

PT:LXN  
F. #2014R1200

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X

14-724 M

UNITED STATES OF AMERICA

- against -

FNU LNU, (Pictured in Exhibit A),  
also known as "Shlomo Dickerman,"  
'Stephen G. Dickerman' and  
'Stephen Dickerman'

Defendant.

AFFIDAVIT IN  
SUPPORT OF AN  
ARREST WARRANT  
AND SEARCH  
WARRANT

(18 U.S.C. §1001(a)(2),  
1028A(a)(1), 1028A(b),  
1028A(c)(4); Fed. R. Crim. P. 41)

-----X

-----X

UNITED STATES OF AMERICA

- against -

THE PREMISES KNOWN AND  
DESCRIBED AS THE OFFICE OF  
'SHLOMO G. DICKERMAN,' A  
CUBICLE-STYLE OFFICE SPACE,  
LOCATED AT 128 BRIGHTON 11<sup>th</sup> ST.,  
FIRST FLOOR, BROOKLYN,  
NEW YORK 11235,

-----X

EASTERN DISTRICT OF NEW YORK, SS:

Hannah M. Buch, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation (FBI), duly appointed according to law and acting as such.

On or about and between February 10, 2012 and February 24, 2012, within the Eastern District of New York and elsewhere, the defendant FNU LNU, , also known as ‘Shlomo Dickerman,’ ‘Stephen G. Dickerman’ and ‘Stephen Dickerman,’ did knowingly and willfully make one or more materially false, fictitious and fraudulent statements and representations, in a matter within the jurisdiction of the judicial branch of the Government of the United States, to wit: the defendant submitted an application to be admitted to practice law in the United States District Court for the Eastern District of New York (the ‘EDNY’) and swore an oath in which the defendant falsely represented that (1) his name was ‘Stephen G. Dickerman’ and (2) that he was an attorney and a member in good standing of the bar of the State of New York.

(Title 18, United States Code, Section 1001(a)(2))

On or about and between February 10, 2012 and the present, within the Eastern District of New York and elsewhere, the defendant FNU LNU, also known as ‘Shlomo Dickerman,’ ‘Stephen G. Dickerman’ and ‘Stephen Dickerman,’ did knowingly and intentionally possess and use, without lawful authority, means of identification of another person, to wit: the name ‘Stephen G. Dickerman,’ during and in relation to the crime of knowingly and willfully making materially false, fictitious and fraudulent statements and representations in a matter within the jurisdiction of the judicial branch of the Government of the United States.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), and 3551 et seq.)

The source of your deponent's information and the grounds for her belief are as follows:<sup>1</sup>

I. Background and Qualifications

1. I have been a Special Agent with the FBI for approximately nine years. I am currently assigned to a public corruption squad that investigates violations of federal criminal laws, including bribery and various forms of white collar crime. In this position, I have conducted physical surveillance, interviewed witnesses, reviewed documents obtained through the service of subpoenas, and used other investigative techniques to secure relevant information for use in criminal prosecutions.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative files; and reports of other law enforcement officers involved in the investigation.

II. Description of the SUBJECT PREMISES

3. Based on my observations, the SUBJECT PREMISES, further described in Attachment A, is the Office of "Shlomo G. Dickerman," which consists of a cubicle-style office space on the first floor of a two-story building located at 128 Brighton 11<sup>th</sup> St., Brooklyn, New York 11235. On the outside of the building is a large sign stating "LAW OFFICE" and the number "128." A photograph of the outside of the building in which the SUBJECT PREMISES is located is attached hereto as Exhibit B, and a photograph of the

---

<sup>1</sup> Because the purpose of this Affidavit is to set forth only those facts necessary to establish probable cause to arrest and to search the SUBJECT PREMISES, I have not described all the relevant facts and circumstances of which I am aware.

SUBJECT PREMISES is attached hereto as Exhibits C1 and C2. The SUBJECT PREMISES is on the first floor and is accessible by entering the front door of the building at the top of the stairs outside the building, walking past a receptionist's desk, entering a small hallway on the right and then walking down a flight of stairs; once at the bottom of the stairs, taking a right and walking past the first cubicle-style office space to a second cubicle-style office space, which is against the left, back wall. The SUBJECT PREMISES contains, among other things, a desk with a computer, two bookshelves, a black briefcase, a brown briefcase, multiple files and other papers.

4. I have reviewed a letter electronically filed with the EDNY by the defendant FNU LNU, , also known as "Shlomo Dickerman," "Stephen G. Dickerman" and "Stephen Dickerman," in the name of "Stephen G. Dickerman" on July 21, 2014. The letterhead of this letter lists the firm name as "Dickerman, Khan & Shpigel," and "128 Brighton 11<sup>th</sup> St. Suite 1, Brooklyn, NY 11235" as its "Kings County Office."

III. Probable Cause as to the SUBJECT PREMISES and for the Arrest Warrant

5. I have spoken with a representative of the New York State Unified Court System, Office of Court Administration, Attorney Registration Unit ("Attorney Registration Unit"), and have learned that when an individual is admitted to practice law in the State of New York, he or she is assigned a unique attorney registration number (the "Attorney Registration Number"). I have also learned that all attorneys admitted to practice law in the State of New York must renew their attorney registration every two years, within 30 days of their birthday.

6. I have spoken with an individual (hereinafter "Victim"), who showed me his New York State Driver's License verifying his identity, and have reviewed records from the

Attorney Registration Unit. I have learned, among other things, that Victim has been admitted to practice law in the State of New York since in or about 1970. In or about June 2004, Victim submitted a renewal application to practice law in the State of New York by filing a Form for Attorney Registration (the“Attorney Registration Form”) with the State of New York, Office of Court Administration (the“OCA”). The Attorney Registration Form contained Victim’s name, the year that he first had been admitted to the New York Bar, a business address in Manhattan (the“Manhattan Business Address”), a home address in Manhattan (the“Manhattan Home Address”), his social security number, date of birth, the name of the law school he attended, his Attorney Registration Number and Victim’s signature. In 2006, Victim again renewed his New York attorney registration by submitting an Attorney Registration Form with the same information. I have reviewed that 2006 Attorney Registration Form as well. In connection with each of these Attorney Registration Forms, Victim paid a registration fee of \$350 to the OCA.

7. From in or about May 2008 through in or about February 2009, the OCA repeatedly sent Victim renewal notices at both the Manhattan Home and Business Addresses via the United States mail notifying him that he was required to renew his attorney registration and owed an attorney registration fee of \$350. Victim did not respond to these notices, file the Attorney Registration Form or pay the \$350 registration fee. Accordingly, the Attorney Registration Unit classified Victim as“delinquent”in his registration.

8. In or about June 2009, an individual appeared in person at the Attorney Registration Unit’s Manhattan office. The individual claimed to be Victim and sought to renew his attorney registration. The Attorney Registration Unit provided the individual with

a copy of a 'Delinquent Notice' form, which reflected the fact that Victim had not timely renewed his attorney registration. The 'Delinquent Notice' contained Victim's name, the year that he first had been admitted to the New York Bar, the Manhattan Business and Home Addresses, the last four digits of Victim's social security number, his date of birth, the name of the law school he attended and his Attorney Registration Number. The Delinquent Notice contained a section where an applicant could make changes to his or her personal information. The individual sought to make three changes in that section: (1) he wrote the name 'Shlomo G. Dickerman' in an attempt to change Victim's name to 'Shlomo G. Dickerman,' (2) he listed 'Mitigation and Litigation Strategies Inc.' as the name of his business and provided a different Manhattan business address (the 'Penn Plaza Address'), and (3) he listed a home address in Nassau County, New York (the 'Nassau Address'). The individual signed the Delinquent Notice form in Victim's name, affirming that 'the statements contained herein are true to the best of my knowledge and belief.'

9. At or around the same time, the individual also paid the attorney registration fee of \$350 for Victim with a United States Postal Service money order (the 'Money Order'). I have reviewed a copy of the Money Order, which shows that it was paid to the order of the 'NYS Office of Court Admin' and listed the name 'Shlomo G. Dickerman,' the Penn Plaza Address and Victim's Attorney Registration Number in the payor section.

10. In or about May 2010, the Attorney Registration Unit mailed an Attorney Registration Form to Victim at the Nassau Address. A completed Attorney Registration Form and a Money Order for a \$350 registration fee were returned to the Attorney Registration Unit. I have reviewed a copy of this Money Order, which shows that it was paid

to the order of the 'NYS Office of Court Administration, Attorney Reg. Unit' and listed the name 'Shlomo G. Dickerman JD LLM; c/o Mitigation and Litigation Strategies Inc.,' and the Penn Plaza Address in the payor section. I have also reviewed the 2010 Attorney Registration Form, which contained a section where changes to personal information could be made. The only change was that the name 'Shlomo G. Dickerman' was written in an attempt to change Victim's name to 'Shlomo G. Dickerman.' The 2010 Attorney Registration Form was signed 'Shlomo G. Dickerman JD, LLM,' affirming that 'the statements contained herein are true to the best of my knowledge and belief.'

11. A letter, purportedly written and signed by 'Shlomo G. Dickerman, J.D., LLM' was returned to the Attorney Registration Unit with the 2010 Attorney Registration Form. This letter requested that the Attorney Registration Unit change Victim's name to 'Shlomo G. Dickerman,' because 'Shlomo' was 'Hebrew' for Victim's first name. The letter further noted the same request had been made the previous year, in 2009, when the attorney registration fee was paid. Finally, the letter requested that any subsequent Attorney Registration Form be sent to the Penn Plaza Address.

12. I have also reviewed Attorney Registration Forms for 2012 and 2014, which the Attorney Registration Unit mailed to Victim at the Penn Plaza Address, and which were subsequently filed with the Attorney Registration Unit. In 2012 and 2014, the \$375<sup>2</sup> registration fee was paid with checks from 'Mitigation & Litigation Strategies Inc.' In 2012, in the section where changes to personal information could be made, the name 'Shlomo G.

---

<sup>2</sup> The attorney registration fee increased from \$350 to \$375.

Dickerman' was written in an attempt to change Victim's name to "Shlomo G. Dickerman" based on "religious reasons." Both the 2012 and 2014 Forms were signed "Shlomo G. Dickerman," affirming that "the statements contained herein are true to the best of my knowledge and belief."

13. I have spoken with a representative of the Attorney Registration Unit and learned, among other things, that (1) there is no record indicating that a "Shlomo G. Dickerman" is or has ever been a member of the Bar of the State of New York, and (2) the Attorney Registration Unit does not change the name of registered attorneys without legal documentation of a legal name change. Accordingly, the Attorney Registration Unit did not change Victim's name despite the efforts to change that name described in paragraphs 8, 10, 11 and 12 above.

14. I have spoken with Victim and learned, among other things, that (1) Victim has never gone by the name "Shlomo;" (2) Victim has never been associated with "Mitigation and Litigation Strategies Inc." or bank accounts held in that name; (3) Victim did not appear in person at the Manhattan office of the Attorney Registration Unit in or about June 2009 and did not file or sign a "Delinquent Notice" at that time; (4) Victim has never, after 2008, attempted to renew his New York State attorney registration or pay an attorney registration fee; and (5) Victim did not use the Penn Plaza or Nassau Addresses for any purpose.

15. I have reviewed a copy of a Petition for Admission (the "Petition") filed on February 10, 2012, in connection with an application (the "Application") to be admitted to practice as an attorney in the EDNY. Victim is identified in the Petition as the attorney seeking admission to the EDNY. The Petition and Application reflect, among other things, the following:

- a. A statement that the attorney signing the Petition is a member of the bar in good standing in the State of New York;
- b. The purported signature of Victim on both documents;
- c. A certificate of good standing issued for Victim by the Appellate Division of the Supreme Court of the State of New York, First Judicial Department;
- d. The name of the law school that Victim attended;
- e. A statement that the attorney seeking admission to the EDNY had also received an LL.M. degree from New York University Graduate School of Law (‘NYU’);
- f. The Nassau Address; and
- g. The Penn Plaza Address.

16. I have reviewed a copy of an Oath of Admission (the ‘Oath’), sworn and subscribed to on or about February 24, 2012, before the Honorable Lois Bloom, United States Magistrate Judge, EDNY. Victim is identified as the attorney taking the oath of admission.

The Oath also reflects, among other things, the following:

- a. The purported signature of Victim;
- b. The name of Victim’s purported law firm, ‘Sirota & Assoc PC’ and a business address of ‘128 Brighton 11<sup>th</sup> Street, Brooklyn, New York 11235’;
- c. Victim’s purported business telephone number;
- d. Victim’s purported business email address; and
- e. The last four digits of Victim’s social security number.

17. I have reviewed records from NYU, which reflect that NYU never conferred an LL.M degree on anyone with the name of Victim or ‘Shlomo Dickerman.’

18. I have reviewed a database available to law enforcement, which shows that the law firm of "Sirota & Associates, P.C." is located at "128 Brighton 11<sup>th</sup> St., Ste. 2, Brooklyn, New York, 11235."<sup>3</sup>

19. I have spoken with Victim and learned, among other things, that (1) Victim has never sought to be admitted to the EDNY and has never appeared in the EDNY; (2) Victim has never signed a Petition for admission to the EDNY; (3) Victim did not appear before Judge Bloom or any other judge on February 24, 2012 or on any other date, to be sworn into the EDNY; (4) Victim has never been associated with a firm or business containing the name "Sirota;" (5) Victim has never been associated with the address "128 Brighton 11<sup>th</sup> Street, Brooklyn, New York 11235;" or with the business telephone number and email address listed in the Oath; and (6) Victim has never received an LL.M. degree from NYU.

20. I have reviewed a civil complaint (the "Complaint") filed electronically in the EDNY on or about May 7, 2014.<sup>4</sup> Victim is identified as the attorney filing the Complaint. I have also reviewed a "Civil Cover Sheet" (the "Cover Sheet") filed in the EDNY, together with the Complaint. The Cover Sheet reflects, among other things, the following:

---

<sup>3</sup> To be clear, the government is only seeking to search for materials located within the SUBJECT PREMISES, and not in other areas of 128 BRIGHTON 11<sup>th</sup> ST., BROOKLYN, NEW YORK 11235. Specifically, the government is not seeking to search the second floor or Suite 2 of 128 BRIGHTON 11<sup>th</sup> ST., BROOKLYN, NEW YORK 11235, or any other part of that building other than the SUBJECT PREMISES.

<sup>4</sup> Based on my review of court filings, the defendant has appeared as an attorney in approximately seven other cases in the EDNY since 2009. The defendant has also appeared as an attorney in approximately three cases in the United States District Court for the Southern District of New York (the "SDNY"). I have spoken with Victim, who has stated that he has never appeared as an attorney in the EDNY or the SDNY.

- a. A statement that Victim is an attorney admitted to practice law in the EDNY;
- b. A statement that Victim is a member of good standing with the 'bar of this court';
- c. A statement that the information provided in the Cover Sheet is accurate; and
- d. The purported signature of Victim in two separate places.

21. I have compared the signature of Victim in the 2004 Attorney Registration Form to the purported signatures of Victim in the 2008 "Delinquent Notice," the 2010 and 2012 Attorney Registration Forms, the Petition, the Oath and the Civil Cover sheet. The signature in the 2004 Registration Form is different from the other signatures. I have shown Victim the signature in the 2004 Registration Form, and he has identified it as his signature.

22. An initial conference was held on July 15, 2014, before the Honorable Joan M. Azrack, United States Magistrate Judge, EDNY, in connection with the civil action that was initiated via the Complaint.

23. On July 15, 2014, at approximately 3:23 p.m., I observed the defendant enter Courtroom 6E of the United States Courthouse for the EDNY in Brooklyn. A photograph attached herein as Exhibit A was taken of the defendant soon before he entered Courtroom 6E on that date.

24. I have reviewed a videotape and audiotape of the initial conference held before Judge Azrack on July 15, 2014 in connection with the lawsuit initiated via the Complaint. The defendant FNU LNU, also known as "Shlomo Dickerman," Stephen G.

Dickerman' and "Stephen Dickerman," identified himself as Victim and represented that he was the attorney for the plaintiff. I met Victim when I interviewed him, and Victim is not the same person as the defendant.

25. On July 29, 2014, two Special Agents of the FBI, acting in an undercover capacity (UC1 and UC2), entered 128 Brighton 11th Street, Brooklyn, New York 11235, through the front door, and sought to speak to a lawyer. UC1 had a recording device that recorded both audio and video. I have reviewed the recording.

26. UC1 and UC2 spoke with a receptionist, who stated that none of the lawyers associated with the law firm were available. She said, however, that there "was one more attorney downstairs; he's not our attorney."<sup>5</sup> He rents here. . . . His name is Shlomo Dickerman." She then gestured to UC1 and UC2 to go down the stairs to speak to him.

27. UC1 and UC2 walked down the stairs to the first floor. At first UC1 and UC2 turned left and saw an individual inside an office with a door. UC1 and UC2 asked the individual whether he was "Mr. Dickerman;" the individual indicated, in sum and substance, that he was not Mr. Dickerman and informed UC1 and UC2 that they were walking in the wrong direction. UC1 and UC2 then went back to the stairs, turned right, and walked past a first cubicle-style office space and to the SUBJECT PREMISES, the second cubicle-style office space. The defendant FNU LNU, , also known as "Shlomo Dickerman," "Stephen G. Dickerman" and "Stephen Dickerman," was sitting behind the desk at the SUBJECT PREMISES.

---

<sup>5</sup> Upon information and belief, based on the investigation, I believe that when the receptionist was referring to "our attorney," she was referring to attorneys associated with "Sirota & Associates, P.C."

I have spoken with UC1, who was present in courtroom 6E during the initial conference held on July 15, 2014, before Judge Azrack. UC1 recognized the individual sitting behind the desk as the defendant who had identified himself in court as Victim.

28. The defendant FNU LNU, also known as “Shlomo Dickerman,” “Stephen G. Dickerman” and “Stephen Dickerman,” confirmed that he was “Mr. Dickerman” and provided UC1 and UC2 with a business card. The defendant stated, among other things, that he would represent UC2 in a civil action for a \$10,000 retainer fee plus a fee of \$400 per hour; he subsequently indicated that he would reduce his retainer fee to \$5,000.

29. Based on my review of the recording, I observed that the defendant FNU LNU, , also known as “Shlomo Dickerman,” “Stephen G. Dickerman” and “Stephen Dickerman,” took the business card out of a small cardboard box on his desk, which appeared to contain more business cards. I have reviewed the business card the defendant gave UC1 and UC2, which lists the name as “Shlomo G. Dickerman, JD, LL.M., Esq.,” “Attorney at Law,” and shows “128 Brighton 11<sup>th</sup> Street, Suite One, Brooklyn, New York 11235” as the address. I also observed that the defendant took a legal pad from the bookshelf, placed it on his desk and took notes on it while he was talking to UC1 and UC2.

30. Also, based on my review of the recording, I observed that the SUBJECT PREMISES consisted of, among other things, a desk with a computer, two bookshelves, a black briefcase, a brown briefcase, multiple files and other papers. The bookshelf contained multiple photographs of the defendant with other individuals.

#### IV. Agent’s Experience and Items to Be Seized

31. Based on my training and experience, as more fully described above at paragraph 1, and as supplemented by my conversations with other Special Agents of the FBI who are experienced investigators of mail and wire fraud, false statements and identity theft, I know:

(i) that individuals involved in false statements and identity theft, particularly on the scale on which the defendant engaged in those crimes, frequently maintain, among other documents and materials: financial statements and bank records in the name of other persons; correspondence, notes, diaries and calendars reflecting personal identification information about other persons; identification documents, including picture IDs, counterfeit or stolen checks, and Social Security numbers in others' names; telephone and other utility bills and records in other persons' names; mail, FedEx air bills, and other courier packages addressed to other persons; fax machines used to send and receive documents used in furtherance of such schemes; and computers and computer equipment; and

(ii) that individuals involved in false statements and identity theft frequently maintain custody of documents and records of the sort described above for long periods of time in order to potentially reuse the stolen identity information to commit further fraud with those identities; and that this stolen identity information is often hidden within closed and/or locked cabinets, briefcases and other containers; and

(iii) The defendant is also being investigated for mail fraud and wire fraud, in violation of 18 U.S.C. §1341 and 1343. As described in paragraphs 28 and 29 above, the defendant FNU LNU, also known as "Shlomo Dickerman," "Stephen G. Dickerman" and "Stephen Dickerman," falsely held himself out as a lawyer to UC2 and then solicited UC2 for a

monetary retainer fee and legal fees. Upon information and belief, the defendant likely impersonated a lawyer to other client-victims, who were defrauded out of legal fees. The investigation has also revealed that in connection with his schemes, the defendant, among other things, used the mails to communicate with the Attorney Registration Unit and electronically filed court documents with the EDNY. I also know that individuals involved in mail and wire fraud, particularly the type which involves the preparation and filing of documents, including court documents, in other persons' names, typically keep books and records of these activities, including electronic versions of these items. These books and records include but are not limited to: copies of court documents and filings (and notes made in preparation of such documents and filings), "attorney" files and notes, "attorney" registration forms, applications for admission, including to federal and state court, notices of appearance, related correspondence, copies of Certificates of Good Standing, identification documents, electronic filing records, address lists, Rolodex or other similar contact information, bank account records and cancelled checks.

32. I have been informed by an Assistant U.S. Attorney that, under the relevant case law, in the event of a search of business premises that are "permeated with fraud," a broad search warrant that authorizes the search and seizure of voluminous business records does not run afoul of the Fourth Amendment. National City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) (citing United States v. Brien, 617 F.2d 299, 309 (1st Cir. 1980)); see also United States v. Johnson, 108 F.3d 1370, 1997 WL 136332, at \*3 (2d Cir. Mar. 21, 1997) (unpublished summary order) (affirming broad search where affidavit "show[ed] ample ground for finding pervasive fraud"). In this case, given that the defendant FNU LNU,

also known as “Shlomo Dickerman,” “Stephen G. Dickerman” and “Stephen Dickerman,” is impersonating a lawyer and has set up an office at the SUBJECT PREMISES in order to engage in the resulting false statements, identity theft and fraud schemes, a broad seizure of data from the SUBJECT PREMISES is warranted.

V. TECHNICAL BACKGROUND

33. As described above and in Attachment B, this application seeks permission to search for records constituting evidence, fruits or instrumentalities of violations of False Statements (18 U.S.C. § 1001), Mail and Wire Fraud (18 U.S.C. §§ 1341, 1343); and aggravated identity theft (18 U.S.C. § 1028A) that might be found within 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 computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

34. I submit that if a computer<sup>6</sup> or storage medium<sup>7</sup> is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

---

<sup>6</sup> For purposes of the requested warrant, a “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

<sup>7</sup> A “storage medium” for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs and DVDs, and flash drives.

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person ‘deletes’ a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

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

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory ‘swap’ or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

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

e. Based on my review of court filings related to this investigation, I believe that computer equipment was used (1) to generate court documents, including complaints and motions, (2) to electronically file such court documents, in federal and state courts, and (3) store and print documents, all in furtherance of the false statements and aggravated identity theft scheme. As previously discussed above at paragraph 20, I have also been informed that the Complaint and Civil Cover Sheet were electronically filed. There is reason to believe that there is a computer system currently located on the SUBJECT PREMISES.

35. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic “attribution” evidence that establishes how the 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 computer or 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, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

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 the 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. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular

item 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.

36. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to "image" the data stored on such devices. 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 time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. 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 electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the SUBJECT PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items 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.

b. 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 SUBJECT 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.

c. The 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.

37. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would authorize seizing, imaging, or otherwise copying computers and 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.

V. SEALING

38. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application,

including the Affidavit, Arrest Warrant and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents could result in the flight of targets and subjects of this investigation, and the destruction of evidence and tampering with witnesses.

VI. Conclusion

39. WHEREFORE, your deponent respectfully requests that a warrant be issued for the arrest of the defendant FNU LNU, also known as “Shlomo Dickerman,” “Stephen G. Dickerman” and “Stephen Dickerman,” so that he may be dealt with according to law.

40. Your deponent further respectfully requests that a warrant be issued to search SUBJECT PREMISES, further described in Attachment A, and seize the things described in Attachment B.

S/ Hannah M Buch

—  
Hannah M. Buch  
Special Agent, Federal Bureau of Investigation

Sworn to before me this  
\_5th\_ day of August, 2014

S/ Ramon Reyes, Jr.

---

THE HONORABLE RAMON E. REYES, JR.  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

Attachment A  
Property to Be Searched

The property to be searched is the Office of “Shlomo G. Dickerman,” which consists of a cubicle-style office space on the first floor of a two-story building located at 128 Brighton 11th St., Brooklyn, New York 11235. On the outside of the building is a large sign stating “LAW OFFICE” and the number “128.” A photograph of the outside of the building in which the SUBJECT PREMISES is located is attached hereto as Exhibit B, and a photograph of the SUBJECT PREMISES is attached hereto as Exhibits C1 and C2. The SUBJECT PREMISES is on the first floor and is accessible by entering the front door of the building at the top of the stairs outside the building, walking past a receptionist’s desk, entering a small hallway on the right and then walking down a flight of stairs; once at the bottom of the stairs, taking a right and walking past the first cubicle-style office space to a second cubicle-style office space, which is against the left, back wall. The SUBJECT PREMISES contains, among other things, a desk with a computer, two bookshelves, a black briefcase, a brown briefcase, multiple files and other papers.

Attachment B

Evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 1001, 1341, 1343 and 1028A, including the following:

1. Any document or item with the name Stephen G. Dickerman, Shlomo Dickerman, or variants thereof;
2. Calendars, address books, Rolodex, appointment books, records, ledgers, papers, correspondence and other documents reflecting information such as names, telephone numbers and personal identification information;
3. Any form of identification to include photo ID, business cards, social security cards, and credit cards;
4. Court documents or filings, in electronic or paper form, including: copies of court documents and filings (and notes made in preparation of such documents and filings), attorney files and notes, attorney registration forms, applications for admission, including to federal and state court, notices of appearance, related correspondence, copies of Certificates of Good Standing;
5. Tax information, in electronic or paper form, including: Federal Income Tax Returns (Forms 940, 941, 990, 1040, 1120, 1120-S), IRS Forms W-2, and IRS Forms 1099; written correspondence to and from the IRS; electronic filing records; and all books, work papers and records used to prepare tax returns, including back-up documentation, identification documents, electronic filing records, address lists, Rolodex or other similar contact information, bank account records and cancelled or uncashed checks;
6. Financial documents, in electronic or paper form, including: bank records, bank statements, deposit slips, withdrawal slips, checks deposited, cancelled checks, check stubs, all debit and credit memos, and financial statements;
7. Computers<sup>8</sup> or storage media<sup>9</sup> that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of Title 18, United States Code, Sections

---

<sup>8</sup> A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

<sup>9</sup> A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

1001, 1341, 1343 and 1028A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1001, 1341, 1343 and 1028A, involving the defendant FNU LNU, , also known as “Shlomo Dickerman,” “Stephen G. Dickerman” and “Stephen Dickerman” since 2009, including:

- a. evidence of who used, owned, or controlled the COMPUTER 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, email, email contacts, instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, 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 lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment;
- j. routers, modems, and network equipment used to connect the Computers to the Internet;
- k. Internet Protocol addresses used by the COMPUTER; and

1. records or information about the COMPUTER'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; and
8. All closed and/or locked containers, including but not limited to briefcases, file folders, file cabinets and safes, and any keys to the containers, file cabinets or safes.