IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF 2303 BANCROFT PLACE, NW, WASHINGTON, D.C. 20008	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

I, Daniel Rzepecki, being duly sworn, depose and say that:

I. AFFIANT'S BACKGROUND AND EXPERIENCE

Your Affiant, Daniel Rzepecki, a duly sworn and appointed Special Agent of the Federal Bureau of Investigation (hereinafter "FBI"), hereby makes the following statements, based upon information obtained by myself, other Special Agents of the FBI, as well as information conveyed to me by other law enforcement officials and other sources.

I have been a Special Agent of the FBI since October 2008. I am currently assigned to the Washington Field Office where I conduct white collar crime investigations, primarily in the health care fraud field. I have training and experience in the enforcement of laws of the United States, including training in the preparation, presentation, and service of criminal search warrants. I have duties that include investigations of, among other matters, mail fraud, wire fraud, health care fraud, false claims, and money laundering. Through my training at the FBI Academy and my participation in searches and arrests conducted by my squad and other squads, I have assisted and/or participated in the preparation and/or execution of search and arrest warrants. The statements contained in this affidavit are based on my personal knowledge, information obtained from other law enforcement officers, or information obtained from others. This affidavit does not set forth every fact discerned throughout the investigation; rather, it

contains a summary of the investigation to date and sets forth only those facts that I believe necessary to establish probable cause to search the premises described herein.

Based on the facts set forth in this affidavit, your affiant submits that there is probable cause to believe that a search of the residence of Dean Addem, formerly known as Tarek Abou-Khatwa, located at 2303 Bancroft Place, NW, Washington, D.C. 20008, which is described in greater detail in Attachment A to this search warrant affidavit, will uncover the evidence, fruits, and/or instrumentalities described in Attachment B, relating to violations of 18 U.S.C. 1347.

This affidavit is not intended to include each and every fact relating to this investigation. This affidavit sets forth those facts necessary to support probable cause to believe that kept and concealed within 2303 Bancroft Place, NW, Washington, D.C. 20008, are fruits, instrumentalities, and evidence of health care fraud, in violation of 18 U.S.C. § 1347.

II. RELEVANT STATUTE

Title 18, United States Code, Section 1347 (Health Care Fraud) makes it unlawful for anyone to knowingly and willfully execute or attempt to execute a scheme or artifice: (a) to defraud any health care benefit program; or (b) to obtain, by means of materially false or fraudulent pretenses, representations, or promises, any of the money or property owned by, or in the custody and control of, any health care benefit program.

III. CAREFIRST/ASSOCIATED FIELDS

In January 1998, Maryland Blue and Washington Blue announced combined operations under a new holding company, CareFirst, Inc. and began operations under their new name CareFirst BlueCross BlueShield. CareFirst, Inc. (hereinafter "CareFirst") is the not-for-profit, non-stock, parent company of CareFirst of Maryland, Inc., and Group Hospitalization and Medical Services, Inc., affiliates that do business as CareFirst BlueCross BlueShield. CareFirst

is governed by a Board of Directors and special statutes regulating its business in Maryland, the District of Columbia, and Northern Virginia. CareFirst is a private "health care benefit program" in that it provides health insurance and managed care services throughout the state of Maryland, the District of Columbia, and northern Virginia. Its main products are HMO, PPO, and traditional indemnity plans for individuals and groups, but it also offers dental and vision insurance and Medicare Part D coverage. CareFirst is the largest health care insurer in the Mid-Atlantic region, serving 3.4 million members.

An insurance Broker (also insurance agent) sells, solicits, or negotiates insurance for compensation. Insurance Brokers are regulated by the states and most states require anyone who sells, solicits, or negotiates insurance in that state to obtain an insurance Broker license, with certain limited exceptions. The District of Columbia, Maryland, and Virginia require insurance Brokers to have a license. In order to obtain a Broker's license, a person typically must take pre-licensing courses and pass an examination. An insurance Broker also must submit an application (with an application fee) to the state insurance regulator in the state in which the applicant wishes to do business, who will determine whether the insurance Broker has met all the state requirements and will typically do a background check to determine whether the applicant is considered trustworthy and competent. A criminal conviction, for example, may result in a state determining that the applicant is untrustworthy or incompetent. A felony conviction will terminate a license; however, a misdemeanor will not necessarily terminate a license.

Brokers play a significant role in helping small employers find health insurance, particularly in more competitive markets. Average small group commissions range from two percent to eight percent of premiums.

Group health insurance coverage is a policy that is purchased by an employer and is offered to eligible employees of the company (and often to the employees' family members) as a benefit of working for that company. A group health insurance plan is a key component of many employee benefits packages that employers provide for employees. The majority of Americans have group health insurance coverage through their employer or the employer of a family member. One of the advantages for employees in a group health plan is the contribution most employers make toward the cost of the health coverage premium. In many cases employers pay one-half or more of the monthly premium for an employee.

IV. COMPANY BACKGROUND AND SYNOPSIS OF THE SCHEME

BCA is a Small Business Administration 8(a) government contractor, owned by Tarek Abou-Khatwa[1] (hereinafter, "Abou-Khatwa"). The 8(a) Business Development Program assists in the development of small businesses owned and operated by individuals who are socially and economically disadvantaged, such as women and minorities. BCA has one current office location in Washington, D.C., located at 1025 Connecticut Ave, NW, Suite 611, Washington, D.C. 20036. Abou-Khatwa maintains a personal residence at 2303 Bancroft Place, NW, Washington, D.C. 20008, from which he also conducts BCA business, as detailed below.

After failing to earn a government contract with the U.S. Securities and Exchange Commission at the end of 2009, Abou-Khatwa decided to redirect BCA's focus on health insurance for businesses. Abou-Khatwa had entered into a Broker/Agent Agreement with CareFirst, Inc. in June 2006. The CareFirst Broker/Agent Agreement lists the following states licenses for Abou-Khatwa: Virginia, expired on 06/30/2012; District of Columbia, expires on 02/28/2015; and Maryland, expires on 02/28/2014. All three states utilize the National Producer Number (hereinafter "NPN"). Abou-Khatwa's NPN number is: 3039641.

[1] In late 2012, Abou-Khatwa legally changed his name to Dean Addem.

As a Broker for CareFirst, BCA solicited potential clients, mainly non-profit organizations, located in Washington, D.C. Early in 2010, BCA paid for a subscription to a web-based service that provided a list of nonprofit organizations that BCA would cold-call. The calls were designed to arrange meetings to propose financially beneficial health insurance rates for the nonprofit organizations. If the prospective client was interested in pursuing business with BCA, the nonprofit organization completed a standard CareFirst application which BCA submitted to CareFirst in order to receive the formal health insurance rates.

Abou-Khatwa is the only licensed Broker at BCA and is responsible for acquiring the formal health insurance rates from CareFirst. Abou-Khatwa or a designated BCA employee provided the health insurance rates to the prospective client for their final decision. If the prospective client decided to accept the rates and work with BCA, the client completed the enrollment process and eventually received their CareFirst health insurance cards. BCA was paid a 5% commission from CareFirst based on the total premium amount. The Patient Protection & Affordable Care Act dropped BCA's commission to 3.5%.

CareFirst terminated its Broker/Agent Agreement with BCA as of May 1, 2011. Among the reasons for terminating BCA's agreement, CareFirst discovered that: (1) BCA altered client identifiers – such as dates of birth – for client employees; (2) BCA combined small client employer groups with other larger client employer groups, in order to fraudulently reduce the rate of insurance for the client employer group; and (3) BCA moved client employees from one client employer group to another client employer group in an effort to influence the overall age of a given client employer group. All other variables being equal, premium rates are generally lower if the average age of the employer group is younger. Based on my review of the records in

this investigation, it is believed that BCA attempted to fraudulently reduce the average age of certain client employer groups in order to lower their premiums and maintain their business.

BCA continued to work with CareFirst as an independent contractor, but lost many of the privileges BCA had under the Broker/Agent Agreement.

Based on documentation provided by CareFirst, from January 2008 through July 2012 BCA managed 19 CareFirst client accounts, generating $3,803,615.59 in premiums that BCA paid to CareFirst.

Evidence obtained as part of this investigation to date reveals that BCA submitted fraudulent invoices to its clients that contained an approximate 20% increase, or more, of the actual health insurance rates provided by CareFirst. There are no fees associated with Brokers. The Broker/Agent Agreement states in Section VI, Paragraph G: "The only payment due under this Agreement from Insurer (CareFirst) to Contractor (BCA) shall be for Broker/Agent Fees and applicable bonuses and not for any other expenses or costs incurred by Contractor." Therefore, this increase was not a legitimate fee or payment.

V. EVIDENCE SUPPORTING PROBABLE CAUSE

In October 2012, the District of Columbia Department of Insurance, Securities & Banking, Enforcement & Consumer Protection Bureau provided the FBI with a referral concerning Abou-Khatwa and BCA and their business practices with CareFirst.

Through the course of the investigation it was found that Abou-Khatwa directed clients to not communicate with CareFirst and only deal directly with BCA. Abou-Khatwa further shielded CareFirst/client communication by making himself the point of contact with CareFirst for all of his clients. The Broker/Agent Agreement states in Section VI, Paragraph E: "Insurer (CareFirst) shall retain an absolute right to contact the Group and/or Subscriber directly for any

purpose at Insurer's discretion. Every effort will be made to keep Contractor (BCA) informed of any such contacts." BCA arranged all CareFirst client invoices to be mailed to BCA, when those invoices should have been mailed directly to the client employer group. In turn, BCA letterhead invoices were mailed to the client employer groups.

In many instances, the invoices that BCA sent to the client employer group contained invoice charges over and above that which CareFirst charged. The fraudulent increases passed on by BCA to the client employer group were as high as 20% of the original CareFirst invoice charge.

During the course of the investigation, it was discovered that CareFirst does not allow payment to be submitted to CareFirst through the Broker/Agent; instead, CareFirst requires that payment be made from the client employer group directly to CareFirst. Although BCA submitted several payments in such a manner, CareFirst did not discover BCA's impermissible billing practice. If CareFirst had noticed BCA's billing methods, CareFirst would have taken immediate corrective measures.

As part of the investigation, I reviewed CareFirst invoices sent to BCA on behalf of BCA clients. I have also reviewed client employer group documents, including invoices sent to the client employer groups by BCA. In addition, I interviewed representatives from several BCA clients. I discovered similar issues across clients, including (1) fraudulently inflated invoices sent by BCA to the client; (2) altered identification information (for example, incorrect dates of birth) of individual client employees; and (3) receipt of health care information by the client for employees who did not work for the client.

From my review of documents and interviews conducted among these client employer groups, I have selected two examples of client employer groups who were defrauded by BCA.

In each case, BCA fraudulently overcharged the client employer group for health insurance from CareFirst.

BCA Client Number One

In April 2011, a BCA employee made a cold-call to BCA Client Number One ("Client #1) during a time period when Client #1 was considering options for more affordable health insurance rates. Client #1 met with BCA representatives to review and discuss if BCA could offer lower health insurance rates. After the initial meeting, Client #1 received a formal health insurance rate quote, which was lower than Client #1's rate at the time. The lower rate offered by BCA which persuaded Client #1 to procure group health insurance through BCA.

Client #1 received monthly invoices for CareFirst group health insurance from BCA on BCA letterhead. For the first year Client #1 experienced no problems with its health insurance. Client #1's first year (July 2011 – June 2012) monthly premiums were $4,877.00. In the spring of 2012, BCA sought renewal of Client #1's health insurance business and presented revised rates for the 2012-2013 contract year. The revised rates contained an "expected" 7% increase in Client #1's group rates. On July 12, 2012, Client #1 received an email from a BCA representative indicating that Client #1's new point of contact with BCA was Abou-Khatwa.

On July 30, 2012, Client #1 received a health insurance card for an individual that did not work for their organization. Client #1 contacted Abou-Khatwa, who advised Client #1 that he would take care of the situation. On August 9, 2012, representatives from Client #1 met with Abou-Khatwa. One representative from Client #1 recalled Abou-Khatwa overemphasizing that Client #1 should not contact CareFirst directly. Abou-Khatwa explained that CareFirst was a large company, and that CareFirst would not be able to assist Client #1 when Client #1 needed

help. Abou-Khatwa stated to this representative that BCA was the point of contact for all of Client#1's health insurance questions.

On August 10, 2012, Client #1 received a letter from CareFirst which provided invoices for June, July, and August 2012. The invoices included names of five unknown individuals, all of whom were not employed by Client #1. The charges in the CareFirst invoices were as much as $1,700 less for each month than the invoices that BCA had presented to Client #1. Client #1 called CareFirst and explained the discrepancy. Subsequently, Client #1 dealt directly with CareFirst on billing issues.

Client #1 paid its last monthly premium to BCA for October 2012, but has not paid any money to BCA since that time. Nevertheless, BCA kept sending invoices to Client #1.

The chart below illustrates a sampling of the fraudulent invoice practices that BCA engaged in with regard to Client #1. The chart compares BCA invoices versus CareFirst invoices for Client #1 that were provided for the same time period for the same services, in three selected months. I have calculated Client #1's financial loss as a result of BCA's fraudulent invoices in the fourth column.

MONTH	**BCA INVOICE TOTAL**	**CAREFIRST INVOICE**	**CLIENT #1'S FINANCIAL LOSS**
July 2011	$4,877.00	$3,462.00	$1,415.00
January 2012	$4,877.00	$3,737.00	$1,140.00
September 2012	$5,221.00	$4,328.00	$893.00

BCA Client Number Two

In June 2011, BCA Client Number Two ("Client #2") began searching for more affordable health insurance rates for its employer-based group health insurance. Around that same time, a representative from Client #2 was referred by a friend to a BCA employee for the purpose of potentially soliciting group health insurance services. After a meeting between the BCA employee and the representative from Client #2, Client #2 hired BCA as Client #2's Broker for health insurance with CareFirst.

Client #2 did not experience any problems with BCA in the first year. In May or June of 2012, BCA sought to renew Client #2's health insurance contract, and advised Client #2 of an expected increase in health insurance rates within a normal range. Client #2 renewed its contract with BCA and CareFirst for an additional 12-month period.

On or about August 8, 2012, Client #2 received a letter from CareFirst asking Client #2 to verify Client #2's employees and any irregularities found on CareFirst invoices. On the invoices provided from CareFirst, Client #2 identified eight different individuals who were unknown to Client #2 and who were not employed by Client #2.

Client #2 also noticed differing premium charges on the CareFirst invoices versus the BCA invoices. Client #2 compared the invoices sent by BCA to the invoices sent by CareFirst, covering the same services for the same time period. Client #2 identified overcharges by as much as 24% in the BCA invoices compared to the CareFirst invoices. Client #2 calculated that the difference between the invoices generated by BCA versus those generated by CareFirst over a 14-month period represented a total loss of $10,976.00.

In the chart below, I selected invoices from three out of the 14 months in which Client #2 was overcharged to illustrate the fraudulent billing practices that BCA engaged in with regard to Client #2.

MONTH	BCA INVOICE TOTAL	CAREFIRST INVOICE	CLIENT #2'S FINANCIAL LOSS
September 2011	$3,512.00	$2,604.00	$908.00
December 2011	$3,126.00	$2,604.00	$522.00
August 2012	$4,650.00	$4,138.00	$512.00

Other BCA Clients

Based on documentation provided by CareFirst, BCA managed 19 CareFirst client accounts from January 2008 through July 2012.[2] Over that same time period, BCA generated a total of $3,803,615.59 in health insurance premiums that BCA paid to CareFirst.

Among other individuals, I interviewed an accountant, Contractor #1, who works for the firm that provides accounting services for BCA on a contract basis. During the interview, Contractor #1 was confronted with an email sent to Contractor #1 from a BCA client accusing BCA of stealing money from the client. Contractor #1 indicated that Contractor #1 simply forwarded that email to Abou-Khatwa for handling, but that Contractor #1 had no knowledge of any fraudulent activity involving BCA.

Contractor #1 indicated that as of July 2013, BCA maintained a client list of approximately 20 client employer groups with whom BCA (or some derivation thereof) acted as

[2] Although CareFirst terminated Abou-Khatwa as a Broker in May 2011, some of the insurance contracts that About-Khatwa procured for BCA prior to termination remained active through July 2012.

a Broker and has secured employer-based health insurance through CareFirst. These 20 client employer groups are in addition to the 19 client employer groups reported by CareFirst, indicated above. I had not been made aware of these additional 20 clients previously in my investigation. To my knowledge, CareFirst is not aware that BCA and/or Abou-Khatwa represent these 20 clients as a Broker for employer-based health insurance through CareFirst. It is suspected that BCA (or some derivation thereof) and/or Abou-Khatwa has defrauded CareFirst in that BCA and/or Abou-Khatwa continues to act as an insurance Broker for employer-based health care services through CareFirst despite CareFirst having terminated Abou-Khatwa as a Broker in May 2011.

Based on my interview with Contractor #1 and my initial review of documents, BCA appears to follow the same pattern with these 20 additional client employer groups as with the 19 initial client employer groups; that is, BCA manipulated client rosters in order to obtain fraudulently reduced premiums from CareFirst, and provided fraudulent invoices to these clients containing unauthorized overcharges for insurance services.

BCA Employees

I conducted an interview with a BCA employee ("Employee #1) on February 26, 2012. Employee #1 advised that over the course of its employment, Employee #1 became aware of fraudulent schemes taking place at BCA with CareFirst. On July 11, 2012, Employee #1 confronted Abou-Khatwa with concerns about the information Employee #1 discovered. After a discussion concerning the information, Abou-Khatwa disagreed with Employee #1's concerns. Employee #1 was fired from BCA shortly after that conversation. Employee #1 learned that, within the remainder of that same week, two other BCA employees, BCA Employee #2 and BCA Employee #3, were also fired.

Summary of Findings

Based on my review of BCA and CareFirst invoices for the two Clients discussed above, BCA fraudulently overcharged its clients by an approximate average of 20% in health insurance premiums that was beyond the specific rate set forth by CareFirst. This review does not account for all of BCA clients, some of whom have not yet been interviewed and documents from whom have not been received.

BCA Business Activities Related to Abou-Khatwa's Residence

In interviews with four different witnesses, each of the witnesses indicated that Abou-Khatwa regularly conducted BCA-related work from his residence located at 2303 Bancroft Place, NW, Washington, D.C. 20008, and which is described in greater detail in Attachment A to this search warrant affidavit.

In a March 12, 2013 interview, Witness #1 stated that Abou-Khatwa worked from his residence on a regular basis and often conducted business via his cell phone and lap top computers. Furthermore, Witness #1 observed Abou-Khatwa transporting BCA-related documents and files from the BCA office space, with the stated intention of returning to Abou-Khatwa's residence to complete work.

In a March 26, 2013 interview, Witness #2 states that Abou-Khatwa often worked from his residence and communicated to the BCA employees via emails or phone calls while Abou-Khatwa was at his residence.

In a March 28, 2013 interview, Witness #3 states that Abou-Khatwa frequently worked from home on a laptop computer. Witness #3 often received emails from Abou-Khatwa when Abou-Khatwa was out of the office, and reportedly working from Abou-Khatwa's residence.

In a July 10, 2013 interview, Witness #4 stated that on one occasion it observed Abou-Khatwa collecting BCA-related documents in order to remove the documents from the BCA offices to store the documents off-site. Abou-Khatwa stated to Witness #4 that he was moving the BCA documents to his residence for storage.

Through the course of the investigation it was discovered that Abou-Khatwa hired an Information Technology company to regularly back up and save data from his lap top computer to a BCA server. This is the same lap top that Abou-Khatwa used to work from home.

The employees interviewed did not know Abou-Khatwa's residence address. Based on my investigation, Abou-Khatwa lives at 2303 Bancroft Place, NW, Washington, D.C. 20008 as his primary residence. To my knowledge, Abou-Khatwa does not have any other residences.

Based on my interviews with the four witnesses captioned above, Abou-Khatwa consistently conducts business on behalf of BCA from his residence using his lap top computer and cell phone; Abou-Khatwa also stores BCA-related work records at his residence at 2303 Bancroft Place, NW, Washington, D.C. 20008.

VI. RECORDS RETENTION

Based on my knowledge, training and experience, Brokers such as BCA maintain books and records at the address registered with CareFirst. Based on my investigation, Abou-Khatwa also maintains books and records at his residence at 2303 Bancroft Place, NW, Washington, D.C. 20008.

Your affiant has reviewed the regulations governing the CareFirst Broker's record retention, which states, for a minimum of three years "no person shall fail to maintain its books, records, documents, and other business records in such order that data regarding complaints, claims, rating, underwriting, and marketing are not accessible and retrievable for examination by

the Commissioner. Data for at least the current calendar year and the 2 preceding years shall be maintained."

Based on my knowledge, training, and experience, I know that business owners keep records pertaining to their business for months if not years.

VII. ELECTRONIC EVIDENCE

Your affiant knows that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation: (a) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (b) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are instrumentalities, fruits, or evidence of crime, or storage devices for information about crime.

Based upon the facts set forth above, there is probable cause to believe that computer hardware, software, related documentation, passwords, data security devices (as described below), and data that may be found at the business of BCA were integral tools of these crimes and constitute the means of committing it. As such, they are instrumentalities and evidence of the violation designated. Rule 41 of the federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them. It is the intent of the Agents to copy the electronic evidence at the search site (by creating a "mirrored" image of the data). If this copying cannot be accomplished, then the procedures outlined in paragraphs below will be followed:

Hardware: Computer hardware 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. Hardware includes, but is limited to, any data processing devices (such as central processing units); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, and other memory storage devices); 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 (such as physical keys and locks).

Software: Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored electronic, magnetic, or other digital form, including zip drives. It commonly includes programs to run operating systems, applications (like tax preparations, word-processing, or spreadsheet programs), and utilities.

Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, and other programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include programming code that creates test keys or hot keys, which perform certain preset 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 process to restore it.

Based upon my knowledge, training and experience, and consultation with computer specialists from the FBI, your affiant knows that searching and seizing information from computers almost always require agents to seize most or all electronic storage devices (along

with related peripherals, as discussed below) to be searched later by a qualified computer expert in a laboratory to other controlled environment. This is true because of the following:

Volume of Evidence: Computer storage devices (like hard disks, and diskettes) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files is evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

Technical Requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. However, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby-trap"), a controlled environment is essential to its complete and accurate analysis.

Based upon my knowledge, training and experience and consultation with forensic computer examiners, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires Agents to seize most or all of the computer system's input/output peripheral devices, related software, documentation, and data security

devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

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. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications 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.

If, after inspecting the I/O devices, software, documentation, and data security devices, the analyst determines that these items are no longer necessary to retrieve and preserve the data evidence, the government will return them within a reasonable time period.

Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to, the following: examining file directories and subdirectories for the lists of files they contain, opening or reading the first few pages of selected files to determine their contents; scanning for deleted or hidden data; searching for key words or phrases ("string searches").

This specifically excludes a search of any kind of unopened electronic mail, or no warrant is herein sought for such unopened electronic mail. If unopened electronic mail is to be searched, a separate warrant will be sought supported by probable cause.

VIII. REQUEST FOR SEALING

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 application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation.

Based upon my training and experience, I have learned that, criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

IX. CONCLUSION

Based on the foregoing information and upon my training, and experience in the investigation of health care fraud, I believe there is probable cause to believe that fruits, instrumentalities and evidence of violations of Title 18 United States Code 1347 (Health Care Fraud), as described in the Attachment B, are kept and concealed within the premises listed in Attachment A (2303 Bancroft Place, NW, Washington, D.C. 20008).

_____
Daniel Rzepecki, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this _____ day of August 2013.

_____
UNITED STATES MAGISTRATE JUDGE