JEK:sdh

AO 106 (Rev. 04/10) Application for a Search Warrant

2015R00086

UNITED STATES DISTRICT COURT

for the
District of Minnesota

In the Matter of the Search of:

SALAMA CHILD CARE CENTER LOCATED AT 1411 NICOLLET AVENUE, MINNEAPOLIS, MINNESOTA

Case No. ~~9E~~ 15-mj-343 (JSM)

APPLICATION FOR A SEARCH WARRANT

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

SALAMA CHILD CARE CENTER LOCATED AT 1411 NICOLLET AVENUE, MINNEAPOLIS, MINNESOTA

located in the State and District of Minnesota (further described in **Attachment A**), there is now concealed:

See attached list of items to be seized (**Attachment B**).

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 641	Theft of Public Money
Title 18, United States Code, Section 1343	Wire Fraud
Title 18, United States Code, Section 1028(a)	Aggravated Identity Theft

The application is based on these facts: **See attached Affidavit.**

Applicant's Signature

Kathryn Morrissey, FBI Special Agent
Printed Name and Title

Sworn to before me and signed in my presence.

Date: 5/12/15

Judge's Signature

City and State: Minneapolis, MN

Janie S. Mayeron, U.S. Magistrate Judge
Printed Name and Title

15-mj-393 CJSM

STATE OF MINNESOTA)
) ss. **AFFIDAVIT OF KATHRYN MORRISSEY**
COUNTY OF HENNEPIN)

I, Kathryn Morrissey, being duly sworn under oath, hereby depose and state as follows:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been so employed for more than five years. I am currently assigned to one of the two white collar crime squads within the Minneapolis Field Office. As such, I am primarily responsible for investigating Civil Rights violations, including human trafficking. I am also responsible for investigating fraud committed against the United States government, including allegations of child care fraud.

2. In addition to successfully completing New Agent Training at the FBI Academy in Quantico, Virginia in November 2009, I also completed the FBI Criminal Investigative Division Stage Two School in August 2011. Since that time, I have received additional formal and informal training related to white collar crime investigations, and I have assisted in multiple search warrants and arrests related to financial fraud investigations. While employed by the FBI, I have participated in numerous investigations in which I have collected evidence in electronic and in paper form.

3. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510 (7) of Title 18, United States Code, in that I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

4. The statements in this affidavit are based in part on my own investigation, my training and experience as a Special Agent of the FBI, and information provided to me by others, including but not limited to: law enforcement officers and civilian investigators from the United States Department of Health and Human Services (HHS); the Internal Revenue Service (IRS); the Minnesota Bureau of Criminal Apprehension (BCA); the Hennepin County Fraud Investigations Unit (HCF); and the Minnesota Department of Human Services (DHS).

5. Because this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause that evidence, contraband, fruits, and instrumentalities of violations of federal law will be found at or in the Subject Premises, **Salama Child Care Center** ("Salama"), located at **1411 Nicollet Avenue, Minneapolis, Minnesota**. There is reason to believe that the location listed above will contain evidence of violations of Title 18, United States Code, Sections 641 (Theft of Public Money), 1343 (Wire Fraud), and 1028A (Aggravated Identity Theft). The Subject Premises are further described in Attachment "A."

6. In summary, the following affidavit sets forth facts that establish there is probable cause that the subjects of this investigation caused the transmission by wire of fraudulent transactions involving programs receiving federal funding, and that evidence of such activity may be located within the Subject Premises.

PERTINENT FEDERAL CRIMINAL STATUTES

7. Title 18, United States Code, Section 641 prohibits a person from receiving, concealing, or retaining public funds with the intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted.

8. Title 18, United States Code, Section 1343 prohibits a person from having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, by means of wire transmission.

9. Title 18, United States Code, Section 1028A prohibits a person from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another, during and in relation to other enumerated felony offenses including Theft of Public Money and Wire Fraud.

OVERVIEW OF THE CHILD CARE ASSISTANCE PROGRAM

10. The Administration for Children and Families (ACF) is an agency within the HHS. One program under the ACF is child care assistance, which is administered in Minnesota by counties and DHS. Child care assistance is jointly funded by HHS and the State of Minnesota, with roughly fifty percent of funding coming from HHS and the other roughly fifty percent coming from the State of Minnesota. Each year, ACF provides federal funding to states to subsidize the cost of child care for low-income families. This federal investment provides early care and education services for children in Minnesota each month and supports a host of efforts to improve the quality and supply of child care for all families.

11. The Minnesota Department of Human Services-Child Care Assistance Program (CCAP) was designed to help make child care affordable for income-eligible families. Families have a copayment requirement based on their gross income and family size, and most families on Minnesota Family Investment Program (MFIP) child care have a copayment of $0. Child Care Assistance is available to: families participating in MFIP or Diversionary Work Program (DWP); families that had an MFIP or DWP case closed within the last 12 months; and low-income families that may be eligible for the Basic Sliding Fee program.

12. CCAP pays child care costs for children age 12 and younger, and for children with special needs up to age 14. Child care costs may be paid for qualifying families while they go to work, look for work, or attend school. To qualify for CCAP, families must comply with child support enforcement, if applicable, for all children in the family. Care must be provided by a legal child care provider over the age of 18. Family size, family income, and participation in authorized activities are considered. The amount of available funding also may be a factor.

13. There are maximum reimbursement amounts for child care providers who serve families participating in CCAP. Maximum reimbursement rates vary by the age of the child, the type of provider, and the location where care is provided. The rate paid to a provider caring for a child through CCAP cannot be higher than their typical private pay charge.

14. Families may select any licensed child care center, family provider, or legally non-licensed family provider to care for their children. DHS is responsible for

approving the licenses of centers and family providers. In addition, the chosen child care providers must have a service authorization with the particular counties in which the children receiving the child care reside. Child care providers submit child care claims directly to the county where the child being cared for resides in order to receive reimbursement for child care services. The reimbursements are paid by the state of Minnesota through DHS.

CHILD CARE PROVIDER REQUIREMENTS

15. Child care providers are required to comply with various requirements designed to ensure that providers are providing quality care to children. In addition, providers are required to submit reimbursement claims that accurately reflect the services that were actually provided. Child care providers are informed of the requirements that govern their participation in CCAP. The guidelines include billing procedures, which are available in the CCAP Child Care Manual and online at the DHS website. Through a computer program called MEC2Pro, child care providers are able to access the Child Care Assistance Program Child Care Provider Guide and the Child Care Assistance Program Policy Manual. In addition, the CCAP Provider Guide and Child Care Provider and Responsibilities and Rights sheet are sent to providers as part of the application and renewal packet for registration with the counties.

16. With only a few exceptions, child care centers must be licensed by DHS. Providers must notify the county where they are registered immediately of any changes to the information submitted on their registration form. In addition, child care providers

must have a service authorization with the counties where the children reside before payment can be approved.

17. Registered child care providers are required to keep daily attendance records on-site for a period of the last six months. The provider is responsible for maintaining the attendance records for six years from the date that service is provided. Specifically, as it pertains to this investigation, Hennepin County requires that providers maintain the following information as a record of a child's attendance: date of service; name of child; parent/guardian signature; and the sign-in and sign-out times.

BILLING AND BILLING PROCEDURES

18. Using MEC2Pro, child care providers may access and submit via the internet electronic child care assistance billing forms. Providers bill on a two-week cycle. When a provider or their designee accesses the online billing system, they must use a unique user name and password. The license holder determines who is approved to access the online system on behalf of the provider. Some counties permit providers to receive billing forms through the mail. The billing forms are for each family and list each child by name, along with the family's county identification number.

19. Regardless of whether a provider is submitting the billing form electronically or in paper form to one of the counties that permit or require paper billing forms, the provider completes the billing forms by filling in the number of hours of child care provided to each child for each day in the two-week billing cycle on which child care services were provided to that child. The provider is also responsible for indicating in the billing forms a child's absence or a holiday. DHS rules permit providers to be

reimbursed on days that a child is absent, up to 25 days per year. The provider signs the billing forms—electronically in the case of billing forms submitted electronically—certifying that the information reflected on the forms is accurate. The provider then submits the billing forms to the county for reimbursement.

20. If a child care center is closed, the provider is not allowed to bill DHS for those hours or days (s) of service, unless it is closed due to a designated holiday. Child care providers are allowed to bill for ten recognized state and federal holidays per year, which are listed by DHS. A child care provider that wishes to observe alternate holidays for religious or cultural reasons can substitute them for the official holidays listed so long as the provider gives advance notice to the county child care administrator. The holiday should be identified on the billing claim form for each child in the attendance box.

21. DHS pays for child care services at different rates for infants, toddlers, preschoolers, and school age children. In addition, those rates vary from county to county.

DEFINITIONS

22. The following non-exhaustive list of definitions applies to this Affidavit and any attachments to this Affidavit:

a. "Computer" as used herein, is defined pursuant to 18 U.S.C. 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. "Computer hardware" as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. "Computer software" as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

d. "Computer-related documentation" as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. "Computer passwords and data security devices" as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security

hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Internet Service Providers" or "ISPs" are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

g. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information,

account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

h. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses can also be static if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic, or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video discs (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory

sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

BACKGROUND ON COMPUTERS AND FRAUD

23. Based upon my knowledge, training, and experience in white collar crime investigations, and the experience and training of other law enforcement officers with whom I have worked, computers and computer technology have revolutionized the way in which fraud can be conducted.

24. The Internet, the World Wide Web, and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing, and locating person's identities, for communicating with others to do so, or for filing false or fraudulent documents for reimbursement.

25. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files for tax records in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of tax records is often found on the user's computer. Even in cases where online storage or a third party software program is used, evidence of fraud can be found on the user's computer in most cases.

26. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked"

files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

27. Importantly, the interplay between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of theft of public money and wire fraud.

28. Data that exists on a computer is particularly resistant to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person deletes a file on a home computer, the

data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

PROCEDURES FOR COMPUTER SEARCH

29. Based on my training and experience, I know that computer hardware and computer software may be used to store records which relate to both business activities and criminal activities. Based on my training and experience, I also know that:

a. Electronic data can be recovered from a computer or hard drive or disk, even if it has been erased;

b. Computer users often keep computer hardware, software, and electronic data in their offices;

c. Computer users often use backup copies of data and software to protect against loss of that data if their computer malfunctions, and they keep these backup copies on their person, in their vehicles, at their residence, and at their business; and

d. Persons utilizing the computer to commit crimes often attempt to conceal evidence of the crime from law enforcement.

30. Based on my training and experience, businesses generally retain customer transactional and financial information and records for a period of years.

31. Based upon my knowledge, training, and experience, I know that searching and seizing information from computers often requires law enforcement officers to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence: Computer storage devices can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal evidence; he or she might also store it in random order with deceptive file names. 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 often it would be impractical to attempt this kind of search on site.

b. Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. For example, on-site and laboratory analysis by a qualified computer specialist is often required in order to properly retrieve and analyze electronically stored (computer) data, to document and authenticate the data, and to prevent the loss of the data either from accidental or deliberate destruction. In many cases, the evidentiary data can

be backed up to government-owned computer data storage devices at the site of the search. However, there are circumstances that may necessitate the seizure and removal of the entire computer system and peripheral devices to a secure laboratory setting in order to analyze and extract the evidence.

32. Accurate and complete analysis may require seizure of all computer equipment and peripherals which may be interdependent, the software to operate the computer system, data security devices (including passwords), and related instruction manuals which contain directions concerning the operation of the computer system and software programs. This is true because the peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software.

33. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the computer expert be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence. In addition, the computer expert needs the relevant system software (operating systems, interfaces, and hardware drivers) and any application software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

OVERVIEW OF INVESTIGATION

34. I am conducting an investigation along with law enforcement personnel from IRS, HHS, and BCA regarding a child care center operating under the name Salama Child Care Center, and located at 1411 Nicollet Avenue, Minneapolis, Minnesota 55403.

In December 2009, Ardo Y. Diriye was listed as the license holder on the application that was submitted to DHS requesting a license be issued for Salama. Farah Y. Aidid was listed on the application as the controlling individual and the program director. In 2013, Salama submitted a licensing update form reporting that the program director was an individual named Fozia Sheik Ali. A check of Hennepin County records revealed that Farah Yusuf Aidid was granted a name change to Fozia Sheik Ali in November 2011.

35. The focus of the investigation is on the number of children attending Salama whose child care costs are being reimbursed through CCAP funds. The investigation has revealed that a large discrepancy exists between the number of children actually attending and receiving care at Salama and the number of children for which Salama seeks and receives reimbursement via billing forms submitted electronically via MEC2Pro.

36. In my training and experience and based on information learned from other law enforcement agents who have investigated cases of billing fraud by child care providers, child care providers who fraudulently submit bills to DHS accomplish the fraud by billing for children who do not actually attend the child care center or by billing for more hours than the child care services were actually provided, or both. Child care providers frequently obtain the cooperation of parents to participate in the fraud scheme with the providers. In order to entice the parents, providers pay a portion of the child care reimbursement money to the parents in exchange for the ability to use the CCAP families' identifying information to submit billing form to the various counties. Occasionally, the payments to parents are disguised by "hiring" parents as employees of

the child care center. In many cases, parents do not work at the child care centers and their children do not attend the child care centers.

37. Salama has been approved to provide care for 60 children at one time. Information obtained during this investigation indicates that in March 2015, Salama had approximately 229 children enrolled in CCAP for that month alone. Law enforcement officers and civilian investigators have conducted surveillance of Salama on a number of days between December 2013 and April 2015, including the days identified in the chart below. Although Salama has three entrances, surveillance indicates that children attending Salama always enter through one particular door, the front door, which faces Nicollet Avenue. On the days identified in the chart below when surveillance was conducted, the front door was constantly monitored during the entire portion of the day when individuals were present at Salama. A comparison between observations made during surveillance and a review of billing records submitted by Salama showed that Salama has billed for more children than were actually present, as described in more detail in the chart below. There were numerous other days in addition to those identified below when Salama billed for more children than were observed during surveillance as being present.

Date of Service	**Number of Children Observed at Salama (Approximately)**	**Number of Children Billed for by Salama (Approximately)**	**Number of Children Overbilled (Approximately)**
12/20/2013	37	99	62
12/30/2013	30	111	81

01/01/2014	0	7	7
01/23/2014	44	150	106
01/27/2014	25[1]	132	107
02/02/2014	16	29	13
01/02/2015	41	103	62
01/08/2015	71	146	75
01/19/2015	0	5	5
01/21/2015	92	136	44
04/11/2015	31	59	28
04/12/2015	35	56	21

38. As indicated in the chart above, physical surveillance established that on both January 1, 2014, and January 19, 2015, Salama provided no child care services and was in fact closed. Billing forms submitted by Salama, however, claimed that several children were present and received services. The billing forms did not include a holiday designation for the above dates, nor an "absent" designation to count toward the 25 absent days permitted by CCAP. Rather, the billing forms represented that Salama was open and that children were in attendance on those dates.

39. Through this investigation, law enforcement personnel have determined that Salama has only one MEC2Pro account and that Salama consistently uses that

[1] Surveillance personnel observed a total of 24 children entering the building and a total of 25 exiting the building. The analysis in the chart above credits Salama with 25 children.

account to submit billing forms to the various counties, including the billing forms that would have been for the dates of service identified in the chart in paragraph 37 above. The USER ID on that account is for Farah.a@salamachildcarecenter.com, which I believe to be for Farah Aidid (now named Fozia Ali), the name listed on the original license application as the "Controlling Agent" of Salama Child Care Center. Fozia Ali is also listed as the point of contact for Salama Child Care Center in MEC2Pro records that are accessible to DHS. According to a DHS licensing employee, Fozia Ali identified her cellular telephone number as being (952) 564-9218. The DHS licensing employee KM also indicated that Fozia Ali's cell phone was a Smartphone. JM

40. On May 6, 2015, investigators working on this investigation learned that a T-Mobile IP address 172.56.12.54 accessed the Farah.a@salamachildcenter.com account in MEC2Pro. Also on May 6, 2015, Fozia Ali represented to a DHS licensing employee that the best way to reach her was on her cell phone (952) 564-9218. Records obtained from T-Mobile regarding cellular phone number (952) 564-9218 revealed that the account holder is Mohamed Ibrahim at 500 Cambridge Street, Apartment 303, Hopkins, Minnesota. Investigators have confirmed that Fozia Ali resided at 500 Cambridge Street, Apartment 303, Hopkins, Minnesota, prior to moving to apartment number 322 in the same building and that Mohamed Ibrahim is Fozia Ali's son and lives with Fozia Ali.

41. Based on the information listed above, it is believed that the MEC2Pro website is being accessed by a browser on Fozia Ali's cellular phone or that her cellular phone is being used as a mobile "hot spot" to permit another computer to connect via the internet to submit billing forms for Salama via MEC2Pro. Thus, it is believed that

evidence of Fozia Ali accessing the MEC2Pro website for the purpose of completing attendance and/or billing records for Salama will be located on Fozia Ali's cellular phone.

LOCATIONS TO BE SEARCHED

42. In my training and experience, I have learned that when individuals and businesses are engaged in criminal activity of the nature outlined here, evidence of that activity can be found at the place of business of the perpetrating agency or individual. Individuals also maintain records which show the possession of assets and personal financial transactions within their businesses. Evidence that can corroborate allegations of theft and fraud include, but is not limited to, the child care provider's personnel files and client files; documents related to the provision of child care services; documents related to the management and/or billing practices of the child care provider; records demonstrating ownership, control, affiliation, and/or the operation of the child care provider; financial records; and the other categories of documents and records identified in Attachment A ("Items to be Seized"). Providers retain their records in paper form, and also electronically. Providers have computer programs designed to assist them in operating a business, but which may include pertinent information regarding the provider's services, employees, payroll, and billing.

43. In particular, Salama is expected to keep certain records related to the provision of child care services on site at Salama, such as personnel files and client files; documents related to the provision of child care services; documents related to the management and/or billing practices of the child care provider; records demonstrating ownership, control, affiliation, and/or operation of the child care provider; financial

records; and the other categories of documents and records identified in Attachment B ("Items to be Seized"). In fact, many records falling within the above categories of records are required by CCAP to be physically kept on site.

44. Through my training and experience, I have learned that financial records and correspondence help determine business and/or personal income and expenses. They can also contain personal financial information which may be evidence of how money/profits obtained through fraud are being used to further personal interests and/or expenses. In other words, financial information can be used to identify the receipt of funds derived from criminal activity, as well as trace the ultimate disposition of those funds. Through this investigation, copies of Salama bank records have been obtained. Some of the financial statements and correspondence indicate that 1411 Nicollet Avenue, Minneapolis, Minnesota, is the mailing address for Salama Child Care Center.

45. I have learned that child care centers are required to maintain records for a period of 6 years. Due to the fact that Salama was first licensed in December 2009, such records are expected to be found at the Subject Premises described in Attachment A. In addition, as of April 2015, the Office of the Minnesota Secretary of State lists the "Principal Executive Office Address," "Registered Office Address," and the address of the "Chief Executive Officer" for Salama Child Care Center as 1411 Nicollet Avenue, Minneapolis, Minnesota 55403.

46. Accordingly, your Affiant submits there is probable cause to believe that evidence of the fraud and other crimes as will be found at the location described in Attachment A.

CONCLUSION

47. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that contraband, evidence, fruits and instrumentalities of violations of 18 U.S.C. § 641, 18 U.S.C. § 1343, and 18 U.S.C. § 1028A will be located at 1411 Nicollet Avenue, Minneapolis, Minnesota 55403.

42. I therefore, respectfully request that the attached warrant be issued authorizing the search of premises described further in Attachment A and seizure of the items described further in Attachment B.

Further your Affiant sayeth not.

Kathryn Morrissey, Special Agent
Federal Bureau of Investigation

Subscribed and Sworn to before
me this 13th day of May, 2015.

JANIE S. MAYERON
United States Magistrate Judge

Attachment A
Place(s) To Be Searched

1. 1411 Nicollet Avenue, Minneapolis, Minnesota 55403, is part of a multi-unit building, which is adjacent to The Music Box theatre.

2. The building is brick and stone and has a mural/painting, green in color, on the south side of the building which says "Salama Child Care Center" in black letters.

3. The windows on the west side of the building near the entrance are tinted.

4. There is a parking lot located on the south side of the building.

5. The front entrance of the building faces Nicollet Avenue South.

Attachment B
Items To Be Searched for and Seized

1. Any and all records that show ownership, control, affiliation, and operation of any of the above-listed entities, or any other companies, entities, investments, or assets associated with Farah Aidid, Fozia Ali, Ardo Diriye, or Salama Child Care Center, including but not limited to, articles of incorporation, corporate resolutions or minutes, other business or corporate records, corporate memoranda, by-laws, shareholder information, service agreements, contracts, partnership agreements, memoranda of understanding, and other documents evincing ownership, control, affiliation, and operation.

2. Financial statements and reports, ledgers, journals, contracts, agreements, statements, bills, invoices, banking and loan records, financial institution records, customer records, correspondence, facsimiles, memorandum, tax-related records or other records utilized in the preparation of tax filings, travel records, and other records related to revenues, expenses, assets, liabilities, financial obligations, capital expenditures, and the receipt, disposition, or expenditure of income, monies, funds, or assets.

3. Personnel files/employee information for all employees and/or independent contractors including, but not limited, to applications for employment, background checks, background study clearance reports, payroll records, employment tax returns, 1099, W-2 and W-4 forms, credentials, teaching certificates or licenses, orientation schedules and attendance records, training provided and attendance records, performance evaluations, informal supervisor files or notes, disciplinary actions records, incident reports, internal investigations, staff meeting attendance records, and correspondence.

4. Property records, receipts, investment records, stock and bond records, mortgages, 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, or property.

5. Any (without regard to the entities/person listed above) money orders, bank or cashier's checks, cash and currency, negotiable instruments, monetary instruments, jewelry and precious metals, art work, and collectibles.

6. Address books, photographs, and other documents or items tending to show the identities of associates or co-conspirators, or tending to identify the location or possession of criminally-derived property.

7. Documents or other items tending to show occupancy, residency, ownership, or possession of the premises and residences to be searched.

8. Documents submitted to the State of Minnesota, United States Government, or any governmental agency within the State of Minnesota related to the operation of the day care center.

Computer Hardware, Software, and Access Devices

9. Any computers, as defined in 18 U.S.C. §1030(e) (1), (and related instructions or manuals) that contain any of the records, information or objects described above, including but not limited to:

(a) data processing devices such as desktop computers, laptop computers, Palm Pilots or other personal digital assistants ("PDA's"), file servers, Smartphones, or mainframe computers;

(b) peripheral computer equipment such as a keyboards, monitors, printers, scanners, CD "burners," or modems; and

(c) data storage devices such as hard disks, floppy disks, zip disks, CD disks, magnetic tapes, Smartphones, and other permanent or transient storage devices.

10. 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 manage and record transactions, including but not limited to Internet browsers, Internet access software, word processing programs, email software, banking software, business management tools, and accounting software.

11. 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.

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 floppy diskettes, hard disks, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, 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 microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).