UNITED STATES DISTRICT COURT

for the

Eastern District of California

FILED
Feb 18, 2025
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

SEALED

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE EMAIL ADDRESS AKASH@ALBOT.IO THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION USA

Case No. 2:25-sw-0136 JDP

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

SEE ATTACHMENT A, attached hereto and incorporated by reference,

located in the Western District of Washington, there is now concealed:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 1344	Bank fraud
18 U.S.C. § 1957	Conducting financial transactions with proceeds of unlawful activity

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Marshall Miller
Applicant's signature

Marshall Miller, IRS-CI Special Agent
Printed name and title

Sworn to and signed telephonically.

Date: February 18, 2025

Judge's signature

City and state: Sacramento, California

Jeremy D. Peterson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Marshall Miller, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Microsoft Corporation USA ("Microsoft"), an internet service and email service provider headquartered at 1 Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in Attachment A, hereby incorporated by reference. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B (hereby incorporated by reference), government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with Internal Revenue Service-Criminal Investigation, and have been since 2018. My duties include the investigation of criminal violations of the Internal Revenue Code, anti-money laundering statutes, and other related offenses. My professional training consisted of approximately twenty-six weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, which included training in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search, seizure, and arrest warrants. I have also received training in financial investigative techniques, legal principles, and statutes representing criminal violations of the United States Code as enumerated in Titles 18, 26, and 31. Furthermore, I have a master's degree in accounting from the University of California at Davis and a bachelor's degree in criminology from the University of California at Irvine.

3. I have led or been involved in numerous investigations of money laundering, health-care fraud, wire fraud, bank fraud, conspiracy, tax evasion, and other related offenses. I

have led or participated in numerous interviews, and have been the affiant for multiple federal search warrants involving suspected criminal violations where records of the type involved in this investigation were seized. I have personally authored affidavits in support of warrants for the seizure of property that constituted the proceeds of money laundering or fraud under the forfeiture statutes found within Title 18 of the United States Code. I have personally traced the proceeds of fraud between financial accounts, utilizing various accounting methods to determine the balance of fraud proceeds held within certain accounts on a given date.

4. Based on my training and experience and that of others with whom I work, I am familiar with the methods and practices used by individuals and organizations engaged in financial crimes. These individuals often maintain records of their financial activities, such as bank records, receipts, and documentation of expenditures, notes, or correspondence, negotiated instruments, contracts, and other financial documents, within their email accounts. I am aware that individuals engaged in financial crimes commonly participate in these activities for profit. It is common for the proceeds of financial crimes to be in the form of cash, negotiable instruments, or other assets. Furthermore, it is common for persons engaging in financial crimes to invest the profits in other assets, reduce current or long-term liabilities, convert the profits to other forms of financial instruments, and/or pay personal expenditures. I am aware that such transactions, transfers, or expenditures of criminally derived profits cause the creation of numerous types of documents, which reflect the fruits of financial crimes. Documents such as bank records, cashier's check records, receipts, invoices, expenditure records, escrow documents, notes or notations, and other similar documents are generated upon the transactions, transfers, and/or expenditures of criminally derived funds. I know from training and experience, and the experience of other law enforcement officers with whom I work, that correspondence or records related to these financial activities are commonly kept in the email accounts of individuals engaging in criminal activity.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. §§ 1343, 1344, and 1957 have been committed by Akash Kumar Singh ("Singh") using the email address akash@albot.io (the "Target Account"). I further submit that there is probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

7. The Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. *Id.* § 2711(3)(A)(i).

II. FACTS ESTABLISHING PROBABLE CAUSE

A. Summary of Investigation and Scope of Requested Warrant

8. Singh purports to be the head of two corporations operating in California: Kryptoblocks Inc. ("Kryptoblocks") and Albot Technologies ("Albot"). In summary, evidence obtained to date by the government indicates that Singh used his status as Chief Executive Officer of Kryptoblocks to apply for and obtain from a federally insured financial institution called KeyPoint Credit Union ("KeyPoint") more than $3 million in subsequently forgiven loans that were earmarked for COVID-19 relief to small businesses meeting certain requirements.[1]

9. In support of his applications, Singh submitted a range of apparently fraudulent documentation, including Internal Revenue Service ("IRS") forms that were never actually filed with that agency, payroll spreadsheets containing names and wages of employees who apparently resided outside the United States, and more. Singh's fraudulent loan applications indicated that the Target Account was the contact email address for Singh in his capacity as CEO of Kryptoblocks. Additionally, Singh used the Target Account to correspond with KeyPoint personnel about and in furtherance of his fraudulent loan applications.

[1] Per information made available online by the National Credit Union Administration, KeyPoint is federally insured by that entity.

10. After Singh obtained millions of dollars in pandemic loans to Kryptoblocks from KeyPoint, he transferred much of the proceeds through personal bank accounts and corporate bank accounts linked to Kryptoblocks and Albot that he controlled. Singh spent a substantial portion of the loan proceeds he received on expenditures that were not authorized by the applicable loan program's rules, such as personal expenses, residential mortgage payments, luxury goods, travel-related expenses, and transfers to individuals located overseas.

11. The warrant for which I am applying would authorize law enforcement to search the contents of the Target Account in order to seize evidence relating to Singh's fraud and connecting Singh to the use of that account to perpetrate his fraud.

B. Background on Paycheck Protection Program

12. At all relevant times, the United States Small Business Administration (the "SBA") operated the Paycheck Protection Program (the "PPP"), a congressionally mandated program through which third-party lenders like KeyPoint funded forgivable loans to businesses in the United States affected by the COVID-19 pandemic. These loans were guaranteed by the United States Treasury and overseen by the SBA.

13. PPP rules required prospective borrowers to certify, among other things:

a) That an applicant business was in operation on February 15, 2020;

b) That it employed workers for whom it paid salaries and payroll taxes or paid independent contractors as reported on IRS Form 1099-MISC;

c) That the principal places of residence for employees of the applicant business were in the United States;

d) The accuracy of the average monthly payroll expenses and number of employees of the applicant business; and

e) The accuracy of information and documents submitted in support of the loan application.

14. PPP rules provided that loan proceeds could only be used for business payroll costs, business rent or mortgage costs, business utilities, or other business expenses.

15. In general, successful applicants for PPP loans received their loan proceeds directly from the financial institutions that processed their loan applications, and on terms that required the loans to be repaid over time at a low interest rate (around 1%). Loan recipients who demonstrated that they spent loan proceeds on allowable business expenses could seek to have their PPP loans entirely forgiven.

16. PPP rules required borrowers seeking forgiveness of their loans to certify, among other things:

a) That PPP loan proceeds had been used to pay business costs eligible for forgiveness, such as payroll costs to retain employees, business utility payments, covered worker protection expenditures, and the like;

b) That at least 60% of the amount for which the borrower sought forgiveness consisted of payroll costs;

c) That the borrower verified the accuracy of the eligible payroll and nonpayroll costs for which forgiveness was sought; and

d) The accuracy of information and documents submitted in support of the forgiveness application.

17. Applicants seeking PPP loans and their subsequent forgiveness generally submitted their applications directly to third-party financial institutions, such as KeyPoint, using the internet.

C. Singh successfully applied for a PPP loan of $1.4 million.

18. In or around April 2020, KeyPoint received an application for a PPP loan to Kryptoblocks (the "First Draw" loan) that purported to be submitted by Singh. In support of this application, Singh represented the following, among other things:

a) He was the Chief Executive Officer and sole owner of Kryptoblocks;

b) The Target Account was the email address associated with Kryptoblocks's application;

///

c) The business phone number associated with the application was 650-391-8550 (the "8550 number");[2]

d) The taxpayer identification number associated with the application was Singh's personal Social Security Number;

e) The principal place of business for Kryptoblocks was Singh's residence in Sacramento;

f) Kryptoblocks employed eighty-four people, with an average monthly corporate payroll of over $570,000;

g) The United States was the principal place of residence for all employees used to calculate Kryptoblocks's payroll; and

h) Any loan proceeds would be used for Kryptoblocks's payroll, rent or mortgage interest, or utilities.

19. In support of his application, Singh submitted what purported to be a true and accurate IRS Form W-3 showing that Kryptoblocks paid employee wages of more than $9 million in 2019 and withheld more than $1.3 million in federal income tax in 2019. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024.

20. In or around May 2020, KeyPoint approved Singh's First Draw loan application and funded a loan of $1,426,847.00 to Kryptoblocks. KeyPoint deposited the First Draw loan proceeds via interstate wire into a Kryptoblocks corporate bank account held at Bank of America, the account number for which ended in 8845 (the "8845 account").[3] According to records provided by Bank of America, Singh opened the 8845 account in Sacramento in November 2019 and was the sole signatory on the account. At the time the First Draw loan

[2] According to records obtained by investigative personnel from Sprint, Singh was the owner of the 8550 number through at least April 2020.

[3] The investigation indicates this wire was made using Fedwire, a system operated by the Federal Reserve. I am aware, based upon my training, experience, and consultation with others, that Fedwire transactions since 2015 involve two separate computer servers, one in Texas, and the other in New Jersey.

proceeds were deposited into the 8845 account, the 8845 account had a balance of less than $5,000.

21. Between May 2020 and August 2021, according to records provided to investigators for the 8845 account and for other financial accounts associated with Singh, Singh spent the majority of the First Draw loan proceeds on a variety of expenditures that were not authorized for PPP funds. These expenditures included regular payments on Singh's home mortgage; over $1 million in direct transfers to individuals located in India; incidentals such as food, clothing, transportation, and luxury goods; and other personal expenses.

22. Based on the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. §§ 1343 and 1344 by submitting a PPP loan application to a federally insured credit union that contained material misrepresentations and that involved an interstate wire transmission.

1. Forgiveness of First Draw Loan

23. In or around October 2021, KeyPoint received an application for forgiveness of the First Draw loan issued to Kryptoblocks, which again purported to be submitted by Singh. In support of his forgiveness application, Singh represented the following, among other things:

a) The Target Account was the email address associated with Kryptoblocks's application;

b) The 8550 number was the business phone number associated with Kryptoblocks's application;

c) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;

d) The business address for Kryptoblocks was Singh's residence in Sacramento;

e) At the time of its application for forgiveness of the First Draw loan, Kryptoblocks employed ninety people; and

f) Between May and October 2020, Kryptoblocks paid out $1,426,847.00 for payroll costs to employees whose principal places of residence were in the United States.

24. To substantiate the certifications made on the application for forgiveness of the First Draw loan, Singh used the Target Account to send KeyPoint personnel what purported to be true and accurate documents, including the following:

a) An IRS Form 940 for 2020 bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid $9.2 million in wages, requiring it to remit $3,738 to the IRS in federal unemployment tax that year;

b) An IRS Form 941 for the second quarter of 2020, bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid more than $2 million in employee wages that quarter and withheld more than $650,000 in federal income tax that same quarter;

c) An IRS Form 941 for the third quarter of 2020, bearing Singh's name and the 8550 number and purporting to show that Kryptoblocks paid more than $2 million in employee wages that quarter and withheld more than $650,000 in federal income tax that same quarter; and

d) A spreadsheet purporting to show that Kryptoblocks employed eighty-eight people to whom it paid more than $9 million in wages (along with associated federal and California taxes) in 2019 and $3 million in wages (along with associated federal and California taxes) in 2020, including approximately $110,000 paid to Singh himself, $106,000 paid to Singh's wife Neelam Singh, and $95,000 paid to Singh's brother Neeraj Masih.[4]

25. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. Additionally, according to records obtained by investigators from the California Employment Development Department (the "EDD"), Kryptoblocks did not report any wages paid to employees in California in 2020. And according to information provided to investigators by the California Franchise Tax

[4] Singh reported that Neelam Singh was his spouse and that Neeraj Masih was his brother on tax returns filed with the IRS that were reviewed as part of this investigation.

Board (the "FTB"), Kryptoblocks did not file a corporate tax return in California for 2019 or 2020. Furthermore, according to bank records for the 8845 account, Singh did not make any payments to tax authorities from this account in 2019 or 2020.

26. In or around October 2021 and based on Singh's representations in support of his First Draw loan forgiveness application, KeyPoint requested that the SBA forgive the First Draw loan previously extended to Kryptoblocks. That same month, the SBA forgave the First Draw loan in full.

27. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1344 by submitting the false First Draw loan forgiveness application to KeyPoint.

D. Singh successfully applied for a second PPP loan of $1.9 million.

28. In or around January 2021, Singh submitted an application to KeyPoint for a subsequent PPP loan to Kryptoblocks (the "Second Draw" loan). In support of his application, Singh represented the following, among other things:

a) He was the Chief Executive Officer and sole owner of Kryptoblocks;

b) The Target Account was the email address associated with Kryptoblocks's application;

c) The business phone number associated with the application was the 8550 number;

d) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;

e) The principal place of business for Kryptoblocks was an address in an office building on Promenade Circle in Sacramento, which is located less than two miles from Singh's residence and which currently houses a lending company doing business as Regional Finance;

f) Kryptoblocks employed eighty-nine people;

g) Kryptoblocks maintained an average monthly payroll of approximately $838,911.00;

h) Kryptoblocks sought a Second Draw loan to pay for eligible payroll costs, rent/mortgage interest, utilities, and covered operations expenditures;

i) The United States was the principal place of residence for all employees included in Kryptoblocks's payroll calculation; and

j) Kryptoblocks used its First Draw loan proceeds only on eligible expenses.

29. In support of the Second Draw loan application, Singh used the Target Account to submit a bank statement for the 8845 account displaying Singh's residential address as the contact address for Kryptoblocks and demonstrating the withdrawal of approximately $86,000 from that account in January 2021.

30. KeyPoint's loan file for the Second Draw loan also includes the following documents:

a) An IRS Form 940 for 2019 displaying Singh's residence address and the 8550 number, and purporting to show that Kryptoblocks paid $9.2 million in wages;

b) An IRS Form W-3 for 2019 displaying the Target Account and the 8550 number, and purporting to show that Kryptoblocks paid more than $9 million in wages and withheld more than $1.3 million in federal income tax that year;

c) A purportedly true and accurate profit-and-loss statement showing that Kryptoblocks generated more than $17 million in net revenue in 2019 and more than $12 million in net revenue in 2020; and

d) A purportedly true and accurate spreadsheet showing that Kryptoblocks employed eighty-eight people to whom it paid more than $9 million in wages (along with associated federal and California taxes) in 2020, including to Singh himself, Singh's wife, and Singh's brother.

31. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. Additionally, according to records obtained by investigators from the EDD, Kryptoblocks did not report making any wage payments to California employees in 2020. And according to records obtained

by investigators from the FTB, Kryptoblocks did not file a California corporate tax return for 2019 or 2020.

32. In or around March 2021, KeyPoint approved Singh's Second Draw loan application and funded a loan of $1,990,152.00 to Kryptoblocks. KeyPoint deposited these Second Draw loan proceeds via interstate wire into a Kryptoblocks corporate bank account held at Bank of America, the account number for which ended in 5717 (the "5717 account").[5] According to records received from Bank of America, Singh opened the 5717 account in Sacramento in May 2020 and was the sole signatory on the account. At the time the Second Draw loan proceeds were deposited into the 5717 account, that account had a balance of less than $2,500.

33. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. §§ 1343 and 1344 by submitting a PPP loan application to a federally insured credit union that contained material misrepresentations, and that involved an interstate wire transmission.

1. Expenditures of Second Draw Loan Proceeds

34. Between March 2021 and February 2022, nearly all of the proceeds Kryptoblocks received from the Second Draw loan were spent from the 5717 account. According to records provided to investigators for the 5717 account, Singh spent some of the Second Draw loan proceeds on expenditures that could qualify as legitimate uses of PPP funds, such as payments to business solutions providers like Amazon Web Services, Apple, Google, Atlassian, and the like.

35. However, according to records provided to investigators for the 5717 account and for other financial accounts associated with Singh, Singh spent much of the Second Draw loan proceeds on a variety of expenditures that do not appear to have been authorized for PPP funds. These expenditures included:

///

[5] This transaction was made using Fedwire and, accordingly, involved an interstate wire transmission.

a) Hundreds of thousands of dollars in transfers to an Albot corporate bank account for which Singh was the sole signatory;

b) Transfers to other companies such as engineering and biosciences firms, one of which issued a press release in or around June 2021 touting its partnership with Albot to distribute COVID-19 diagnostic testing kits;

c) Tens of thousands of dollars of transfers to a personal banking account held at Bank of America on which Singh and his wife were the sole signatories;

d) An approximately $500,000 payment to Singh's home mortgage lender; and

e) Incidentals such as food, clothing, and luxury goods.

36. I conducted a tracing of the proceeds of Kryptoblocks' Second Draw loan using an accounting method approved by the Money Laundering and Asset Recovery Section of the United States Department of Justice. This tracing analysis revealed that the approximately $500,000 payment to Singh's mortgage lender necessarily contained greater than $10,000 of the proceeds of Singh's fraudulent conduct in obtaining the Second Draw loan. Thus, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1957 by conducting this financial transaction using more than $10,000 in proceeds from his fraudulent scheme.

2. Forgiveness of Second Draw Loan

37. In or around February 2022, Singh submitted an application to KeyPoint for forgiveness of the Second Draw loan issued to Kryptoblocks. In support of his forgiveness application, Singh certified the following, among other things:

a) The Target Account was the email address associated with Kryptoblocks's application;

b) The business phone number associated with the application was the 8550 number;

c) The taxpayer identification number associated with the application was Kryptoblocks's federal Employer Identification Number;

d) The principal place of business for Kryptoblocks was Singh's residence in Sacramento;

e) At the times of its applications for the Second Draw loan and for its subsequent forgiveness, Kryptoblocks employed 101 people;

f) Between March and September 2021, Kryptoblocks paid its employees over $5 million in wages; and

g) Kryptoblocks used its Second Draw loan for payroll costs paid to employees.

38. To substantiate the certifications he made on his application for forgiveness of the Second Draw loan, Singh used the Target Account to submit to KeyPoint personnel what purported to be true and accurate copies of various documents, including the following:

a) An IRS Form 941 for the first quarter of 2021, displaying Singh's residence address and the 8550 number and purporting to show that Kryptoblocks paid more than $2.6 million in employee wages that quarter and withheld more than $744,000 in federal payroll taxes that same quarter;

b) An IRS Form 941 for the second quarter of 2021, displaying Singh's residence address and the 8550 number and again purporting to show that Kryptoblocks paid more than $2.6 million in employee wages that quarter and withheld more than $744,000 in federal payroll taxes that same quarter;

c) An IRS Form 941 for the third quarter of 2021, displaying Singh's residence address and the 8550 number and again purporting to show that Kryptoblocks paid more than $2.6 million in employee wages that quarter and withheld more than $744,000 in federal payroll taxes that same quarter; and

d) A spreadsheet purporting to show that Kryptoblocks employed ninety-nine people to whom it paid more than $10 million in wages (along with associated federal and California taxes) in 2021, including more than $110,000 paid to Singh himself, more than $106,000 paid to Singh's wife, and more than $95,000 paid to Singh's brother.

39. However, according to records maintained by the IRS, Kryptoblocks did not report any income, payroll, or employees to the IRS between 2016 and 2024. And according to

records obtained by investigators from the EDD, Kryptoblocks did not report making any wage payments to employees in 2021. Additionally, according to information provided to investigators by the FTB in 2022, Kryptoblocks did not file a corporate tax return with the State of California for 2021. Furthermore, according to bank records for the 8845 account and the 5717 account, Singh did not make any payments to tax authorities from these accounts in 2020 or 2021.

40. In or around March 2022 and based on Singh's representations in support of his Second Draw loan forgiveness application, KeyPoint requested that the SBA forgive the Second Draw loan previously extended to Kryptoblocks. In April 2022, the SBA forgave the Second Draw loan in full.

41. Based upon the foregoing, I submit that probable cause exists to believe that Singh violated 18 U.S.C. § 1344 by submitting a false Second Draw loan forgiveness application to KeyPoint.

E. <u>The Target Account is associated with loan applications submitted to other financial institutions.</u>

42. Investigators requested and received records from other financial institutions regarding financial applications linked to Singh and the Target Account. I reviewed these records, which, in summary, revealed the following:

a) In or around March 2020, the SBA received an application for an Economic Injury Disaster Loan to Kryptoblocks that displayed Singh's home address, Social Security Number, date of birth, the 8550 number, and the Target Account;

b) In or around April 2020, Singh submitted a PPP loan application from Kryptoblocks to a financial institution doing business as Ready Capital that displayed Singh's name, residential address, the 8550 number, and the Target Account;

c) In or around March 2021, Singh submitted a PPP loan application to Northeast Bank on behalf of Albot that displayed his name and Social Security Number, the Promenade Circle address, the 8550 number, and the Target Account;

d) In or around February and March of 2021, the Target Account corresponded with personnel from a financial lender associated with Northeast Bank regarding a PPP loan application;

e) In or around March 2021, the SBA received an application for an Economic Injury Disaster Loan to Albot that displayed Singh's home address, Social Security Number, date of birth, the 8550 number, and the Target Account;

f) In or around February 2022, Singh submitted a credit application to Mechanics Bank for a vehicle loan that displayed Singh's home address, California driver license, the purported Kryptoblocks headquarters address on Promenade Circle, the 8550 number, and the Target Account; and

g) In or around March 2022, the Target Account corresponded with KeyPoint personnel regarding an application by Kryptoblocks for a small business loan known as an SBA 7(a) loan.

F. Facts Regarding Relevant Identifiers

43. In or around late 2022, investigators received records from Sprint regarding the 8550 number. These records revealed that the 8550 number was created in 2019 and that for at least between January and April 2020, the customer of record for the 8550 number was Akash Singh at an address on Riggs Avenue in Sacramento.

44. According to records maintained by the SBA regarding PPP loan applications submitted by Kryptoblocks, Singh's California driver record listed this Riggs Avenue address as his residence in 2018. In November 2019, Singh also listed this Riggs Avenue address as his then-current address on his mortgage loan application for his residence on Amelia Earhart Avenue in Sacramento.

45. In late 2024, investigators received records from Google regarding any Google accounts associated with the email address akash@albot.io as well as with the email address

///

///

akash.labs@gmail.com.[6] These records revealed the following about the Google account associated with the email address akash@albot.io:

a) The account was created on or about March 2, 2020, in the name "akash singh" and with the recovery email address of akash.labs@gmail.com;

b) The account was last updated in or around December 2024;

c) In or around October 2024, a number of Google services were removed from the account, including Gmail, Google Chat, Google Calendar, Google Drive, and more; and

d) Google has no record of any communication headers associated with the account.

46. The records received from Google also revealed the following about the Google account associated with the email address akash.labs@gmail.com:

a) The account was created on or about August 19, 2013, in the name of "Akash Singh" and with the 8550 number as the associated contact and recovery SMS number;

b) The account was last updated in November 2024; and

c) Google maintains email header records for the account indicating that it was copied on emails that were also sent to the Target Account.

47. Google operates a tool on the internet that analyzes email header data and is publicly available at https://toolbox.googleapps.com/apps/messageheader/. On or about January 30, 2025, I ran the headers of emails sent from the Target Account to KeyPoint personnel in 2021 and 2022 through this header analyzer tool. For some of these emails, the header analyzer tool did not return an output indicating the source domain of the emails. But for two of the emails sent from the Target Account to KeyPoint personnel in April 2022, the header analyzer tool returned an output indicating that the emails sent from the Target Account originated from

[6] Singh's name, the email address akash.labs@gmail.com, and the 8550 number each appear at the top of a *curriculum vitae* submitted by the Target Account to KeyPoint personnel in or around March 2022 in connection with an apparently aborted application for a SBA 7(a) loan.

computers associated with domains ending in prod.outlook.com. Based on my training and experience, I know this domain to be associated with Microsoft's email communication solutions such as Outlook and Microsoft Office 365, which is an email communication platform operated by Microsoft.

48. In or around November 2024, investigators requested and received records regarding the domain albot.io from an internet hosting provider doing business as Cloudflare. These records indicated that the domain was created in December 2023 and registered to an individual with the initials R.G. at an address in Colchester, Great Britain.

49. On or around January 22, 2025, I submitted a preservation request to Microsoft requesting that it preserve the contents of the Target Account. Based on my training and experience, I know that in general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft servers for a certain period of time.

III. BACKGROUND CONCERNING EMAIL

50. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including email access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name Microsoft.com and that are associated with a custom domain name, like the Target Account. This service offered by Microsoft is sometimes referred to as "Office 365."

51. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience,

such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

52. A Microsoft Office 365 subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

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

54. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

55. In addition, email providers often have records of the Internet Protocol address (the "IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address,

IP address information can help to identify which computers or other devices were used to access the email account.

56. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

57. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

58. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner.

///

59. Additionally, information stored at the user's account may indicate the geographic location of the account user at a particular time (such as location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offenses under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (for instance, communications relating to the crime), or consciousness of guilt (for example, deleting communications in an effort to conceal them from law enforcement).

IV. CONCLUSION AND REQUEST FOR SEALING

60. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Microsoft.

61. Based on the foregoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

///

///

///

///

///

///

///

///

///

///

///

///

///

62. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

/s/ Marshall Miller
Marshall Miller
Special Agent
Internal Revenue Service-Criminal Investigation

Subscribed and sworn to telephonically on: February 18, 2025

THE HONORABLE JEREMY D. PETERSON
United States Magistrate Judge

/s/ Sam Stefanki
Approved as to form by AUSA SAM STEFANKI

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email address akash@albot.io that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation USA, a company headquartered at 1 Microsoft Way, Redmond, Washington 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to Be Disclosed by Microsoft Corporation USA (the "Provider")

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

1. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

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

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

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

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1343, 1344, or 1957, those violations involving Akash Kumar Singh and occurring after March 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Communications and records that discuss or otherwise show the user(s) of the target accounts and any company or entity affiliation or employment of that person or persons, including all communications and records relating to or purporting to be on behalf of the following:

a) Kryptoblocks;

b) Albot;

c) Akash Kumar Singh;

d) Neelam Singh; or

e) Neeraj Masih.

2. Communications and records that discuss or relate to, in coded or un-coded language, knowledge of the following:

a) The Paycheck Protection Program;

b) The CARES Act;

c) Economic Injury Disaster Loans;

d) COVID-related tax credits, refunds, or advances from the IRS; or

e) The application processes for any of these loans, credits, refunds, or advances.

3. Communications and records that discuss or relate to, in coded or un-coded language, the following:

a) Preparation of company books and records for Kryptoblocks, Albot, or any other business entities associated with Akash Kumar Singh;

b) Preparation of federal personal income tax returns, federal business income tax returns, federal payroll tax returns, or any other claims for refunds or advances from the IRS;

c) Preparation of state payroll tax returns (including but not limited to California Forms DE 9 and DE 9C), refund amounts, methods of payment, bank account information, status of prepared and/or filed tax returns or their associated claims for refunds or advances, and knowledge of tax laws and regulations;

d) Financial loans, such as mortgage or vehicle loans; or

e) Personal financial expenditures (such as electronic receipts or other records of purchases made).

4. Communications and records that discuss or relate to, in coded or un-coded language, information regarding the acquisition and distribution of funds received from the violations listed above or the proceeds of other fraud, including:

a) Bank account information;

b) Commission payments;

c) Bank account set-up instructions;

d) Identities of individuals listed with access to bank accounts;

e) Method of deposits;

f) Acceptance from federal or financial authorities;

g) Information regarding individuals with ability and access to virtually deposit checks.

5. Communications and records that discuss or relate to, in coded or un-coded language, information regarding agreements and business contracts involving Kryptoblocks, Albot, or any other business entities associated with Akash Singh, Neelam Singh, or Neeraj Masih, including monetary agreements and non-monetary agreements, employment agreements, contracting agreements, and the like.

6. Communications and records that discuss or relate to, in coded or un-coded language, personal identifying information, names, routing numbers, bank account numbers, addresses, dollar amounts, financial transfers, wiring instructions, pre-paid debit cards, or any other details related to financial accounts or financial transactions.

7. Records tending to show who created, used, or communicated with the account, including records about their identities and whereabouts.

8. Records tending to identify other accounts, domains, IP addresses, and computers owned or controlled by the same individual or individuals controlling the account.

9. Records tending to establish the identity of the person or persons in control of the account, including identification documents (such as driver licenses or passports), photographs, bills, receipts, vehicle registration documents, statements, leasing agreements, personal address books, calendars, daily planners, personal organizers, and the like.

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

11. Evidence indicating the state of mind of each of the users of the account as it relates to the crime under investigation.

12. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

///

///

13. Records evidencing the use of the account to communicate with Microsoft mail servers, including:

a) Records of IP addresses used;

b) Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE EMAIL ADDRESS AKASH@ALBOT.IO THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION USA

Case No. 2:25-sw-0136 JDP

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before March 4, 2025 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: February 18, 2025 at 4:46 p.m.

Judge's signature

City and state: Sacramento, California

Jeremy D. Peterson, U.S. Magistrate Judge

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

_____

Subscribed, sworn to, and returned before me this date.

_____ _____

Signature of Judge Date

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email address akash@albot.io that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation USA, a company headquartered at 1 Microsoft Way, Redmond, Washington 98052.

ATTACHMENT B

Particular Things to be Seized

I. Information to Be Disclosed by Microsoft Corporation USA (the "Provider")

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

1. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

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

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

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

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1343, 1344, or 1957, those violations involving Akash Kumar Singh and occurring after March 1, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Communications and records that discuss or otherwise show the user(s) of the target accounts and any company or entity affiliation or employment of that person or persons, including all communications and records relating to or purporting to be on behalf of the following:

a) Kryptoblocks;

b) Albot;

c) Akash Kumar Singh;

d) Neelam Singh; or

e) Neeraj Masih.

2. Communications and records that discuss or relate to, in coded or un-coded language, knowledge of the following:

a) The Paycheck Protection Program;

b) The CARES Act;

c) Economic Injury Disaster Loans;

d) COVID-related tax credits, refunds, or advances from the IRS; or

e) The application processes for any of these loans, credits, refunds, or advances.

3. Communications and records that discuss or relate to, in coded or un-coded language, the following:

a) Preparation of company books and records for Kryptoblocks, Albot, or any other business entities associated with Akash Kumar Singh;

b) Preparation of federal personal income tax returns, federal business income tax returns, federal payroll tax returns, or any other claims for refunds or advances from the IRS;

c) Preparation of state payroll tax returns (including but not limited to California Forms DE 9 and DE 9C), refund amounts, methods of payment, bank account information, status of prepared and/or filed tax returns or their associated claims for refunds or advances, and knowledge of tax laws and regulations;

d) Financial loans, such as mortgage or vehicle loans; or

e) Personal financial expenditures (such as electronic receipts or other records of purchases made).

4. Communications and records that discuss or relate to, in coded or un-coded language, information regarding the acquisition and distribution of funds received from the violations listed above or the proceeds of other fraud, including:

a) Bank account information;

b) Commission payments;

c) Bank account set-up instructions;

d) Identities of individuals listed with access to bank accounts;

e) Method of deposits;

f) Acceptance from federal or financial authorities;

g) Information regarding individuals with ability and access to virtually deposit checks.

5. Communications and records that discuss or relate to, in coded or un-coded language, information regarding agreements and business contracts involving Kryptoblocks, Albot, or any other business entities associated with Akash Singh, Neelam Singh, or Neeraj Masih, including monetary agreements and non-monetary agreements, employment agreements, contracting agreements, and the like.

6. Communications and records that discuss or relate to, in coded or un-coded language, personal identifying information, names, routing numbers, bank account numbers, addresses, dollar amounts, financial transfers, wiring instructions, pre-paid debit cards, or any other details related to financial accounts or financial transactions.

7. Records tending to show who created, used, or communicated with the account, including records about their identities and whereabouts.

8. Records tending to identify other accounts, domains, IP addresses, and computers owned or controlled by the same individual or individuals controlling the account.

9. Records tending to establish the identity of the person or persons in control of the account, including identification documents (such as driver licenses or passports), photographs, bills, receipts, vehicle registration documents, statements, leasing agreements, personal address books, calendars, daily planners, personal organizers, and the like.

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

11. Evidence indicating the state of mind of each of the users of the account as it relates to the crime under investigation.

12. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

///

///

13. Records evidencing the use of the account to communicate with Microsoft mail servers, including:

a) Records of IP addresses used;

b) Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied 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 investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.