I believe that Buoi made materially false representations to Bank of America, Fountainhead, Fundbox, and Newtek, in order to wrongfully obtain PPP loan funds.

47. As set forth above, Buoi submitted at least four PPP loan applications on behalf of the same entity. In three of the four applications, Buoi provided different information concerning the number of Sosuda employees and the company's average monthly payroll. For example, in the Fountainhead PPP Loan Application, Buoi claimed that Sosuda had 18 employees and an average monthly payroll of \$150,000, but in the loan applications to Fundbox and Newtek, Buoi

claimed that Sosuda had 96 employees and an average monthly payroll of \$800,000, and in the loan application to Bank of America, Buoi claimed that Sosuda had 353 employees and an average monthly payroll of \$3 million.

48. With each PPP loan application, Buoi submitted payroll documentation in the form of an Excel spreadsheet. The spreadsheets provided no breakdown of Sosuda's employees or their specific salaries. As with the associated loan applications, three of the four spreadsheets contained very different average monthly payroll numbers.

49. I also compared the IRS Form 940s that Buoi provided in support of the four PPP loan applications, which likewise reflect inconsistencies that I believe are consistent with fraud.

50. All four forms purport to have been signed on January 31, 2020. On the IRS Form 940s provided to Fundbox and Newtek, Buoi indicated total payments to employees of \$9.6 million in 2019. On the IRS Form 940 provided to Fountainhead, Buoi indicated total payments to employees in that same period of just \$1.8 million, while in the IRS Form 940 provided to Bank of America, Buoi indicated total payments to employees of \$34.8 million.

51. Moreover, according to information obtained from Bank of America, Buoi initially did not include an IRS Form 940 with his Bank of America PPP Loan Application, which was the first of the four PPP loan applications he submitted. On or about April 28, 2020, in response to Bank of America's request for additional documentation, including an IRS Form 940, Buoi represented that Sosuda did not file federal tax returns in 2019, and therefore did not have an IRS Form 940 for 2019. Thereafter, however, on or about May 11, 2020, Buoi provided Bank of America with an IRS Form 940 purporting to be for the 2019 tax year, as well as an IRS Form 941 for the first quarter of 2020.

52. Furthermore, while Buoi indicated on each of the IRS Form 940s for 2019, that Sosuda's employees are located in Massachusetts, there is no record that Sosuda registered or filed Quarterly Wage-Earning reports with the Massachusetts Department of Unemployment Assistance ("DUA"), as an employer with employees in the state is required to do.

53. Likewise, three of the four IRS Form 941s that Buoi provided in support of his applications list a different number of employees and different amount in wages, tips and other compensation for the first quarter 2020. The form supplied to Bank of America indicated that Sosuda has 353 employees and wages, tips and other compensation in that period of \$9,498,987. The forms supplied to Fundbox and Newtek both indicated 96 employees and wages, tips and other compensation of \$2.4 million, while the form supplied to Fountainhead indicated 18 employees and wages, tips and other compensation of \$450,000.

54. Bank records for Sosuda Tech are also inconsistent with Buoi's claimed payroll expenses. A review of Bank of America's records for two accounts in the name of Sosuda Tech show no record of large expenditures on wages, which would be consistent with the submitted IRS Form 941s.

55. Based on the inconsistencies set forth above, and Buoi's representation to Bank of America that Sosuda did not file a federal tax return in 2019 and did not have an IRS Form 940, and the bank account information reflecting an absence of wage payments consistent with his reported monthly expenditures, I believe the IRS forms Buoi submitted in support of his PPP loan applications are fraudulent.

To the Extent Sosuda Has Employees, They Appear to Be Overseas

56. As set forth above, on each of the four PPP loan applications, Buoi certified that the United States was the primary residence for Sosuda's employees.

57. Public information and records obtained from Bank of America suggest that, to the extent Sosuda has employees other than Buoi, they are located outside of the United States.

58. Specifically, on or about June 18, 2020, I reviewed Sosuda's LinkedIn page, which represents that the company has six employees, including Buoi, and that the other five employees are located in India.

59. According to information obtained from Bank of America, when asked for additional payroll documentation, Buoi indicated that approximately 50 percent of Sosuda's employees are overseas.

60. Records for BOA Account 2641 show that on or about April 21, 2020, Sosuda received \$10,000 from the U.S. Department of Treasury.⁷ On or about April 30, 2020, \$7,300 was transferred by wire from BOA Account 2641 to an account in India in the name of Sosuda Tech Private Limited, with the memo: payroll.⁸

PROBABLE CAUSE FOR SEIZURE WARRANTS

Disbursement and Movement of the PPP Loan Funds from Fundbox

61. A review of available bank records for BOA Account 0252 and BOA Account 2461 reveals the following transaction history. This review is ongoing.

62. On June 15, 2020, a \$2 million deposit was made into BOA Account 2461 from Fundbox as a result of Buoi's Fundbox PPP Loan Application. As set forth above, there is probable

⁷ In addition to the PPP loan program, under the CARES Act, SBA is authorized to issue advances of up to \$10,000 to small businesses in connection with a small business's application for an Economic Injury Disaster Loan ("EIDL"). The amount of the advance is determined by the number of employees the applicant certifies having and is capped at \$10,000. According to information obtained from the SBA, Sosuda also applied for an EIDL.

⁸ Public information indicates that Sosuda Tech Private Limited is registered in India as a subsidiary of a foreign company and has an address in Uttar Pradesh, India.

cause to believe that this \$2 million deposit represents proceeds traceable to wire fraud, in violation of 18 U.S.C. § 1343.

63. Prior to this deposit, BOA Account 2461 had a balance of \$536.07. As of June 17, 2020, no other deposits have been made to BOA Account 2461, although there have been a number of withdrawals. As of June 17, 2020, the balance of BOA Account 2461 was approximately \$772,563.71.

64. Before June 15, 2020, BOA Account 0252 had a balance of \$285.93. On or about June 15, 2020, after the \$2 million in loan proceeds was deposited into BOA Account 2461, two transfers were made from BOA Account 2461 to BOA Account 0252. The first transfer was in the amount of \$900,000, and the second transfer was in the amount of \$300,000, for a total of \$1.2 million. As of June 17, 2020, BOA Account 0252 had a balance of \$1,200,285.93.

65. On or about June 15, 2020, Buoi withdrew approximately \$7,000 in cash from BOA Account 2641. Additionally, Buoi sent a \$20,000 wire to Sosuda Tech Private Limited, in India.

66. The \$1.2 million transferred to BOA Account 0252 represents fraud proceeds, as it is traceable to a portion of the \$2 million in proceeds deposited into BOA Account 2461 on or about June 15, 2020. In addition, up to \$772,000 in proceeds remained in BOA Account 2461.

67. Bank of America has frozen both BOA Account 0252 and BOA Account 2461. Based upon my training and experience, this bars the account holder from transferring funds out of the account. As such, no further movement of funds has occurred.

68. In sum, probable cause exists to believe that Buoi committed wire fraud and that the proceeds of this offense were sent to BOA Account 2461 and then a portion of those same fraud proceeds was moved to BOA Account 0252.

69. As reflected by the transaction history set forth above, probable cause exists to believe that up to \$1.2 million, currently held by Bank of America in, or on behalf of, BOA Account 0252, and up to \$772,000, currently held by Bank of America in, or on behalf of, BOA Account 2641, are proceeds traceable to wire fraud. Accordingly, probable cause exists to believe that the Funds are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

70. This Court has authority to issue a seizure warrant pursuant to 18 U.S.C. § 981(b)(2), which states that “[s]eizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure.” This Court also has authority to issue the requested seizure warrants pursuant to 21 U.S.C. § 853(f), as incorporated by 28 U.S.C. § 2461(c), which authorizes “the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant.”

71. This Court has jurisdiction to enter the requested seizure warrant in the District of Massachusetts because a forfeiture action may be filed in this District. *See* 28 U.S.C. § 1355 (“A forfeiture action or proceeding may be brought in— (A) the district court for the district in which any of the acts or omissions giving rise to the forfeiture occurred, or (B) any other district where venue for the forfeiture action or proceeding is specifically provided for ...”); Fed. R. Crim. P. 41(b) (magistrate judge has authority to issue a warrant to seize property “located in the district” and, “in any district where activities related to the crime may have occurred[, to] issue a warrant for property that is located outside the jurisdiction of any state or district....”).

72. A restraining order, pursuant to 21 U.S.C. § 853(e), will not be sufficient to preserve the assets in question given the ease with which funds may move out of the accounts via wire

transfer, electronic funds transfer, or otherwise, and despite best intentions, financial institutions cannot guarantee that money restrained, but not seized, will be available for forfeiture at a later time.

73. In addition, pursuant to 18 U.S.C. § 984(b), the government is entitled to forfeit any funds in an account to which illegal proceeds were deposited within the last year without tracing those funds directly to the offense, even if the other deposited funds may not be illegal proceeds.

***THE PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES
OF THE TARGET OFFENSES***

74. I also have probable cause to believe the Subject Premises contain evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachment B. Specifically, I believe that the Subject Premises will contain banking information, business records, and communications, located in hard copy documents and/or on computer equipment⁹, which will contain evidence of the Target Offenses.

Buoi Lives at the Subject Premises, Sosuda's Business Address

75. From on or about June 16, 2020 to on or about June 18, 2020, the FBI conducted surveillance at the Subject Premises. A white 2019 Toyota Camry, bearing a Massachusetts license plate with the number 8YW359 and a red 2016 Toyota Corolla, bearing a Massachusetts license plate with the number 2TAL41 were observed parked in front of the Subject Premises. According to the Massachusetts RMV, Buoi is the registered owner of both vehicles. Additionally, Buoi's driver's license lists the Subject Premises as his address.¹⁰

⁹ As defined in this Affidavit and in Attachment B, "computer equipment" includes mobile phones and smartphones. As most phones now operate with the functionality and computing power that was traditionally associated with much larger devices, for purposes of the affidavit these terms are used interchangeably.

¹⁰ Buoi is believed to reside at the Subject Premises with his wife and four children who are between the approximate ages of 11 through 18.

76. As noted above, Buoi advertises the Subject Premises as Sosuda's business address. It is the only address listed on the company's website. The Subject Premises is listed as Sosuda's address on each of the IRS Form 941s that Buoi submitted in support of the above-referenced loan applications and is also listed on bank statements for BOA Account 2641 and 0252.

Probable Cause to Believe the Subject Premises Contains Computer Equipment Used to Commit the Target Offenses

77. The investigation to date has shown that Buoi used computer equipment in the course of submitting the fraudulent PPP loan applications and committing the Target Offenses.

78. First, the PPP loan applications were filled out and submitted electronically. As set forth above, the fact that there are multiple versions of the same IRS forms, all purportedly signed by Buoi on the same date, suggests that the files were digitally manipulated in connection with each application.

79. Second, records from Bank of America, Fountainhead, Fundbox and Newtek indicate that all four loan applications were submitted from IP address 24.147.239.156, owned by Comcast Cable Solutions LLC ("Comcast"). Comcast subscriber records establish that the IP address is assigned to Buoi at the Subject Premises.

80. Third, records indicate that the Subject Premises is the billing address for Buoi's mobile phone. A review of Buoi's phone records reveal that he placed a large volume of calls to various banks. For example, between April 24, 2020 and June 8, 2020, he placed 67 calls to Bank of America, and between June 11, 2020 and June 17, 2020, he placed at least six calls to Fundbox.

81. Fourth, I am aware based on my training and experience that individuals who receive money from illegal activities such as bank fraud and wire fraud, as described above, often communicate with other individuals, who direct the flow of funds, providing specific instructions

on the manner, means, and timing of the transfer of the funds. These communications often occur via smart phones, including by voice, email, text messages, and messaging apps.

82. Fifth, I am also aware that banking activities, including transfers, can be conducted remotely via browsers on mobile phones or via applications or “apps” on devices.

83. Sixth, I am aware based on my training and experience that persons engaged in fraud frequently retain records of their transactions within the place of business or other places under their control. These records may be in the form of written notes and correspondence, receipts, negotiated instruments, contracts, bank statements, and other records. Persons engaged in financial crimes often maintain such records for an extended period of time, particularly when they are involved in ongoing criminal conduct. There are many reasons why criminal offenders maintain evidence for long periods of time. To the offender, the evidence may seem innocuous at first glance (*i.e.*, client or employee lists, financial, credit card, and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. In addition, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden, or further destroyed computer-related evidence, which fact, may be retrievable by a trained forensic expert.

84. Finally, individuals engaged in a legitimate income producing business typically retain records of the financial activities of the business in order to provide such information to their

accountant/return preparer in order to complete financial statements and tax returns. In this regard, it is possible that Sosuda maintained payroll and tax records related to how it compensated its U.S. and foreign employees, to the extent they exist.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

85. From my training, experience, and information provided to me by other agents, I am aware that businesses frequently use computers to carry out, communicate about, and store records about their business operations. These tasks are frequently accomplished through sending and receiving business-related email and instant messages; drafting other business documents such as spreadsheets and presentations; scheduling business activities; keeping a calendar of business and other activities; arranging for business travel; storing pictures related to business activities; purchasing and selling inventory and supplies online; researching online; and accessing banking, financial, investment, utility, and other accounts concerning the movement and payment of money online.

86. From my training, experience, and information provided to me by other agents, I am also 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.

87. 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.

88. 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.

89. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files generated at or to be used at a business, such as e-mail, word-processing documents, photographs, and spreadsheets.

90. From my training, experience, and information provided to me by other agents, I am aware that businesses and individuals commonly store records of the type described in Attachment B in computer hardware, computer software, smartphones, and storage media.

91. As set forth above, I believe that Buoi falsified both IRS Forms and payroll records in support of his PPP loan applications to four different lenders. As such, I believe Buoi's personal and/or work computer will contain evidence of the Target Offenses.

92. Based on my knowledge, training, experience, and information provided to me by 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, and in particular, computers' internal hard drive, 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 inculcating 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 inculcate 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.

j) In addition, based on my knowledge, training, and experience, I know that businesses and businesspeople often retain correspondence, financial, transactional, and other business records for years to identify past customers and vendors for potential future transactions; keep track of business deals; monitor payments, debts, and expenses; resolve business disputes stemming from past transactions; prepare tax returns and other tax documents; and engage in other business-related purposes. 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:

- 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.
- 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.”

93. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

94. The 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 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.

95. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) Buoi. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

- a) In this case, I recognize that Sosuda may perform some legitimate business functions, and that seizing computer equipment may have the unintended and undesired effect of limiting the company's ability to function. As stated above, there are a variety of reasons why law enforcement agents might need to seize the computer equipment for subsequent processing elsewhere. If Sosuda requires access to data that is not contraband or evidence of a crime, the government will work with the company after the search to copy this data onto storage media provided by the company for the company's use.
- b) If the search team determines that there is no reason to seize certain of Sosuda's computer equipment during the execution of this warrant, the team will create an onsite electronic "image" of those parts that are likely to store data specified in the warrant, if imaging is practical. Generally speaking, imaging is the taking of a complete electronic picture of the data, including all hidden sectors and deleted files. Imaging permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer equipment. However, imaging at the premises can often be impractical, because imaging is resource-intensive: it can take hours or days, thus requiring law enforcement agents to remain at the premises for much longer than they

would remain if they seized the items, and it can require personnel with specialized experience and specialized equipment, both of which might be unavailable. If law enforcement personnel do create an image at the premises, they will then search for the records and data specified in the warrant from the image copy at a later date off-site.

96. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CONCLUSION

97. Based on the information described above, I have probable cause to believe that that Buoi has committed the Target Offenses and that evidence, fruits, and instrumentalities of the Target Offenses, described in more detail in Attachment B, are located at the Subject Premises, described in Attachment A.

98. Finally, I have probable cause to believe that the Funds located in BOA accounts ending in 2461 and 0252 are proceeds traceable to wire fraud and that they are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).


Sworn to under the pains and penalties of perjury.

Respectfully submitted,



Sheila Magoon, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 19th day of June, 2020. 6:43 p.m.


David H. Hennessy
United States Magistrate Judge

