UNITED STATES DISTRICT COURT

for the
District of Minnesota

IN THE MATTER OF THE SEARCH OF THE SUBJECT PREMISES DESCRIBED IN ATTACHMENT A

SEALED BY ORDER OF THE COURT

Case No. 25-mj-861 (DTS)

APPLICATION FOR A SEARCH WARRANT

I, Jared F. Kary, 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, incorporated here

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

See Attachment B, 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*
Title 18, United States Code, Section 1343	Wire Fraud
Title 18, United States Code, Section 1347	Healthcare Fraud
Title 18, United States Code, Section 1349	Conspiracy to Commit Wire Fraud and Healthcare Fraud

The application is based on these facts:

See Affidavit, incorporated here

X Continued on the attached sheet.

Applicant's Signature

Special Agent Jared F. Kary
FBI

Printed Name and Title

SUBSCRIBED and SWORN before me on

Date: _____

Judge's Signature

City and State: Minneapolis, MN

The Honorable David T. Schultz
United States Magistrate Judge

Printed Name and Title

IN THE UNITED STATES DISTRICT COURT
FOR MINNESOTA

IN THE MATTER OF THE SEARCH OF THE BUSINESS OFFICE LOCATED AT 9217 17TH AVENUE SOUTH, SUITE 203 BLOOMINGTON, MINNESOTA AS DESCRIBED IN ATTACHMENT A	**UNDER SEAL** Case No. 25-mj-861 (DTS)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jared F. Kary, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since approximately 2008. I am currently assigned to the Minneapolis Division of the FBI. As part of my assigned duties, I investigate violations of federal criminal law, including but not limited to violations of Title 18, United States Code, Sections 1341 (mail fraud) and 1343 (wire fraud). My training and experience include gathering and analyzing large quantities of evidence in physical and electronic formats.

2. This affidavit is submitted in support of an application for a warrant to search for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 (wire fraud), Title 18, United States Code, Section 1347 (healthcare fraud), and Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud and healthcare fraud), at the following locations:

a. The business office of Ultimate Home Health Services LLC, located in Suite 203 in the office building at 9217 17th Avenue South in Bloomington, Minnesota, as further described in Attachment A (the "**Subject Premises**").

3. 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, Section 1343 (wire fraud), Title 18, United States Code, Section 1347 (healthcare fraud), and Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud and healthcare fraud) are located at the Subject Premises.

I. OVERVIEW

4. The requested search warrant is part of an investigation into a massive scheme to defraud the Integrated Community Supports (ICS) Program, a new Minnesota Medical Assistance benefit designed to help adults with disabilities live independently with one-on-one assistance with health, safety, and household tasks so that people can maintain stability and independence in their own homes and communities.

II. LOCATIONS TO BE SEARCHED

A. The Subject Premises

5. The **Subject Premises** is the business office of Ultimate Home Health Services LLC. It is located in Suite 203 at an office building located at 9217 17th Avenue South in Bloomington, Minnesota.

6. According to Minnesota Secretary of State records, the **Subject Premises** is the principal executive office for Ultimate Home Health Services.

7. On December 15, 2025, I interviewed the leasing agent manager for the **Subject Premises**, who indicated that Ultimate Home Health Services still occupied the **Subject Premises** and was using the office suite for their business.

8. On December 16, 2025, I conducted surveillance at the **Subject Premises** and saw a sign that said "UHHS Ultimate Home Health Services" next to the door for Suite 203.

III. BACKGROUND

A. Fraud in Minnesota's Medicaid Programs

9. Over the past several years, the U.S. Attorney's Office and federal law enforcement agents have been investigating and prosecuting a massive scheme to defraud the federal child nutrition program, a program designed to provide free meals to children in need. The conspirators in that case carried out their fraud scheme by falsely claiming to be serving meals to thousands of children a day and submitting fraudulent claims for federal child nutrition program funds for doing so. Collectively, the defendants obtained, misappropriated, and laundered hundreds of millions of dollars in program funds that were intended as reimbursements for the cost of serving meals to children over an 18-month period in 2020 and 2021.

10. The individuals involved in the scheme participated in the federal child nutrition program under the sponsorship of Feeding Our Future and another entity, Partners in Nutrition. During the Feeding Our Future investigation, the government noticed that the amount of federal child nutrition program funds received by entities sponsored by Feeding Our Future and Partners and Nutrition increased dramatically during the time of the fraud scheme. Minnesota Department of Education records of federal child nutrition program payments showed that Feeding Our Future went from receiving $3.4 million in 2019 to more than $197 million in 2021.

Year	Approximate amount of Federal Child Nutrition Program funds to Feeding Our Future
2018	$307,253
2019	$3,487,168
2020	$42,752,626
2021	$199,498,101
Total	**$246,045,149**

11. Partners in Nutrition, the other sponsor involved in the scheme, showed similarly explosive growth during this period, going from receiving approximately $5.6 million in federal child nutrition program funds in 2019 to receiving more than $175 million in 2021.

Year	Approximate amount of Federal Child Nutrition Program funds to Partners in Nutrition
2018	$5,232,714
2019	$5,654,029
2020	$20,891,318
2021	$179,896,117
Total	**$211,674,117**

12. During the Feeding Our Future investigation, the government saw that many individuals and entities who received federal child nutrition program funds under the sponsorship of Feeding Our Future or Partners in Nutrition also owned or received money from autism clinics and other health care companies that provided EIDBI services. At least a dozen of the defendants charged for their roles in the Feeding Our Future scheme owned, received money from, or were associated with autism clinics and other health care companies that received state funds for providing EIDBI services.

1. Early Intensive Developmental and Behavioral Intervention (EIDBI) Services for Autism Program

13. Based on these reports, the U.S. Attorney's Office asked FBI and HHS-OIG agents to obtain and review claims data for Medicaid claims submitted in Minnesota for services provided as part of the EIDBI program. This data showed that the amount of Medicaid money paid out for EIDBI claims in Minnesota has increased dramatically since the EIDBI program began in 2017—and in a manner similar to how the federal child nutrition program funds were paid out by the Minnesota Department of Education skyrocketed during the COVID-19 pandemic.

14. For example, claims data received from the Center for Medicare and Medicaid Services, show that in 2018, Medicaid paid out approximately $670,000 in Medicaid reimbursement claims for EIDBI-related services in Minnesota. That grew to more than $300 million in 2024.

Year	Number of EIDBI Providers	Number of EIDBI Recipients	Total Billed for EIDBI-related Medicaid claims	Total Paid for EIDBI-related Medicaid claims
2018	31	400	$1,115,046	$671,339
2019	73	791	$60,147,793	$20,456,071
2020	113	1338	$99,782,330	$38,121,855
2021	176	2440	$209,575,457	$83,026,547
2022	239	3355	$284,412,878	$124,537,388
2023	326	4331	$400,076,995	$189,139,374
2024	440	5705	$601,268,592	$342,821,719
2025 (though Sept. 30, 2025	482	5887	$471,729,897	$290,403,644
			$2,128,108,988	**$1,089,177,937**

15. The investigation has revealed that many autism clinics are submitting fraudulent claims for EIDBI services that were not actually provided or needed. As

part of the scheme, autism clinics are paying cash kickbacks to parents to have their children diagnosed with autism spectrum disorder and then enrolling them to receive EIDBI services that the children do not actually need or receive. The first defendant in the investigation was charged in September 2025 and is scheduled to plead guilty on December 18, 2025.

2. The Housing Stabilization Services Program

16. The FBI, IRS-CI, and HHS-OIG have an active investigation into large-scale fraud in the Housing Stabilization Services Medicaid program. In July 2020, Minnesota became the first state in the country to offer Medicaid coverage for Housing Stabilization Services. The Housing Stabilization Services (HSS) Program is a Medicaid benefit designed to help people with disabilities, including seniors and people with mental illness and substance use disorders, find and keep housing.

17. The HSS program was designed to make Housing Stabilization Services an easy-to-obtain benefit and to make it easy for would-be providers to participate. Unfortunately, the HSS program has shown to be uniquely vulnerable to fraud, which has resulted in a massive increase in the number of claims and the amount of Medicaid funds paid out to HSS providers.

18. When the state first authorized the HSS Program, the Minnesota Department of Human Services (DHS) estimated that the new program would cost approximately $2.6 million a year.[1] This estimate proved inaccurate. According to

[1] Chris Serres, "Minnesota launches pioneering Medicaid program to combat homelessness," Star Tribune July 25, 2020, available at Https://www.startribune.com/minnesota-launches-pioneering-medicaid-program-to-combat-homelessness/571878882 (last accessed December 17, 2025).

data obtained from the Center for Medicare and Medicaid Services, the HSS program cost more than $27 million in 2021 and grew to more than $100 million in 2024.

Year	Number of HSS Providers	Number of HSS Recipients	Total Billed for HSS-related Medicaid claims	Total Paid for HSS-related Medicaid claims
2021	278	8126	$28,586,371	$27,771,862
2022	458	12,976	$47,651,975	$45,813,047
2023	693	17,470	$83,626,287	$79,287,495
2024	883	21,679	$108,937,271	$105,385,749
2025 (through Sept. 30, 2025)	831	19,004	$58,875,472	$57,244,329
Total			**$327,677,376**	**$315,502,480**

19. In July 2025, federal agents executed search warrants at several HSS companies around in the Minneapolis-St. Paul metropolitan area. In the wake of those search warrants, and the unsealing of the supporting affidavits, Minnesota Governor Tim Walz issued an executive order terminating the HSS program effective October 31, 2025.

20. In October 2025, Governor Walz ordered a third-party audit for 14 Medicaid programs that had been identified as high-risk for fraud, including the EIDBI and HSS programs. According to the state's announcement, the 14 programs were identified as high-risk based on programmatic vulnerabilities, evidence of fraudulent activity, or data analytics that revealed potentially suspicious patterns, claim anomalies, or outliers. Based on the order, payments for the programs were paused for up to 90 days in order to detect suspicious billing activity and scrutinize the use of public funds.

21. According to claims data obtained from the Center for Medicare and Medicaid Services, these 14 high-risk Minnesota Medicaid programs have paid out more than $18 billion in claims since 2018. Medicaid claims data further shows that many of the 14 high-risk Medicaid programs have seen an explosion in claims similar to that seen in the EIDBI, HSS, and federal child nutrition program.

22. The U.S. Attorney's Office and agents from the FBI, U.S. Department of Health and Human Services Office of Inspector General, and IRS-Criminal Investigations are investigating these programs. To date, the government has charged 13 defendants for their role in defrauding the HSS program.

B. The Integrated Community Supports (ICS) Medicaid Program

23. One of the 14 high-risk programs for which the state has issued a payment suspension is the Integrated Community Supports ("ICS") program.

24. Federal investigators had noticed and been concerned about fraud in the ICS program for some time. Those suspicions were confirmed during the investigation of the Housing Stabilization Services program. During a proffer in August 2025, for example, Individual A told federal agents about the ICS program. Individual A has been charged with carrying out a fraudulent scheme to receive Housing Stabilization Services Medicaid payments. Individual A has pled guilty for his role in that scheme and agreed to cooperate with the government in hopes of receiving a reduced sentence.

25. During his proffer, the government asked Individual A about other programs that he has heard have a lot of fraudulent actors. Individual A identified Integrated Community Services, which he described as a lucrative business.

Individual A explained that people participating in the program lease apartments, apply for a provider license, finds clients who qualified for waivered Medicaid services, and then put them in the apartments. He described ICS as "easy money."

26. Minnesota began offering Medicaid coverage for Integrated Community Supports in 2021. According to DHS, ICS is a Medical Assistance (that is, Minnesota Medicaid) benefit designed to fill a gap in the service continuum between a person living in their own home and more restrictive settings such as group homes and assisted living.

27. According to DHS's website, ICS is a Medicaid program designed to "provide support and training/habilitation in community living service categories to adults who reside in a living unit of a provider-controlled ICS setting (e.g., apartment in a multi-family housing building). ICS can be delivered up to 24 hours per day in the person's living unit or in the community."

28. According to its website, "DHS and the legislature are moving away from assisted living models which were geared for older adult populations and don't offer as much client choice in how or if they receive services."

29. ICS was designed to help people live more independently in the community with daily one-on-one help with health, safety, and household tasks. According to DHS, this can include services and training for:

a. Community participation (getting out and doing things you like to do outside of your apartment), such as help finding things to do, learning to get around, and interpersonal skills.

b. Health, safety, and wellness, such as setting up health appointments and learning how to stay healthy and safe.

c. Household management, such as making your home safe, following the rules of your lease, budgeting, and cooking.

d. Adaptive skills (planning, preparing, and safety), such as "crisis prevention, problem-solving, and living safely on your own."

30. ICS services are available to adults who qualify for certain Medicaid waivers that allow them to receive home- and community-based services as an alternative to institutionalization:

a. The "Brain Injury" waiver provides home- and community-based services to adults with a diagnosis of brain injury who would otherwise require the level of care provided in a specialized nursing facility or neurobehavioral hospital.

b. The "Community Access for Disability Inclusion" waiver provides home- and community-based services to adults with disabilities who would otherwise require the level of care provided in a nursing facility.

c. The "Community Alternative Care" waiver provides home- and community-based services to adults who are chronically ill or medically fragile and would otherwise require the level of care provided in a hospital.

d. The "Developmental Disabilities" waiver provides home- and community-based services to children and adults with a diagnosis of a developmental disability or a related condition who require the level of care provided in an intermediate care facility for persons with developmental disabilities.

31. Unfortunately, the ICS program has been vulnerable to fraud. Private ICS providers can bill hundreds of dollars a day for each person for whom they provide services. As with many other state government benefit programs in Minnesota, there has been an explosion in fly-by-night providers who enrolled in the ICS program and immediately began receiving large Medicaid pay-outs.

32. As with the EDIBI and HSS programs, the ICS program has seen soaring cost increases over the five years since it began in 2021. After paying out a total of approximately $4.6 million in 2021, the program has grown to cost more than $170 million in 2024. In all, claims data obtained from the Center for Medicare and Medicaid Services shows that the Medicaid system had paid out more than $400 million for ICS serves since 2021.

Year	Number of ICS Providers	Number of ICS Recipients	Total Billed for ICS-related Medicaid claims	Total Paid for ICS-related Medicaid claims
2021	28	164	$5,989,340	$4,638,314
2022	128	663	$31,757,471	$26,097,517
2023	357	1,634	$96,470,686	$88,082,081
2024	458	2,444	$178,916,125	$170,776,456
2025 (through Sept. 30)	457	2,366	$150,077,911 (on pace for $200,103,881)	$134,511,581 (on pace for $179,348,775)
Total			**$463,211,533**	**$424,105,949**

C. Ultimate Home Health Services LLC

33. The federal investigation has shown that Ultimate Home Health Services LLC fraudulently submitted Medicaid claims for ICS services that it did not actually provide.

34. According to Minnesota Secretary of State records, Ultimate Home Health Services LLC was registered in October 2021. Othman Mohamed and Hasan Abshir are listed as the registered agents. DHS records indicate that Mohamed and Abshir each own 50 percent of Ultimate Home Health Services.

35. According to DHS records, Ultimate Home Health Services submitted claims for reimbursement for over $1.1 million in ICS funds between approximately June 2024 and August 2025. During that time, Ultimate Home Health Services submitted claims on behalf of a total of 13 clients.

36. According to DHS records, 11 of Ultimate Home Health's clients reside in an apartment building located at 1891 7th Street East in St. Paul, Minnesota. Ultimate Home Health rents the building and uses it to house its ICS clients.

37. One of the ICS clients residing at 1891 7th Street East was Kelly R.

38. Agents from the FBI and IRS interviewed Kelly R. during the investigation. Kelly R. explained that she is Medicaid eligible and qualified for the

Community Access for Disability Inclusion (CADI) waiver. Kelly R. explained that her CADI manager initially enrolled her for assistance through the Housing Stabilization Services (HSS) program. According to Kelly R., the HSS company found her a place to live at 1891 7th Street East but said she would have to qualify for ICS services to live there. Kelly R.'s CADI manager helped her qualify for the ICS program by having Kelly R. write an email explaining that she needed a higher level of care. Kelly R. was told she qualified for 9 hours of in-person care and 2 hours of remote care a day.

39. Kelly R. moved into Ultimate Home Health's building at 1891 7th Avenue East in or about June 2024. At the time, she was unemployed. Ultimate Home Health Services agreed to charge her only $60 a month in rent. Just a few months later, in or about October 2024, Kelly R. secured a full-time job, which she has had ever since. Kelly R. continued to live at 1891 7th Avenue East as an ICS client after securing full-time employment, and her rent remained $60 a month. During this time, Ultimate Home Health was submitting claims purporting to be providing ICS services to Kelly R. When asked about any ICS services she received, Kelly R. said that she typically checked in at the front desk when she got home from work. Sometimes no one was there. Kelly R. explained that sometimes an Ultimate Home Health employee would knock on her door to check on her. But Kelly R. explained that many days she had no contact with Ultimate Home Health employees and essentially lived on her own without support.

40. According to DHS records, over a 447-day period from June 1, 2024, through August 21, 2025, Ultimate Home Health claimed to have provided ICS services to Kelly R. on all but four days. Based on its claims that it provided ICS services to Kelly R., Ultimate Home Health received approximately $166,000 in Medicaid payments—an average of $375 a day during this period.

41. Kelly R. said she did not know what services Ultimate Home Health claimed to be providing to her. Kelly R. said she was not aware that Ultimate Home Health was claiming to be providing services to her nearly every day. She said that did not happen.

42. Rick C. was another Ultimate Home Health's ICS client who lived at 1891 7th Street East in St. Paul. Rick C. was a 39-year-old man who suffered from severe mental illness. According to police records, Rick C. was found dead in his apartment at 1891 7th Street East on March 7, 2025. According to police, Rick C. appeared to have been deceased for some period of time before police found him. DHS records show that Rick C. was receiving ICS services from Ultimate Home Health at the time of his death.

43. According to Rick C.'s mother, Rick C. moved into 1891 7th Street East in or about June 2024. He suffered from significant mental illness, and this was the first time he was living on his own. When Rick C.'s mother first visited him at his new apartment, she was concerned about the living situation. She did not see any staff to assist him. Rick C.'s mother visited him at least once a week, generally staying for the entire day. She rarely saw anyone at the apartment to assist Rick C. A month

after he moved in, Rick C.'s mother noticed that he had stopped taking his medication. She explained that Rick C. was schizophrenic and needed his medication to control his mental illness.

44. Rick C. signed a release allowing his mother to obtain and access his medical records. Rick C.'s mother explained that she had no idea what services United Home Health was billing for. She said that they were not providing anywhere near the care for which they were billing Medicaid.

45. According to Police records, St. Paul Police questioned an Ultimate Home Health Services employee at the scene of Rick C.'s death on March 7, 2025. The employee said that he had last seen Rick C. the day before in the morning. The employee said Rick C. was "one of the most independent, you know, residents here. So, we don't got to do much checking on him." When asked if Rick C. used drugs, the Ultimate Home Health Services employee said, "I mean, to be honest, I do my daily check-ins, I have no idea what he does."

46. This statement was inconsistent with the Medicaid claims submitted by Ultimate Home Health Services. According to DHS records, United Home Health claimed to be providing 12 hours of services a day to Rick C., for which they billed Medicaid approximately $460 a day.

47. On or about November 20, 2025, KARE 11 ran a story about fraudulent billing by Ultimate Home Health Services.[2] In the wake of that report, DHS

[2] A.J. Lagoe, Kelly Dietz, Steven Eckert, Gary Knox, "KARE 11 Investigates: Death raises new fraud allegations in Minnesota's Medicaid-funded ICS program," KARE 11 November 20, 2025, available at https://www.kare11.com/article/news/investigations/kare-11-

suspended payments to Ultimate Home Health due to suspected fraud. In a statement, DHS explained that it was suspended payment due to "credible allegations of fraud involving the provider billing DHS for services that were not provided."

COMPUTER SEARCHES AND TECHNICAL TERMS

48. Based on my experience and the experience of other law enforcement agents, as well as on information obtained in the investigation, documents maintained in the normal course of business by medical providers include: dispensing orders; original detailed written orders; recipient's diagnosis from the testing physician; proof of delivery documentation; purchase records; shipment records; billing records; employee work records; and financial records. It is common for equipment and supplies providers to maintain current such records in the place of business and/or at storage facilities.

49. It is also common to maintain at least some of purchase, shipment, financial, billing, client records, employee records, and information in electronic form on computers. Such records assist law enforcement in identifying fraudulent schemes of the business, personal income and expenses, as well as business' assets and liabilities, and can be used to identify the receipt of funds derived from criminal activity, as well as trace the ultimate disposition of those funds.

---

investigates-unattended-death-raises-new-fraud-allegations-minnesota-medicaid-funded-ics-program/89-61240443-b8c1-4a60-969b-0b601c5fbd5d (last accessed Dec. 16, 2025).

50. Because this warrant requests permission to search any seized computer(s) or computer-related materials as defined below, a technician specially trained in the use and retrieval of information from computers will assist law enforcement with their search of any computer(s) or computer-related equipment. It is believed the computer(s) will contain both evidence of criminal activity, as well as be an instrumentality of the crime itself.

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

52. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

53. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

54. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

55. 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 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).

56. *Probable cause.* I submit that if a computer or storage medium is found at 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:

57. 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.

58. 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.

59. 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.

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

61. *Forensic evidence.* As further described in Attachments B-1 through B-8, 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 inculpating or exculpating the computer owner. Further,

computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

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.

62. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

63. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site

review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

64. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

65. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools

or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

66. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

67. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

68. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

69. 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 violations of Title 18, United States Code, Section 1343 (wire fraud), Section 1347 (healthcare fraud), and Section 1349 (conspiracy to commit wire fraud and healthcare fraud) as described in Attachment B, can be found at the Subject Premises, as further described in Attachment A.

Respectfully submitted,

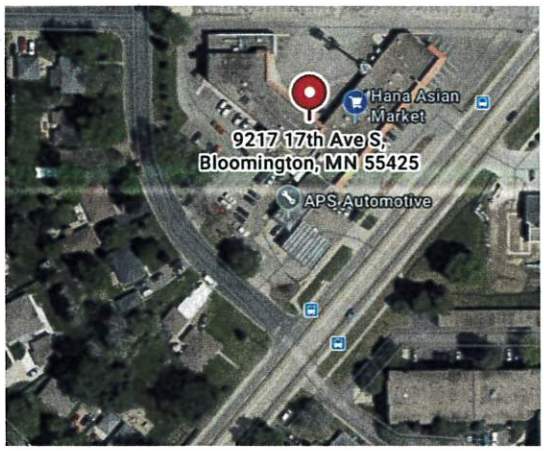
FBI Special Agent Jared F. Kary

SUBSCRIBED and SWORN before me
on December 18, 2025

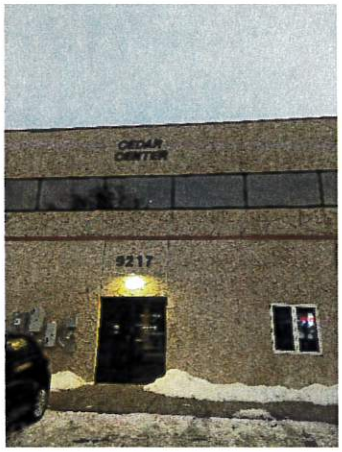
The Honorable David T. Schultz
United States Magistrate Judge

ATTACHMENT A
Location to be Searched

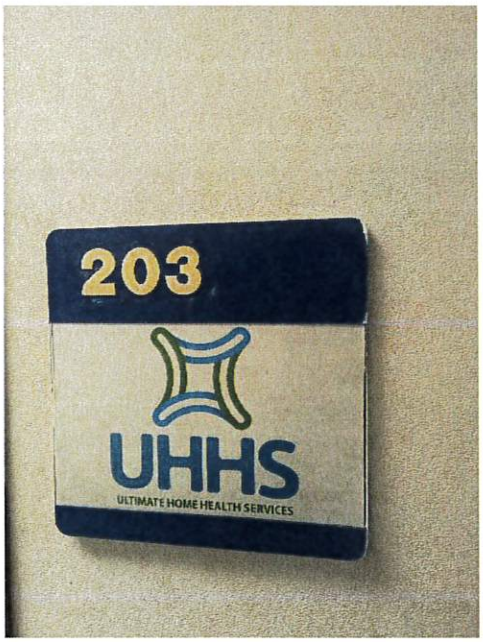
The **Subject Premises** is a business office suite, numbered 203, located inside a multi-tenant commercial-office building at 9217 17th Avenue South in Bloomington, Minnesota. 9217 17th Avenue South, Bloomington, Minnesota is two-story building, known as Cedar Center (Office Plaza). The front of the building is stucco tan in color.



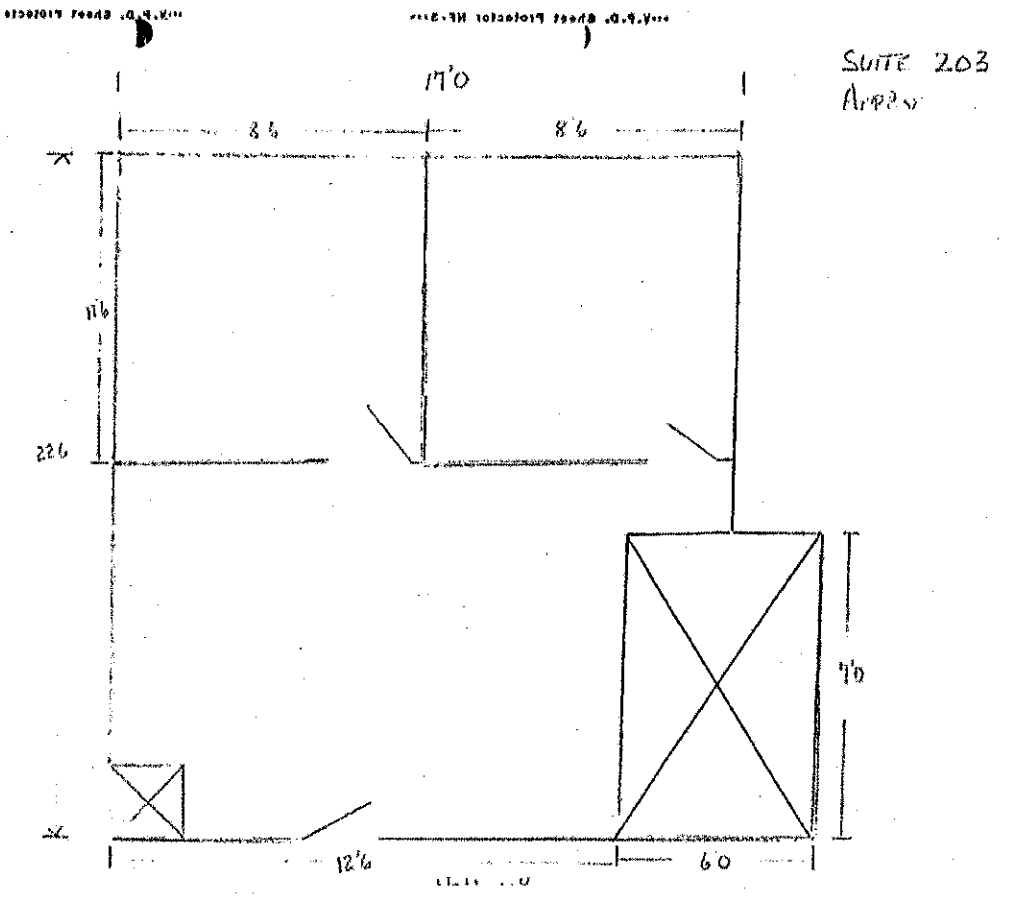
(Photos below taken on December 16, 2025)



There are several office suites located in the interior of the building. The **Subject Premises** is suite 203, located in the interior of the building, on the second floor. A sign indicating "203 UHHS, Ultimate Home Health Services LLC" is fixed to the wall directly next to the door. Above the door is number "203" indicating the suite number.



Additionally, the leasing manager provided, as part of the lease agreement with Ultimate Home Health Services LLC, the sketch of suite 203. (*see below*)



ATTACHMENT B
Particular Things to be Seized

All evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1347 (health care fraud), and 1349 (conspiracy to commit wire fraud and healthcare fraud), for the period of January 1, 2020, through the present, related to a scheme of false billing for Integrated Community Services (ICS), including the following:

1. All documents, correspondence, or information related to the operation of the ICS program including applications, bills, claims, invoices, records, reimbursements, contracts, site locations, and identification of clients served and HSS service providers employed.

2. All correspondence or communication with the Minnesota Department of Human Services, any DHS-licensed MCOs, or other entities related to billing and reimbursements for HSS programming.

3. All personal financial documents, records, and information for Othman Kadar Mohamed and Hasan Abdulaziz Abshir, 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; and

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

4. All documents, records and information pertaining to Compassionate Inspiration LLC or other existing or prospective entities related to HSS or healthcare, including but not limited to the following:

a. Accounting records including financial statements, charts 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 the subject company, 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. Information that constitutes or is related to evidence of treatment or services provided to ICS clients.

8. Cash or cash equivalent, coins, stocks, bonds, gold, jewelry, watches or other proceeds of the fraud offense.

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. All documents, records, communications, photographs, videos, or other media tending to show use or spending of suspected fraud proceeds.

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

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

14. 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.

15. 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.

16. 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, ZIP disks, 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).

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

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

a. Cabinet and desk keys;

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

c. Safe and lock combination and keys.

19. 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.

20. 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.

21. 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.

22. 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 SUBJECT PREMISES DESCRIBED IN ATTACHMENT A

SEALED BY ORDER OF THE COURT

Case No.: 25-mj-861 (DTS)

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, incorporated here.

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

See Attachment B, 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 1, 2026
(not to exceed 14 days)

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

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 Magistrate Judge.

Date and Time issued: _____

_____
Judge's Signature

City and State: Minneapolis, MN

The Honorable David T. Schultz
United States Magistrate Judge
Printed Name and Title

Return

Case No.: 25-mj-861 (DTS)	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 clerk of courts.

Date: _____

_____
Executing officer's signature

_____
Print name and title

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Case No. 25-mj-861 (DTS)

IN THE MATTER OF THE SEARCH OF THE SUBJECT PREMISES DESCRIBED IN ATTACHMENT A	**SEALED BY ORDER OF THE COURT** PETITION OF THE UNITED STATES TO SEAL THE SEARCH WARRANT, APPLICATION, AFFIDAVIT, RETURN, PETITION FOR SEALING, AND ORDER

The United States of America petitions this Court to seal the search warrant and all associated attachments, applications, affidavits, returns, petitions, and orders in this matter.

1. On December 18, 2025, the Court issued a warrant authorizing the search of the subject premises described in Attachment A. On the same date, the Court ordered all documents filed in this matter sealed until the close of business on December 18, 2026.

2. The affidavit submitted in support of the search warrant sets forth facts regarding the investigation.

3. The search warrant documents include detailed and highly sensitive investigative information. Disclosing the information would jeopardize the ongoing investigation into alleged criminal offenses as well as the safety and security of agents who will be executing the search warrant.

4. Nondisclosure of the search warrant documents is necessary to prevent the ongoing investigation from being compromised. Immediate public filing of the search warrant documents would, among other things, jeopardize the safety of the

agents and officers executing the search. Disclosure would also provide witnesses, subjects, and targets an opportunity to destroy evidence or otherwise impede the investigation.

5. The Court's power to prevent disclosure of its files is well established. *See, e.g., Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978) ("Every court has supervisory power over some records and files and access has been denied where court files might have become a vehicle for improper purposes."); *In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 574 (8th Cir. 1988) ("[Search warrant] documents may be sealed if the district court specifically finds that sealing is necessary to protect a compelling government interest and that less restrictive alternatives are impracticable.").

6. Circumstances surrounding ongoing investigations constitute compelling government interests for sealing. *See id.* (finding sealing appropriate where warrant documents "describe[d] in detail the nature, scope and direction of the government's investigation and the individuals and specific projects involved," resulting in "substantial probability that the government's on-going investigation would be severely compromised if the sealed documents were released").

7. Further, search warrant affidavits with references to individuals other than the subjects of the warrant and/or with information revealing the nature, scope, and direction of the government's ongoing investigation may be sealed not only because there are compelling government interests justifying sealing, but also because less restrictive alternatives to sealing are impracticable. *Id.*

8. Based on the above, the United States petitions this Court to issue an Order Sealing the Warrant, Application, Affidavit, Return, this Petition, and the Sealing Order until the close of business on December 18, 2026, unless the United States shows a compelling interest for continued sealing thereafter.

Dated: December 18, 2025

Respectfully submitted,

DANIEL N. ROSEN
United States Attorney

/s/ Joseph H. Thompson
BY: JOSEPH H. THOMPSON
First Assistant United States Attorney

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Case No. 25-mj-861 (DTS)

IN THE MATTER OF THE SEARCH OF THE SUBJECT PREMISES DESCRIBED IN ATTACHMENT A

SEALED BY ORDER OF THE COURT

ORDER FOR SEALING

This Court, having reviewed the Petition of the United States, finds that the United States has shown a compelling interest in the sealing of documents in this matter because nondisclosure of the search warrant documents is necessary to prevent the ongoing investigation from being compromised.

This Court also finds that less restrictive alternatives to sealing are impracticable or not appropriate.

IT IS THEREFORE ORDERED that all documents filed in this matter are sealed until the close of business on December 18, 2026.

IT IS FURTHER ORDERED that these documents will be unsealed on the above date unless the United States shows a compelling interest for continued sealing.

_____
Date

_____
The Honorable David T. Schultz
United States Magistrate Judge