

UNITED STATES DISTRICT COURT
for the
District of Minnesota

IN THE MATTER OF THE SEARCH OF
THE BUSINESS OFFICE TOWNHOUSE
LOCATED AT 13825 EDGEWOOD AVENUE
SOUTH, SAVAGE, MINNESOTA 55378, AS
FURTHER DESCRIBED IN ATTACHMENT A-2

SEALED BY ORDER OF THE COURT

Case No. 22-MJ-009 TNL

APPLICATION FOR A SEARCH WARRANT

I, Travis Wilmer, 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-2, incorporated here

located in the State and District of Minnesota, there is now concealed:

See Attachment B-2, incorporated here

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

- X evidence of a crime;
X contraband, fruits of crime, or other items illegally possessed;
X 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

Table with 2 columns: Code Section and Offense Description. Rows include Title 18, United States Code, Section 1341 (Mail Fraud), Section 1343 (Wire Fraud), Section 1349 (Conspiracy), and Section 1956, 1957 (Money Laundering).

The application is based on these facts:

See Affidavit, incorporated here

X Continued on the attached sheet.

Handwritten signature of Travis Wilmer
Applicant's Signature

SUBSCRIBED and SWORN before me by reliable
electronic means (FaceTime, Zoom and/or email)
pursuant to Fed. R. Crim. P. 41(d)(3)

Date: January 11, 2022

Travis Wilmer, Special Agent
Federal Bureau of Investigation
Printed Name and Title

Handwritten signature of Tony N. Leung
Judge's Signature

City and State: Minneapolis, MN

The Honorable Tony N. Leung
United States Magistrate Judge
Printed Name and Title

STATE OF MINNESOTA        )  
  )  
COUNTY OF HENNEPIN        )        ss.     AFFIDAVIT OF TRAVIS WILMER

Your affiant, Travis Wilmer, being duly sworn, does state the following is true and correct to the best of his knowledge and belief:

1.     I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since November 8, 2021.

2.     As a Special Agent, my primary duties and responsibilities consist of conducting investigations of individuals and businesses for possible violations of federal laws. I am presently assigned to the FBI's Minneapolis, Minnesota field office where I am a member of the Civil Rights and Public Corruption Squad.

3.     During my employment as a Special Agent, I have participated in investigations of varying degrees involving mail fraud, wire fraud, fraud against the government, money laundering, and other criminal acts, including criminal schemes where individuals misappropriate money from the investing public. Furthermore, in the course of my training and experience, I have become familiar with the types of records businesses typically maintain in the course of their regular activity, including ledgers, journals, invoices, receipts, and bank documents.

4.     Based upon my work experience and training, as well as discussions with law enforcement agents, I know that:

a.     Businesses generally maintain or keep journals, ledgers, bank statements and records, receipts, invoices and other documents evidencing the

receipts and disbursements of funds, inventories, assets of the business and personnel information. These records are usually kept and maintained for extended periods of time, often several years, at the place of business or residence. I know from previous investigations that such records are also often maintained at the residence of subjects.

b. Individuals, including those receiving income from fraud schemes, often maintain within their residence records of assets and financial transactions. These items often include financial statements, receipts, invoices, bank statements and records, bank money order and cashier's check receipts, property records, investment records, assets, stock and bond records, tax records, correspondence, diaries, and handwritten notes. These records are often maintained for extended periods of time, often several years.

c. Due to the increasing prevalence of electronic communications and storage, paper records can be converted and stored electronically. As a result, any record or document could be found in either paper or electronic format.

d. Almost all wire transfers, even intrastate wire transfers, cross state lines.

5. This affidavit is submitted in support of an application for warrants to search:

a. The business office located at 200 Southdale Center, Suite 160, Edina, Minnesota 55436, as further described in Attachment A-1 ("**Subject Premises 1**");

b. The townhouse located at 13825 Edgewood Avenue South, Savage, Minnesota 55378, as further described in Attachment A-2 (“**Subject Premises 2**”);

c. The single-family home located at 15418 Hampshire Lane, Savage, Minnesota 55378, as further described in Attachment A-3 (“**Subject Premises 3**”);

d. The single-family home located at 2713 South Fifth Avenue, Minneapolis, Minnesota 55408, as further described in Attachment A-4 (“**Subject Premises 4**”) (collectively, the **Subject Premises**);

for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), and 1956/1957 (money laundering).

6. This affidavit is based on my personal knowledge, interviews of witnesses, physical surveillance, information received from other law enforcement agents, my experience and training, and the experience of other agents. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a search warrant for the Subject Premises, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, instrumentalities, and fruits of violations of Title 18, United States Code, Sections 1341, 1343, 1349, and 1956/1957 are located at the Subject Premises.

## I. OVERVIEW

7. In recent years, individuals and companies in Minnesota have engaged in a large-scale scheme to fraudulently obtain and misappropriate federally funded child nutrition programs. The scheme was carried out by individuals who owned and operated companies purportedly in the business of providing federally funded free meals to underprivileged children and adults, including during the global Covid-19 pandemic. The companies and their owners received tens of millions of dollars in federal funds for use in providing nutritious meals to underprivileged children and adults. Almost none of this money was used to feed children. Instead, the participants in the scheme misappropriated the money and used it to purchase real estate, cars, and other luxury items. To date, the conspirators have stolen millions of dollars in federal funds. The scheme is ongoing.

## II. LOCATIONS TO BE SEARCHED

### A. Subject Premises 1

8. **Subject Premises 1** is the business office located at 200 Southdale Center, Suite 160, Edina, Minnesota 55436. **Subject Premises 1** is an office suite within the Life Time Work Edina co-working space. **Subject Premises 1** is used by ThinkTechAct Foundation, also known as Mind Foundry Foundation., a company that misappropriated millions of dollars in Federal Child Nutrition Program funds.

9. According to the Minnesota Secretary of State, ThinkTechAct Foundation was organized in or about April 2016 by Mahad Ibrahim. The registered office address for ThinkTechAct was listed as 200 Southdale Center, Edina, Minnesota 55435.

10. ThinkTechAct Foundation has a bank account at U.S. Bank. 200 Southdale Center is listed as the address on this account. As explained below, this account was used to received Federal Child Nutrition Program funds that were fraudulently misappropriated by the owners of ThinkTechAct.

11. On or about December 22, 2021, an FBI agent conducted surveillance at 200 Southdale Center. When the agent asked if ThinkTechAct/Mind Foundry was located there, the receptionist at Life Time Work said it was and offered to get “Mahad.” As explained below, Mahad Ibrahim operates ThinkTechAct/Mind Foundry.

12. On or about January 7, 2022, a U.S. Postal Inspector observed Suite 160 and saw that Suite 160 has a plaque to the left of the door that says “ThinkTechAct Foundation.”

**B. Subject Premises 2**

13. **Subject Premises 2** is the townhouse located at 13825 Edgewood Avenue South, Savage, Minnesota 55378. **Subject Premises 2** is the residence of Mohamed Jama Ismail, one of the owners of Empire Cuisine & Marketing LLC. It is also the registered address of Empire Cuisine & Market LLC, a company that fraudulently obtained and misappropriated Federal Child Nutrition Program funds.

14. According to Scott County property and tax records, Mohamed Ismail owns **Subject Premises 2**.

15. Mohamed J. Ismail has a bank account at Wells Fargo Bank. **Subject Premises 2** is listed as the address on this account. As explained below, this account

was used to received Federal Child Nutrition Program funds that were fraudulently misappropriated by the owners of Empire Cuisine & Market LLC and related entities.

16. As explained below, **Subject Premises 2** is also the address for a U.S. Bank account held by Abidiaziz Farhah, the second owner of Empire Cuisine & Market LLC. As explained below, this account was also used to received Federal Child Nutrition Program funds that were fraudulently misappropriated by the owners of Empire Restaurant.

17. According to U.S. Postal Service records, Empire Cuisine & Market LLC and both of its co-owners, Mohamed Ismail and Abidiaziz Farah, regularly receive mail at **Subject Premises 2**, including in December 2021 and January 2022.

**C. Subject Premises 3**

18. **Subject Premises 3** is the single-family home located at 15418 Hampshire Lane, Savage, Minnesota 55378. **Subject Premises 3** is the residence of Abdiaziz Farah, one of the owners of Empire Cuisine & Market LLC. It is also the registered office of Empire Enterprises, LLC, another company that has fraudulently obtained and misappropriated Federal Child Nutrition Program funds.

19. According to Scott County Property and tax records, Abdiaziz Farah owns **Subject Premises 3**. As explained below, Abdiaziz Farah purchased **Subject Premises 3** in or about April 2021 using Federal Child Nutrition Program funds that had been fraudulently obtained and misappropriated by ThinkTechAct Foundation and that had been laundered through accounts held by Empire Cuisine & Market LLC and Empire Enterprises LLC.

20. Empire Enterprises LLC, Empire Cuisine & Market LLC and Abdiaziz Farah all have bank accounts at JP Morgan Chase. **Subject Premises 3** is listed as the address on each of these accounts. As explained below, this account was used to received Federal Child Nutrition Program funds that were fraudulently misappropriated by the owners of Empire Restaurant.

21. According to U.S. Postal Service records, Abdiaziz Farah, Empire Enterprises LLC, and Empire Cuisine & Market LLC have all received mail at **Subject Premises 3** in December 2021 and/or January 2022.

22. On or about January 7, 2022, FBI surveillance teams observed an individual who appeared to be Abdiaziz Farah leave **Subject Premises 3** at approximately 10:00 am in a black GMC Sierra pick up truck, license plate GLX-951. Minnesota Department of Motor Vehicle records show that this truck is registered to Abdiaziz Farah. The truck proceeded to the multiple addresses, including the office of Partners In Quality Care, a sponsoring company from which Abdiaziz Farah's companies received Federal Child Nutrition Program funds.

**D. Subject Premises 4**

23. **Subject Premises 4** is the single-family home located at 2713 South Fifth Avenue, Minneapolis, Minnesota 55408. **Subject Premises 4** is the residence of Said Farah.

24. Hennepin County property records identify Said Farah as the owner of **Subject Premises 4**.

25. According to Minnesota Secretary of State records, **Subject Premises 4** is the registered address of Bushra Wholesalers LLC, a company that was used to



receive, launder, and misappropriate fraudulently obtained Federal Child Nutrition Program funds. Secretary of State records show that Bushra Wholesalers LLC is controlled by Said Farah and Abdiwahab Aftin. Said Farah is believed to be the brother of Abdiaziz Farah, the owner of Empire Cuisine & Market LLC and Empire Enterprises LLC.

26. According to U.S. Postal Service records, Said Farah, Abdiaziz Farah, Bushra Property Management LLC have all received mail at **Subject Premises 4** in December 2021 or January 2022.

27. Abidiaziz Farah has a bank account at Old National Bank and TruStone Financial. As explained below, these accounts are used to receive Federal Child Nutrition Program funds that were fraudulently misappropriated by Abdiaziz Farah and the other owners of Empire Cuisine & Market LLC and Empire Enterprises LLC. **Subject Premises 4** is listed as the address on both of the accounts.

28. On or about January 7, 2022, an FBI agent observed a black male matching the description of Said Farah leave **Subject Premises 4** at approximately 9:00 a.m. He got into a silver Toyota Avalon sedan bearing Minnesota license plate 524 UBP. Minnesota Department of Motor Vehicle records show that this car is registered to Said Farah.

### III. BACKGROUND

#### A. The Federal Child Nutrition Programs

29. This warrant relates to an ongoing investigation into a scheme to defraud United States Department of Agriculture (USDA) programs that provide federal funding to nutrition programs for children and low-income individuals across

the nation. The USDA operates two such programs—the Summer Food Service Program and the Child and Adult Care Food Program.

30. The Summer Food Service Program (SFSP) is a federal program designed to ensure that low-income children continue to receive nutritious meals when school is not in session.

31. The Child and Adult Care Food Program (CACFP) is a federal program that provides reimbursements for nutritious meals and snacks to eligible children and adults who are enrolled for care at participating child care centers, day care homes, and adult day care centers. CACFP also provides reimbursements for meals served to children participating in afterschool care programs or residing in emergency shelters and adults over the age of 60 or living with a disability and enrolled in day care facilities.

32. The Summer Food Service Program and Child and Adult Care Food Program (together, the “Federal Child Nutrition Programs”) operate throughout the United States. The USDA’s Food and Nutrition Service administers the programs at the national and regional levels by disbursing federal funds to state governments, which provide oversight over the Federal Child Nutrition Programs.

33. Within each state, the Federal Child Nutrition Programs are administered by the state department of education or an alternate state-designated agency. In Minnesota, the programs are administered by the Minnesota Department of Education (“MDE”).

34. Locally, meals funded by the Federal Child Nutrition Program are served at sites such as schools or daycare centers (“Sites”). Each Site must be sponsored by a public or private non-profit organization that is authorized to participate in the Federal Child Nutrition Programs (“Sponsors”). Sponsors seeking to participate in the Federal Child Nutrition Programs are required to submit an application to the MDE for approval for each site from which they intend to operate Federal Child Nutrition Programs. Sponsors are responsible for monitoring each of their sites and preparing reimbursement claims for their sites.

35. Federal Child Nutrition Program funds are supposed to be used to provide nutritious meals and food to children and low-income individuals. *See* 7 C.F.R. § 225.15(a)(4) (“All Program reimbursement funds must be used solely for the conduct of the nonprofit food service operation.”).

36. Historically, the Federal Child Nutrition Program has generally functioned through the provision of meals to children involved in educational-based programs or activities. During the Covid-19 pandemic, however, the USDA waived some of the standard requirements for participation in the Federal Child Nutrition Program. Among other things, USDA allowed for-profit restaurants to participate in the program. It also allowed for off-site food distribution to children outside of educational programs. At the same time, the state government’s stay-at-home order and telework policies interfered with the ability to oversee the program. According to MDE officials, this left the program vulnerable to fraud and abuse.

**B. Feeding Our Future**

37. This warrant related to the investigation of the widespread diversion and misuse of Federal Child Nutrition Program funds during the Covid-19 pandemic. Much of this fraud was committed by sites operated under the sponsorship of Feeding Our Future, a non-profit organization purportedly in the business of helping community partners participate in the Federal Child Nutrition Program and related federal programs. Feeding Our Future sponsors and helps administer sites that participate in the Federal Child Nutrition Program. According to its website, Feeding Our Future “utilize[s] the Child and Adult Care Food Program to increase healthy food access for Minnesota’s youth and seniors.” The website lists Aimee Bock as the founder and executive director of Feeding Our Future.

38. Records obtained from MDE show that after being formed in 2017, Feeding Our Future quickly began receiving and distributing millions of dollars in Federal Child Nutrition Program Funds. The company went from receiving \$3.4 million in 2019 to more than \$197 million in 2021.

<b>Year</b>	<b>Approximate amount of Federal Child Nutrition Program funds to Feeding Our Future</b>
2018	\$307,253
2019	\$3,487,168
2020	\$42,681,790
2021	\$197,932,695
<b>Total</b>	<b>\$244,408,906</b>

39. MDE became concerned about the massive increase in Federal Child Nutrition Program funds going to sites sponsored by Feeding Our Future as well as the large increase in number of sites under Feeding Our Future sponsorship.

According to MDE employees, MDE began more carefully scrutinizing new site applications submitted by Feeding Our Future. Feeding Our Future later sued MDE, alleging that it unlawfully denied its site applications and withheld reimbursements to which Feeding Our Future and sites under its sponsorship were entitled. This lawsuit is currently pending in Ramsey County District Court.

40. At various times during this litigation, the presiding judge has concluded that MDE wrongfully withheld funds and violated federal regulations in its attempts to oversee Feeding Our Future and sites under its sponsorship.

41. In April 2021, MDE provided information to the FBI alleging that Feeding Our Future and sites under its sponsorship were diverting funds away from the nutrition program. MDE believed certain sites were submitting fraudulent documents to support reimbursement of funds in addition to artificially inflating the number of children and low-income individuals receiving benefits in order to obtain funds. But MDE did not have access to the participating companies' bank records so was unable to conclusively determine whether they were misappropriating Federal Child Nutrition Program funds.

42. In May 2021, the FBI began investigating the allegations surrounding the misuse of federal funds intended for feeding children and the low-income individuals. As part of this investigation, the FBI obtained records of hundreds of bank accounts that received, either directly or indirectly, Federal Child Nutrition Program funds. A review of these financial records showed a massive fraud scheme

involving the misuse and theft of tens of millions of dollars in Federal Child Nutrition Program funds.

#### IV. PROBABLE CAUSE

43. After learning of the potential scheme to fraudulently obtain and misappropriate Federal Child Nutrition Program funds, an FBI Forensic Accountant reviewed records of Minnesota companies submitting claims for reimbursements through the program. During this review, the Forensic Accountant noticed several companies that were receiving a suspiciously high amount of reimbursements. These companies—including ThinkTechAct Foundation, Empire Cuisine & Market LLC, and Empire Enterprises LLC—appear to be sharing funds and working together to carry out a scheme to fraudulently obtain and launder Federal Child Nutrition Program funds. The Forensic Accountant obtained records of bank accounts used by these companies to receive Federal Child Nutrition Program funds. A review of these records showed that the companies used little, if any, of this money to purchase food or provide meals to underprivileged children. Instead, they transferred the money among several companies in an order to launder and conceal the source and use of the funds. They then used much of the funds to purchase real estate, cars, and other items.

##### A. **ThinkTechAct Foundation a/k/a Mind Foundry Learning Foundation**

44. ThinkTechAct Foundation is one of the companies fraudulently receiving and misappropriating Federal Child Nutrition Program funds.

45. According to the Minnesota Secretary of State, ThinkTechAct Foundation was organized in or about April 2016 by Mahad Ibrahim. According to Minnesota Secretary of State records, Mind Foundry Learning Foundation is an assumed name under which ThinkTechAct Foundation does business.

46. According to its website, thinktechact.org, ThinkTechAct Foundation's mission is "to provide quality STEM educational programming and promote health and wellness initiatives to youth in unserved low income communities."

47. ThinkTechAct Foundation participated in the Federal Child Nutrition Program via the sponsorship of both Feeding Our Future and, as Mind Foundry, under the sponsorship of Partners in Quality Care. According to records obtained from MDE, ThinkTechAct claimed to be serving meals to thousands of children a day. For example, MDE records show that ThinkTechAct claimed to be providing meals to approximately 160,666 children a day at 10 locations in June 2021.

48. ThinkTechAct receives Federal Child Nutrition Program funds from both sponsors into an account at U.S. Bank. Mahad Ibrahim is the signatory on this account.

49. A review of ThinkTechAct Foundation's U.S. Bank account shows that the company received more than \$16 million in Federal Child Nutrition Program funds from February 2021 to November 2021. The company received approximately \$14,292,507 from Partners in Quality Care and approximately \$2,394,100 from Feeding Our Future. Almost 99 percent of the funds deposited into ThinkTechAct Foundation's U.S. Bank account were Federal Child Nutrition Program funds.

50. These Federal Child Nutrition Program funds were intended to reimburse the company for the cost of meals provided to underprivileged children. However, bank records show that the company used little, if any, money to purchase food or provide meals to children. Instead, bank records show that the funds were transferred to other accounts that appear to function essentially as shell companies designed to help launder fraudulently obtained and misappropriated Federal Child Nutrition Program funds. In all, approximately \$11.6 million was transferred to companies owned or controlled by the owners of Empire or other co-conspirators.

<b>Entity</b>	<b>Entity owner/account holder</b>	<b>Amount Transferred (approximate)</b>
Empire Cuisine and Market	Abdiaziz Farah and Abdimajid Mohamed Nur	\$6.9 Million
Empire Enterprises	Abdiaziz Farah and Abdimajid Mohamed Nur	\$3.2 Million
Empire Gas & Grocery LLC	Abdiaziz Farah Mohamed Ismail	\$100,000
Bushra Wholesalers LLC	Said Farah Abdiwahab Aftin	\$1.4 Million
		<b>\$11.6 Million</b>

51. Bushra Wholesalers LLC appears to have been used to help launder fraudulently obtained and misappropriated Federal Child Nutrition Program funds. According to Minnesota Secretary of State records, Bushra Wholesalers LLC was formed on or about February 10, 2021 by Said Farah, who is believed to be Abdiaziz Farah's brother. Since then, the company opened bank accounts at Bank of America and TruStone Financial Credit Union into which flowed thousands of dollars in fraudulently obtained Federal Child Nutrition Program funds.



52. ThinkTechAct Foundation also transferred approximately \$10.2 million in Federal Child Nutrition Program funds to Empire Cuisine & Markets LLC, Empire Enterprises LLC, and Empire Gas & Grocery LLC. As explained below, all of these companies were created and controlled by Abdiaziz S. Farah and Abdimajid Mohamed Nur. None of the Federal Child Nutrition Program money deposited into these accounts was used to purchase food or serve meals to underprivileged children. In addition, Empire Cuisine & Market LLC and Empire Enterprises LLC also participated in the Federal Child Nutrition Program, through which they fraudulently obtained and misappropriated Federal Child Nutrition Program funds.

**B. Empire Cuisine & Market LLC**

53. According to the Minnesota Secretary of State, Empire Cuisine & Market LLC was organized by Abdiaziz S. Farah on or about April 1, 2020.

54. Empire Cuisine & Market LLC has a contract to be a vendor for the Summer Food Service Program (SFSP). The application was submitted to MDE under the sponsorship of Partners in Quality Care. The initial contract listed Abdimajid Nur as the manager for Empire Cuisine & Market. Kara Lomen signed the contract as the Executive Director for Partners in Quality Care, the sponsoring agency. The contract stated that Empire Cuisine & Market would be providing meals to sites participating in the Federal Child Nutrition Program. The application lists 15 addresses/sites for distribution of food including locations in Minneapolis, St. Paul, Faribault, Owatonna, Shakopee, Bloomington, Circle Pines, and Savage.

55. The contract between Partners in Quality Care and Empire Cuisine & Market specified that Partners in Quality Care would pay Empire Cuisine & Market

\$2.01 per breakfast and \$3.52 per lunch for the SFSP. The money paid by Partners in Quality Care were Federal Child Nutrition Program funds.

56. In or about June 2021, Aimee Bock emailed MDE and requested to change Empire Cuisine & Marketing's sponsorship from Partners in Quality Care to Feeding Our Future.

57. Empire Cuisine & Market has received Federal Child Nutrition Program funds from both Partners in Quality Care and Feeding Our Future. These funds were deposited into accounts held by Empire Cuisine & Market at U.S. Bank, JP Morgan Chase, and Old National Bank. Abdiaziz Farah and Abdimajid Mohamed Nur are the signatories on the Old National Bank accounts. Abdiaziz Farah is the only signatory on the JP Morgan Chase and U.S. Bank accounts. A review of these accounts shows that from on or about May 15, 2020, to on or about November 30, 2021. Empire Cuisine & Market received approximately \$11,065,498 in Federal Child Nutrition Program funds via Partners in Quality Care and approximately \$794,157 in Federal Child Nutrition Program funds via Feeding Our Future. Bank records show that during this same time period approximately \$6,943,959 was transferred to Empire Cuisine & Market from ThinkTechAct Foundation, all of which were the proceeds of fraudulently obtained Federal Child Nutrition Program funds.

58. A review of these accounts shows that little of this money was used to buy food or other items related to participation in the Federal Child Nutrition Program. Instead, the most significant withdrawals from the Empire Cuisine & Market bank accounts were to limited liability companies controlled by Empire

Cuisine & Market owners. This money was then used to purchase properties, pay builders, to purchase high end clothing, travel, make international money transfers and other luxury items.

59. For example, approximately \$10,023,795 in Federal Child Nutrition Program funds were deposited into the Empire Cuisine & Marketing LLC account at Old National Bank. A review of bank records show that this money was not used to purchase food or serve meals to underprivileged children. Instead, the majority of the money deposited into the account was transferred to limited liability companies owned or controlled by owners of Empire Cuisine & Market. In all, bank records show that approximately \$4.8 million was transferred to LLCs controlled by the Empire Cuisine & Market owners and associates.

<b>Entity</b>	<b>Entity owner/account holder</b>	<b>Amount Transferred (approximate)</b>
Empire Enterprises LLC	Abdiaziz Farah and Abdimajid Mohamed	\$2.2 Million
Empire Cuisine and Market LLC (US Bank)	Abdiaziz Farah and Abdimajid Mohamed Nur	\$997,000
Bushra Wholesalers LLC	Said Farah Abdiwahab Aftin	\$745,000
Said Farah	Said Farah	\$150,000
Nur Consulting	Abdimajid Mohamamed Nur	\$226,000
MIB Holdings LLC	Madad Ibrahim	\$310,000
Mahad Ibrahim	Mahad Ibrahim	\$30,000
Abdiaziz Farah	Mahad Ibrahim	\$105,000
Abdimajid Nur	Abdimajid Nur	\$39,000
Abdiwahab Aftin	Abdiwahab Aftin	\$42,000
	<b>Total</b>	<b>\$4.8 million</b>

60. The Old National Bank account was also used to send money to various other entities unrelated to the Federal Child Nutrition Program, including \$500,000

to a custom home building and remodeling company, \$14,000 to a lawn care company, and \$4,100 to the Ritz Carlton hotel.

61. More than \$10 million Federal Child Nutrition Program funds were also deposited into an Empire Cuisine & Market LLC account at U.S. Bank. Bank records show that this money was not used to buy food or serve meals to underprivileged children.

62. More than \$2 million of these funds were transferred to an account held by Mohamed Jama Ismail, one of the owners of Empire Cuisine & Market LLC.

**C. Empire Enterprises LLC**

63. ThinkTechAct Foundation also transferred approximately \$3,189,119 to an account held by Empire Enterprises, LLC, another company created and controlled by Abdiaziz Farah and Abdimajid Mohamed Nur.

64. According to the Minnesota Secretary of State, Empire Enterprises LLC was organized on April 5, 2021. The registered office address was listed as 15418 Hampshire Lane Savage, Minnesota 55378 (a/k/a **Subject Premises 3**).

65. Empire Enterprises LLC received more than \$861,000 in Federal Child Nutrition Program funds between in or about April 2021 and in or about September 2021. These funds were deposited into accounts at Old National Bank and JP Morgan Chase. Abdiaziz Farah and Abdimajid Mohamed Nur were signatories on the Old National Bank account. Abdiaziz Farah is the sole signatory on the JP Morgan Chase account.

66. In addition to the \$380,000 in Federal Child Nutrition Program funds received from Feeding Our Future, more than \$4 million in Federal Child Nutrition

Program funds were deposited into the account from accounts held by Empire Cuisine & Market LLC and ThinkTechAct Foundation. In all, from April 2021 to June 2021, more than \$4.2 million in Federal Child Nutrition Program funds were deposited into the Empire Enterprises LLC account at Old National Bank. This represented 99 percent of the funds deposited into the account.

67. These funds were not used to buy food or provide meals to underprivileged children. Bank records show that almost none of this money was used to purchase food. Instead, a large portion of this money was used to purchase real estate in Kenya and the United States.

**D. More Than \$900,000 in Federal Child Nutrition Program Funds Were Used to Purchase Property in Nairobi, Kenya**

68. Bank records show that more than \$700,000 was transferred from the Empire Enterprises LLC account at Old National Bank to Capital View Properties Limited (Kenya) in Nairobi, Kenya in May-June 2021. During this same time period, on May 17, 2021, another \$200,000 was transferred to Capital View Properties Limited (Kenya) from an account held by Bushra Wholesalers LLC at TruStone Financial. Abdiwahab Maalim Aftin requested the wire transfer. As noted above, Bushra Wholesalers is a company controlled by Said Farah and Abdiwahab Maalim Aftin that received large amounts of Federal Child Nutrition Program funds from ThinkTechAct Foundation, Empire Cuisines & Market LLC, and Empire Enterprises LLC.

Date of Wire Transfer	Amount of Wire Transfer	Source	Recipient
-----------------------	-------------------------	--------	-----------

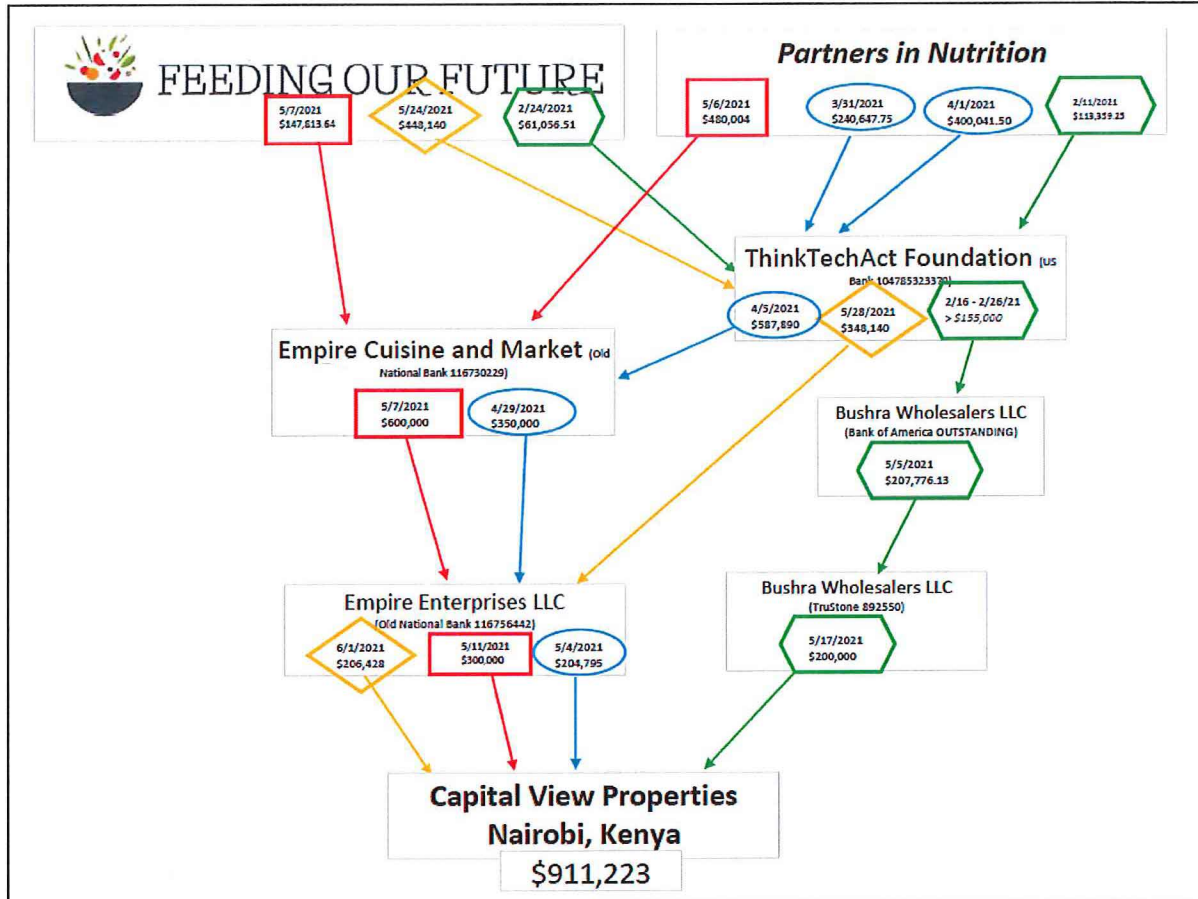
May 4, 2021	\$204,795	Empire Enterprises LLC	Capital Properties (Kenya)	View Limited
May 11, 2021	\$300,000	Empire Enterprises LLC	Capital Properties (Kenya)	View Limited
May 17, 2021	\$200,000	Bushra Wholesalers LLC	Capital Properties (Kenya)	View Limited
June 1, 2021	\$206,428	Empire Enterprises LLC	Capital Properties (Kenya)	View Limited
<b>Total</b>	<b>\$711,223</b>			

69. The documentation of the final wire transfer from Empire Enterprises LLC on June 1, 2021, indicates that the money was related to a “purchase agreement.”

70. In its wire transfer request on May 17, 2021, Bushra Wholesalers LLC claims that the wire related to “supplies for Bushra Wholesale.” Based on my training and experience, and the training and experience of other FBI agents on the case, this appears to be a form of trade-based money laundering. Trade-based money laundering is a process of disguising the proceeds of a crime through the use of international trade transactions in an attempt to legitimize their illicit origins.

71. All of the funds transferred to Capital View Properties Limited (Kenya) were derived from Federal Child Nutrition Program funds received by Empire Cuisine & Market LLC or ThinkTechAct Foundation. As shown in the chart below, these funds were transferred to and from multiple companies and accounts prior to being used to purchase the property in Kenya. Based on my training and experience,

this sort of activity is designed to launder money and conceal the source and use of fraudulently obtained funds.



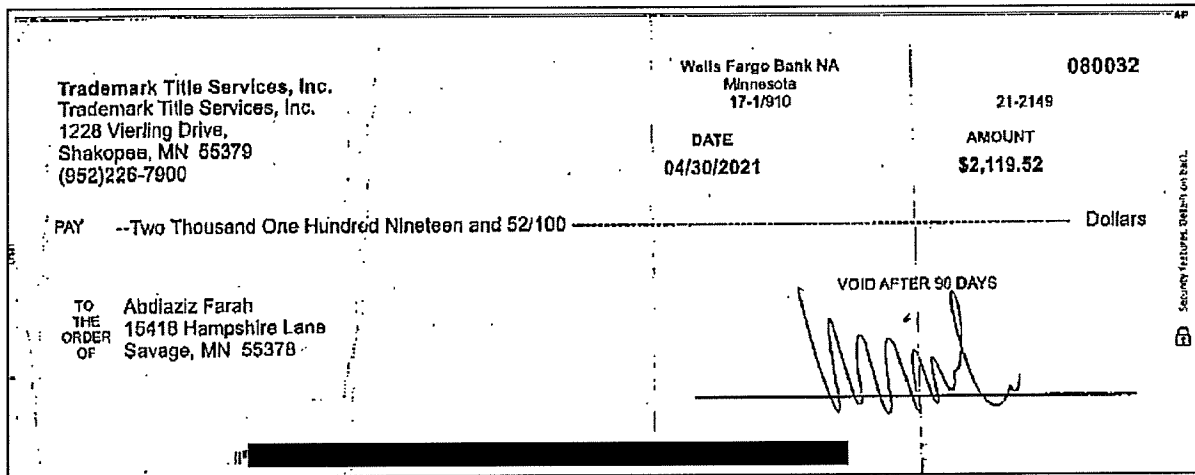
**E. Federal Child Nutrition Program Funds Were Used to Purchase Subject Premises 3 in April 2021**

72. Abdiaziz Farah used Federal Child Nutrition Programs funds from the Empire Enterprises LLC account to purchase a single-family home located at 15418 Hampshire Lane in Savage, Minnesota (a/k/a **Subject Premises 3**). Abdiaziz Farah now lives at 15418 Hampshire Lane.

73. Bank records show that on or about April 15, 2021, \$575,000 was transferred from the Empire Enterprises LLC account at Old National Bank to

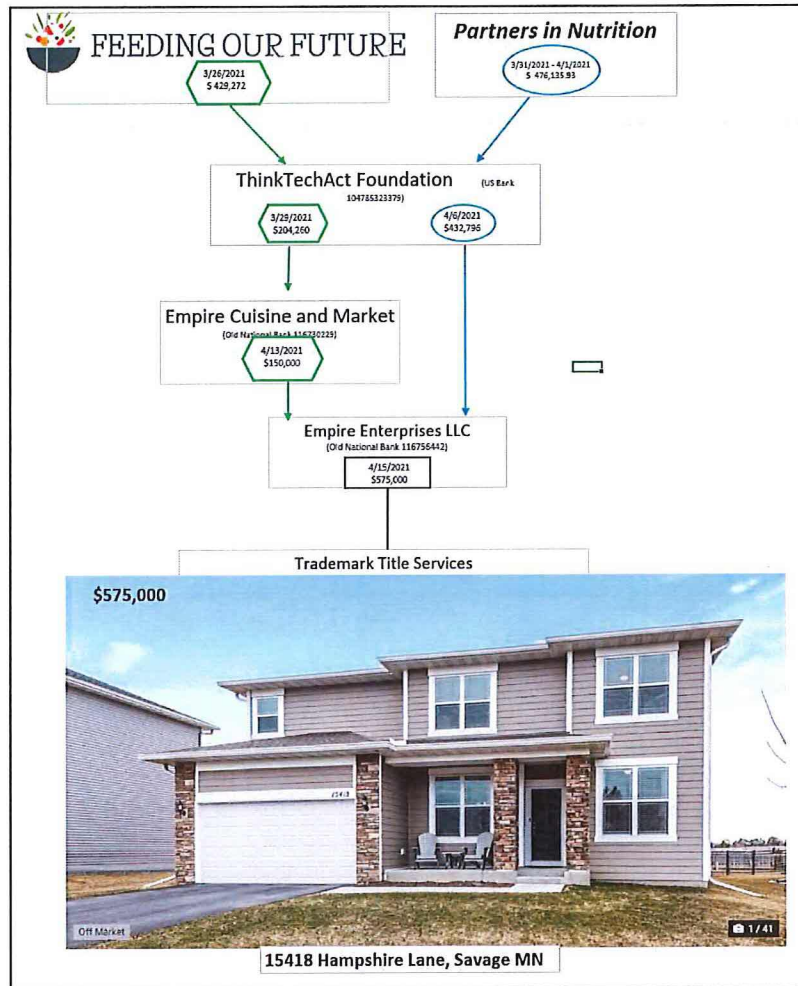
Trademark Title Services. The wire transfer documents indicated that the funds were for the purchase of 15418 Hampshire Lane, Savage, Minnesota.

74. Two weeks later, Trademark Title Services sent a refund check. 15418 Hampshire Lane was listed as Abdiaziz Farah's address on the check.



75. All of the funds used to purchase 15418 Hampshire Lane were derived from Federal Child Nutrition Program funds. After being received from the sponsoring entity, the funds were transferred to one or more other companies in an apparent effort to launder and conceal the source of the funds.

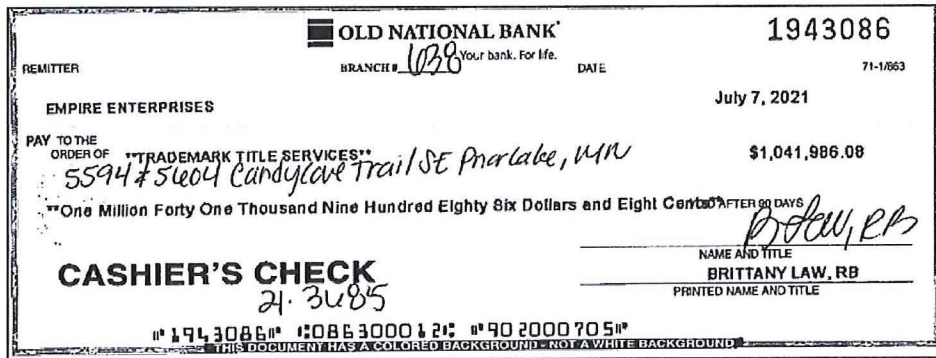




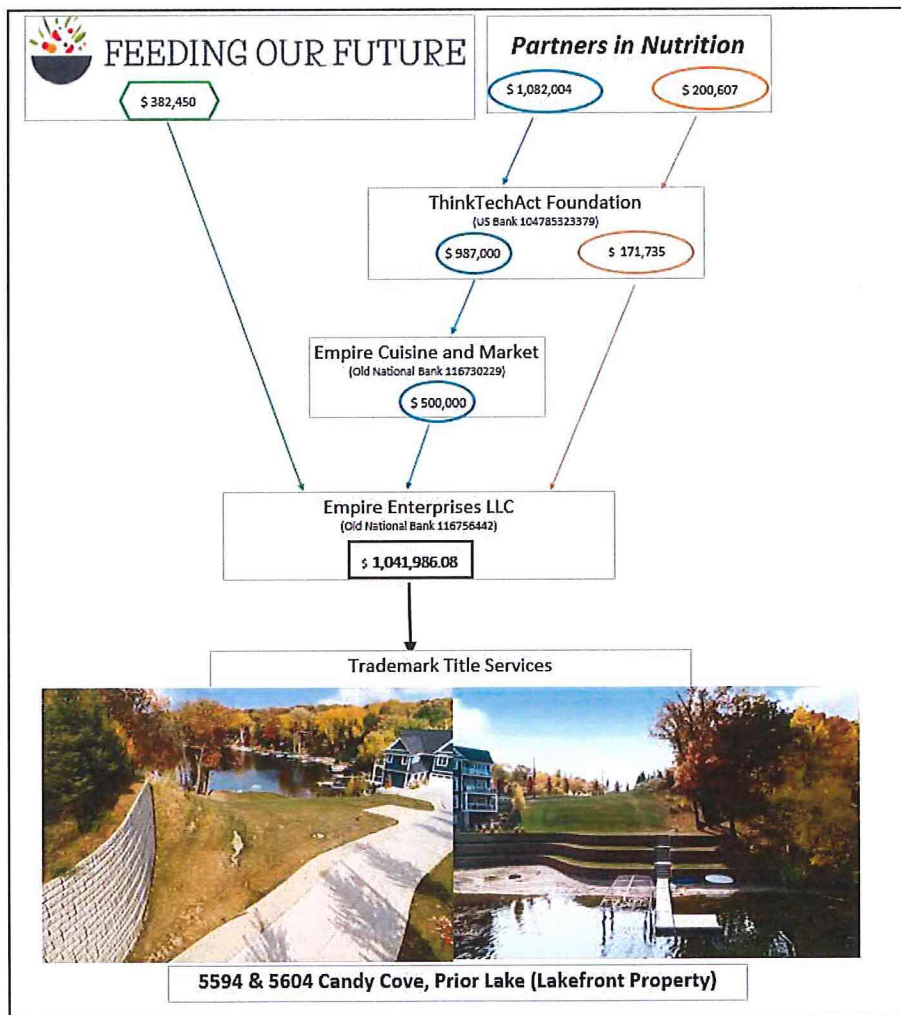
**F. Empire Enterprises LLC Used More Than \$1 Million in Federal Child Nutrition Program Funds to Purchase Two Lots on Prior Lake**

76. More than \$1 million in Federal Child Nutrition Program funds were used to purchase two lakefront lots on Prior Lake for more than \$1 million.

77. On or about July 7, 2021, Abdimajid Mohamed Nur obtained a cashier's check for approximately \$1,041,992 from the Empire Enterprises LLC account at Old National Bank. The check was payable to Trademark Title Services. The addresses 5594 & 5604 Candy Cove Trail SE, Prior Lake, Minnesota were handwritten on the check.



78. A review of bank records shows that all of the money used to obtain this cashier's check was derived from fraudulently obtained Federal Child Nutrition Program funds received by ThinkTechAct Foundation or Empire Enterprises LLC.

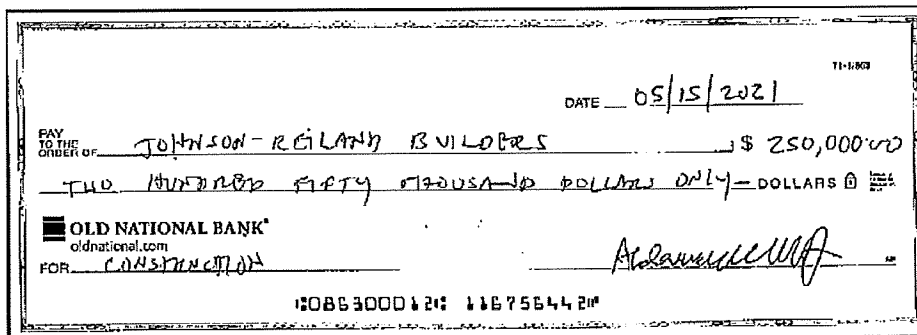


79. This check was used to purchase two lakefront lots on Prior Lake. These lots are located in an upscale residential neighborhood on Prior Lake. According to Minnesota Department of Revenue records, Empire Enterprises LLC purchased these lots on or about July 26, 2021, for \$1.1 million in cash.

**G. More than \$500,000 in Fraudulently Obtained Federal Child Nutrition Program Funds were sent to a Custom Home Builder in Minnesota**

80. The owners of Empire Cuisine & Market LLC and Empire Enterprises have sent hundreds of thousands of dollars in Federal Child Nutrition Program funds to a company that specializes in custom home building and remodeling in the south and southwestern metro area. The checks include:

- a. a \$500,000 check from the Empire Cuisine & Market LLC account at Old National Bank on or about March 19, 2021;
- b. a \$150,000 check for “project construction” from the Empire Cuisine & Market LLC account at Old National Bank on or about July 8, 2021;
- c. a \$250,000 check for “construction” from the Old National Bank account on or about May 15, 2021;



**H. Mahad Ibrahim sent \$320,000 in Federal Child Nutrition Program Funds to a Custom Home Builder in Columbus, Ohio**

81. The Empire companies also sent more than \$500,000 in Federal Child Nutrition Program funds to an account held by MIB Holdings LLC, a company created and controlled by Mahad Ibrahim (the CEO of ThinkTechAct Foundation). Bank records show that MIB Holdings LLC has a bank account at Spire Credit Union. Mahad Ibrahim is the lone signatory on the account. Bank records show that more than \$800,000 was deposited into the account from Empire Cuisine & Market LLC and Empire Enterprises LLC. These funds were all derived from the Federal Child Nutrition Program. Nevertheless, bank records show that MIB Holdings LLC did not use any of this money to purchase food or provide meals to underprivileged children.

82. For example, in the summer of 2021, Mahad Ibrahim sent \$320,000 in Federal Child Nutrition Program funds from MIB Holdings LLC to a custom home builder in Columbus, Ohio. On or about June 1, 2021, Mahad Ibrahim wired \$120,000 from an MIB Holdings LLC account at Spire Credit Union to 3 Pillar Homes, a customer home builder in Columbus, Ohio. On or about August 26, 2021, Mahad Ibrahim wrote a \$200,000 from a MIB Holdings LLC account at Spire Credit Union to 3 Pillar Homes. The memo line on the check read “8592 EF Construction.”

83. Mahad Ibrahim also sent approximately \$30,000 from MIB Holdings LLC to Coinbase.com, a cryptocurrency exchange, in May-June 2021.

**V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

84. Based upon my knowledge, training, experience, and the experience of other law enforcement personnel, I know that computer hardware and computer

software may be utilized to store records which include, but are not limited to: those relating to business activities, criminal activities, associate names and addresses, victims' names, addresses, and images, the identity and location of assets illegally gained through criminal activity, and other information related to criminal activity.

85. As described above and in Attachment B, this application seeks permission to search for records that might be found at the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

**Probable Cause to Seize Electronic Devices at Subject Premises**

86. I submit that if a computer, cellular telephone, or other storage medium is found on the Subject Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when 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.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic 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. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

e. Based on actual inspection of other evidence related to this investigation, including emails obtained through search warrants, I am aware that computer equipment was used to carry out this fraud scheme. There is reason to believe that there is a computer system currently located on the Subject Premises.

87. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the 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, e-mail 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.

b. 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).

c. 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.

d. 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.

88. I know that when an individual uses a computer to commit a crime, in this case, tax evasion and fraudulent tax returns, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

89. *Necessity of seizing or copying entire computers or storage media.* Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, should be processed by a qualified computer specialist in a laboratory or other competent setting. This is due to:

a. *The volume of evidence.* Computer storage devices (like hard disks, removable media, optical media, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with

deceptive file names, or use encryption or steganography software. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site;

b. *The technical requirements.* Searching computer systems for criminal evidence is a highly technical process requiring expert skill 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, so it is difficult to know before a search which expert is qualified to analyze a system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (from external sources or destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis. Further, when a user deletes a file on a computer, only the pointer (a tool that tells the operating system where the file is located on the media) to the file is deleted. The actual file may remain on the media for a long period of time, possibly years. Forensics examiners can use software tools that can locate and partially and/or fully recover deleted files;

c. *System functionality.* Computer systems are very complicated and the proper operation of the system may be dependent upon the hardware that is connected to it. For this reason, it is usually necessary to seize all hardware connected to the equipment in order to ensure the proper operation of the system during the analysis process.

d. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

90. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

91. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant. As set forth above, the Subject Premises are locations from which fraudulent companies are being run and where multiple individuals who, together, commit fraud together may be found. In my training and experience, I know that business locations often contain a variety of electronics, to include computers and cellular telephones. I further know that in this case, such electronic are being actively used to carry out the fraud scheme, to include being used to email lead leads and to make fraudulent phone calls to customers. Digital devices found at the Subject Premises may or may not have a clearly identifiable user based on the exterior of the device and/or may have multiple users whose biometric features may unlock the devices. Thus, if while executing the warrant, law enforcement personnel encounter a digital device within the scope of the warrant that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to, with respect to every person who is located at the Subject Premises during the execution of the search: (1) depress

the person's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the face of the person with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

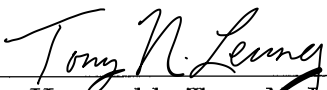
## VI. CONCLUSION

92. Based on the facts set forth above, and based on my training, experience, knowledge, and the aforementioned facts of this investigation, there is probable cause to believe that evidence and instrumentalities of mail fraud, wire fraud, and money laundering, in violation of 18 U.S.C. §§ 1341, 1343, 1956 and 1957, as described in Attachment B, can be found at the Subject Premises, as further described in Attachments A-1 to A-4.

Respectfully submitted,

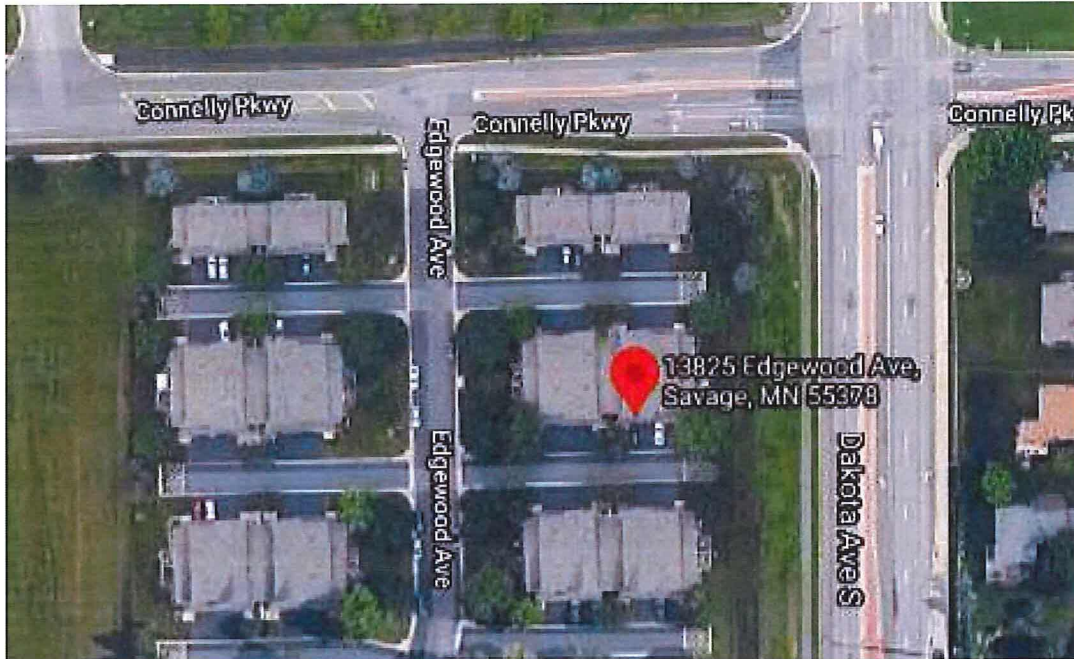
  
\_\_\_\_\_  
FBI Special Agent Travis Wilmer

SUBSCRIBED and SWORN before me by reliable electronic means (FaceTime, Zoom and/or email) pursuant to Fed. R. Crim. P. 41(d)(3)

 January 11, 2022  
\_\_\_\_\_  
The Honorable Tony N. Leung  
United States Magistrate Judge

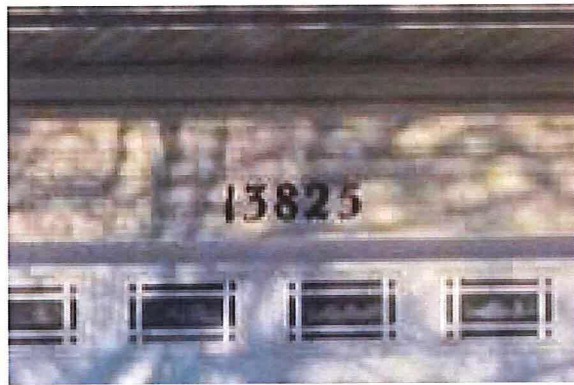
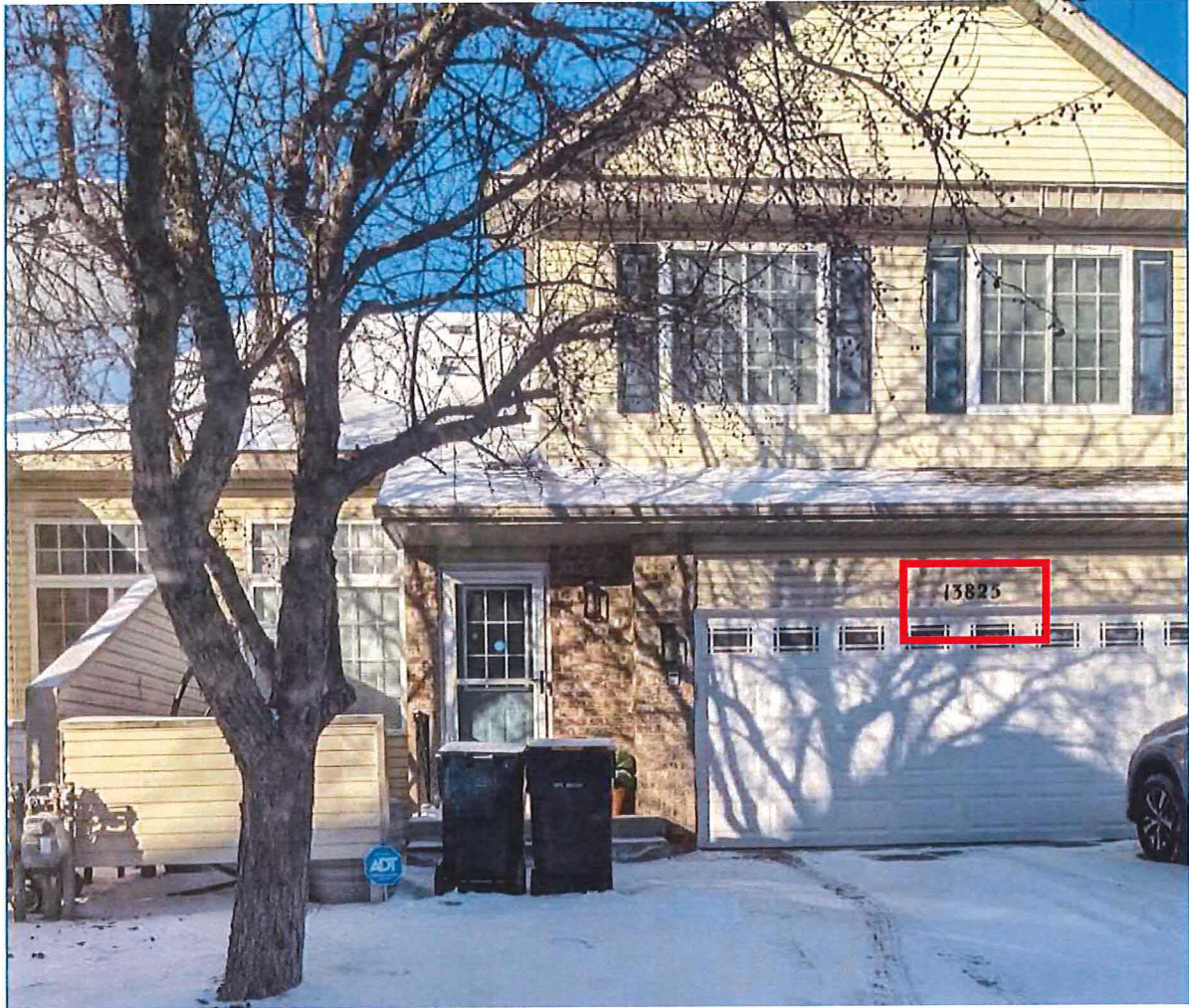
## Attachment A-2

Subject Premises 2 is the townhouse located at 13825 Edgewater Avenue South, Savage, Minnesota 55378. 13825 Edgewater Avenue South is located west of Edgewater Avenue South, south of Connelly Parkway.



13825 Edgewater Avenue South is in a townhouse development. Each individual townhouse has its own street address. 13825 Edgewater Avenue South has yellow siding and a white garage door facing the street. The numbers "13825" appear above the garage door. The front door is located to the left of the garage door.







**ATTACHMENT B**  
**(List of Items to be Seized)**

Items to be seized include all evidence of violations of Title 18, United States Code, Sections 1341 (mail fraud), 1343 (wire fraud), 1349 (conspiracy), 1956 and 1957 (money laundering), for the period of January 1, 2019 through the present, related to a scheme to fraudulently obtain and misappropriate federal child nutrition program funds, including the following:

1. All documents, correspondence, or information related to participation in federal child nutrition programs, including applications, claims, invoices, records, reimbursements, contracts, site locations, and identification of children served.

2. All correspondence or communication with the Minnesota Department of Education, Feeding Our Future, Partners in Nutrition/Partners in Quality Care, or other entities related to participation in federal child nutrition programs.

3. All personal financial documents, records and information for Mahad Ibrahim, Abdiaziz Farah, Abdimajid Mohamed Nur, Said Farah, Mohamed Ismail, Abidwahib Aftin, including but not limited to the following:

a. Financial records including bank statements, deposit tickets, canceled checks, credit and debit memos, wire transfers, bank money orders, cashier's checks, investment records, stock and bond records, loan records, safety deposit box records, financial statements, tax returns, and records utilized in the preparation of tax returns;

b. Retained copies of personal and business tax returns;

c. Receipts and other documents showing disbursement of funds and ownership of assets, including purchases of real estate and other assets, home improvement, and casino player cards; and

d. Documents showing the location of other records including receipts and contracts for rental units, and change of address or post office box records.

4. All documents, records and information pertaining to ThinkTech Act Foundation, Mind Foundry Learning Foundation, Empire Cuisine & Market LLC, Empire Enterprises LLC, Bushra Wholesalers LLC, Empire Gas & Grocery LLC, MIB Holdings LLC, including but not limited to the following:

a. Accounting records including financial statements, chart of accounts, account ledgers, general ledgers, cash receipt journals, cash disbursement journals, payroll registers, check registers, accounts payable ledgers, accounts receivable ledgers, general journal and overhead rates and calculations;

b. Records that show ownership, control, affiliation, and operation of ThinkTech Act Foundation, Mind Foundry Learning Foundation, Empire Cuisine & Market LLC, Empire Enterprises LLC, Bushra Wholesalers LLC, Empire Gas & Grocery LLC, MIB Holdings LLC or any other associated companies, entities, investments, or assets, including but not limited to articles of incorporation, corporate resolutions or minutes, other business or corporate records, memoranda, by-laws, shareholder information, donor information, service agreements, partnership

agreements, memoranda of understanding, and other documents evincing ownership, control, affiliation, and operation.

c. Financial records including bank statements, deposit tickets, canceled checks, credit and debit memos, wire transfers, bank money orders, cashier's checks, investment records, stock and bond records, safety deposit box records, tax returns, and records utilized in the preparation of tax returns;

d. Personnel files and employee information for all employees, volunteers, and/or independent contractors, including, but not limited to, payroll records, time sheets and other records of work performed, applications for employment, background checks, Forms 1099, Forms W-2, and Forms W-4; and

e. Business records including invoices, statements, contracts and agreements, purchase and sale records, records of donations, and correspondence.

5. Property records, receipts, investment records, stock and bond records, mortgages, rental or lease agreements, promissory notes, handwritten notes, calendars, day planners, logs, records related to wire transfers or reflecting financial transactions, and records related to or tending to identify the source, accumulation, disposition, location or ownership of assets, money, wealth, property, safe deposit records, and safe deposit keys.

6. Records reflecting business or personal travel, including passports;

7. All documents identifying potential victim companies, including but not limited to financial records, and business documents.

8. Information that constitutes evidence of meals served to underprivileged children.

9. Correspondence, memos, reports, notes, and e-mails pertaining to the business and personal financial affairs described above.

10. All documents and records tending to show the identities of associates or co-conspirators, or tending to show the location of assets including notes, telephone messages, telephone numbers, email addresses, address books, and appointment books.

11. Smartphones or cellular telephones, computers, tablet computers, and other digital storage media that may contain any of the records or information described above.

12. Any computer software (and related instructions or manuals) that was used or may have been used to operate the computer hardware listed above, access remote computers, communicate with others, or to manage and record financial transactions, including but not limited to Internet browsers, Internet access software, word processing programs, email software, banking software, business management tools, and accounting software.

13. Any access devices, records, or information needed to open or fully operate the computer hardware or software listed above, including but not limited to physical keys, account numbers, screen names, passwords, personal identification numbers (PINs), or digital certificates.

14. 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 electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including hard disks, ZIPdisks, optical discs, backup tapes, smart cards, memory calculators, personal digital assistants, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as prints, negatives, videotapes, motion pictures, photocopies).

15. Any and all records related to the use of post office boxes, virtual offices, or mail service providers.

16. Items needed to access the information listed above, such as:

a. Cabinet and desk keys;

b. Documents and items regarding the rental or use of a storage unit, including contracts, rental agreements, and keys; and

c. Safe and lock combination and keys.

17. Any digital device capable of storing information related to the commission or attempted commission of the above listed violations, or used to facilitate the above-listed violations, and forensic copies thereof.

18. With respect to any digital-device containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

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

c. evidence of the attachment of other devices;

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

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or

“favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

19. As used herein, the terms “records,” “documents,” “programs,” “applications,” and “materials” includes records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

20. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units, desktops, laptops, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

## SEARCH WARRANT ADDENDUM

1. In conducting the search authorized by this warrant, the government shall make reasonable efforts to utilize search methodology that avoids searching files, documents or other electronically stored information which is not identified in the warrant.
2. If electronically stored data, information, documents or other records have been identified and seized by the government pursuant to this warrant, the government may retain the electronic storage device (e.g., computer, hard drive, mobile device, smartphone, cell phone). The person from whom the electronic storage device was seized may request that the government provide him or her with electronic copies of the data, information, documents or other records by making a written request to the United States Attorney's Office, identifying with specificity the data, information, documents or other records sought to be copied. The government must respond to all such requests within a reasonable amount of time, and must provide a copy of the electronically stored data, information, documents or other records requested unless the copies requested constitute contraband, instrumentalities, or property subject to forfeiture.
3. Nothing in this warrant shall limit or prevent the government from seizing the electronic storage device as contraband or an instrumentality of a crime or commencing forfeiture proceedings against the electronic storage device and the data contained in the device. Nothing in this warrant shall limit or prevent the owner of the electronic storage device, files, software, hardware, data, information, documents or other records from (a) filing a motion with the Court pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure for the Return of Property, or (b) making a request of the government to return certain specified electronic storage devices, files, software, hardware, data, information, documents or other records.
4. The government shall establish a search methodology governing the review of seized data to ensure that no attorney-client privileged communications will be inadvertently reviewed by the prosecution team. In the event that data seized pursuant to this warrant are identified by the government as possibly containing attorney-client privileged communications, an Assistant United States Attorney, who is not a member of the prosecution team and who is not participating in the search, shall act as a "taint team" to set up an ethical wall between the evidence and the prosecution team that will prevent any privileged material from getting through to the prosecution team.



UNITED STATES DISTRICT COURT
for the
District of Minnesota

IN THE MATTER OF THE SEARCH OF
THE BUSINESS OFFICE TOWNHOUSE
LOCATED AT 13825 EDGEWOOD AVENUE
SOUTH, SAVAGE, MINNESOTA 55378, AS
FURTHER DESCRIBED IN ATTACHMENT A-2

SEALED BY ORDER OF THE COURT

Case No. 22-MJ-009 TNL

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 State and District of Minnesota:

See Attachment A-2, incorporated here.

The person or property to be searched, described above, is believed to conceal:

See Attachment B-2, incorporated here.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before January 24, 2022 (not to exceed 14 days)

X in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the current United States Magistrate Judge on duty.

Date and Time issued: January 11, 2022, 1:00 am

Tony N. Leung
Judge's Signature

City and State: Minneapolis, MN

The Honorable Tony N. Leung
United States 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 declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.*

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*

\_\_\_\_\_  
*Printed Name and Title*

*SUBSCRIBED and SWORN before me by reliable electronic means (FaceTime, Zoom and/or email) pursuant to Fed. R. Crim. P. 41(d)(3)*

\_\_\_\_\_  
United States Magistrate Judge

\_\_\_\_\_  
Date