

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

CR24-7

IN THE MATTER OF THE SEARCH)
WARRANT OF 4224 BALDWIN AVENUE,)
LINCOLN, LANCASTER COUNTY, NEBRASKA)

SEARCH WARRANT: RETURN

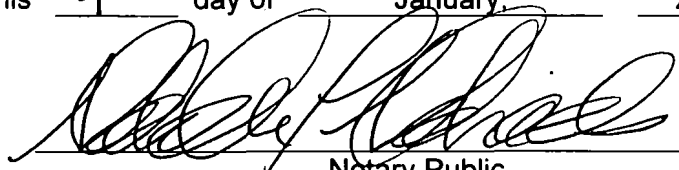
STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)

The undersigned states that he received the search warrant issued herein on the 2 day of January, 2024, and that he executed the same on the 2 day of January, 2024, by seizing the property described in the inventory filed herein and by delivering a copy of the search warrant for said property at the place from which the property was taken.

DATED this 4 day of January, 2024.


Investigator Charles P. Starr

SUBSCRIBED AND SWORN to before me this 4th day of January, 2024.


Notary Public

LANCASTER COUNTY
2024 JAN -4 PM 3:03
CLERK OF THE
DISTRICT COURT

General Notary - State of Nebraska
MICHELLE L. MICHAELS
My Comm. Exp. Oct. 27, 2027.



002107233D02



RECEIPT

The undersigned hereby acknowledges receipt of the following items which were seized from 4224 Baldwin Avenue, Lincoln, Lancaster County, Nebraska, in accordance with the Search Warrant issued by the County Court of Lancaster County, Nebraska.

- RED Samsung cell phone with red case
- Mailing Allstate to Jeffrey Smith, 4224 Baldwin Ave NE
- DELL LAPTOP # 8WZ53J3
- WELLS FARGO ENVELOPE WITH NOTES & BITCOIN TRANSACTIONS
- JEFFERSON CAPITAL PAYMENT DOC
- CAPITAL ONE ACCT INFO
- CHASE ACCT INFO
- RED SPERAL NOTEBOOK, BLUE SPERAL NOTEBOOK
- (2) green debit cards
- Jeffrey Smith Allaccess CARD 4151580664583924
- " NET SPEND CARD 5226288289090868
- IDES CARD 'GARAWAY' 5115653938524805
- " 'JONES' 5115653938574297
- " 'SKAUG' 5115653938374904
- " 'VAN FOSSAM' 5115653938139361
- " 'Greenfield' 5115653938103923
- SAMSUNG Phone in black case
- SAMSUNG Phone Charger
- DELL LAPTOP # 42D NQ12 w/CORD
- DELL LAPTOP # 19KCI1F3
- 'TARGUS' DOCKING STATION
- DELL MOUSE & KEYBOARD
- NOTES, NAMES, PASSWORDS,

LANCASTER COUNTY
2024 JAN -4 PMD: 03
CLERK OF THE
DISTRICT COURT

2

day of

January,

2024.

Investigator Charles P. Starr

SUBSCRIBED AND SWORN to before me this

day of

January,

2024.

Notary Public

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA

)

COUNTY OF LANCASTER

)

)

ss. SEARCH WARRANT

TO: Investigator Charles Starr, a law enforcement officer with the Nebraska Department of Insurance, Insurance Fraud Prevention Division, State of Nebraska, and any and all law enforcement officers, and agents thereof.

WHEREAS, Charles Starr has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, and said written Affidavit, having been duly considered, the court finds that the facts set forth in said Affidavit are true, and that those facts do constitute grounds and probable cause for the issuance of a Search Warrant.

THEREFORE, you are commanded to search and seize the items as described in **Attachment A**, hereby attached, and incorporated by reference, to include any specific authorization as contained in **Attachment A**.

THEREFORE, you are commanded to execute and return this Search Warrant in the manner as prescribed in **Attachment A**.

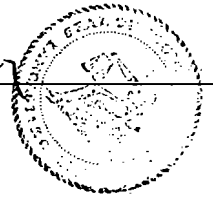
Given under my hand and seal this 2nd day of January, 2024.

Garr J. Yauer

Judge of the County Court

Lawrie J. Yardley

Printed Name of Judge



LANCASTER COUNTY
2024 JAN -4 PH 3: 03
CLERK OF THE
DISTRICT COURT

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
)
COUNTY OF LANCASTER) ss. AFFIDAVIT FOR SEARCH WARRANT

Charles Starr, being first duly sworn upon oath deposes and stated that he is a Criminal Investigator for the Nebraska Department of Insurance, Insurance Fraud Prevention Division, Lincoln, Lancaster County, Nebraska. AFFIANT stated he is currently involved in the investigation of an insurance fraud, Neb.Rev.Stat. §28-631, occurring over an extended period in 2023, Lincoln, Lancaster County, Nebraska. AFFIANT has reviewed reports regarding this investigation prepared by investigators employed with Allstate Insurance Company.

Attachments

- Attachment A: Location and Digital Device(s) to be Searched
- Attachment B: Technical Information Regarding the Search of Digital Devices

The above are hereby attached and incorporated by reference.

Affiant's Background

Your affiant has been a Nebraska Law Enforcement Officer since 1973 with nearly 26 years with the Insurance Fraud Prevention Division. Since 1973 Affiant has been investigating misdemeanor and felony crimes with the Lincoln Police Department and the Insurance Fraud Prevention Division to include homicide, burglary, robbery, assault, weapon offences, narcotics, and fraudulent activity. Your Affiant has training and experience in conducting criminal investigations.

This Affidavit is submitted in support of a search warrant. Your Affiant may not have set forth every fact known to your Affiant regarding this investigation. The information contained in this Affidavit is from your Affiant's criminal investigation and may include information provided by other law enforcement, or others.

Case Facts

On November 13, 2023, the Insurance Fraud Prevention Division received a "Suspected Fraudulent Claim Referral" from Kailah Combs, Investigator with American Heritage Life Insurance Company, DBS Allstate. Combs indicates that Jeffrey Smith, 4224 Baldwin Avenue, in Lincoln, Nebraska, was a claims examiner with American Heritage. As a claims examiner, Mr. Smith had the ability to work from home. Mr. Smith reviewed insurance claims on policies issued by American Heritage Life. Mr. Smith would review the claim, review policy benefits, collect documents pertaining to the claim, and make payments if appropriate. Mr. Smith had a threshold of \$20,000 on any one claim. Payments were made through electronic transfers or entries were made which would cause the creation of physical checks payable to the policyholder.

Mr. Smith had his own American Heritage Life accident policy, number 55CA584994. It was discovered in 2023 a claim handled by Mr. Smith exceeded the threshold of \$20,000 which triggered an audit of his policy. It was found that as of November 3, 2023, claims totaling \$935,830 had been submitted on the policy with \$885,230 having been paid out electronically to accounts controlled by Mr. Smith. Upon review of those claims, it was found there were no supporting documents for the alleged medical services in which benefits were allowed. Mr. Smith was the claims handler associated with all of the unsupported claims made on his policy.

LANCASTER COUNTY
2024 JAN -4 PM 3:04
CLERK OF THE
DISTRICT COURT

According to Investigator Combs, Smith was interviewed in a telephone call after the discovery by Izabela Zeglen with Allstate regarding the claims. Mr. Smith admitted in the interview the claims were bogus. Mr. Smith indicated to Zeglen he was being "blackmailed."

On December 26, 2023, Investigator Starr and Division Chief Kimberly Church contacted Jeffrey Smith at his residence, 4224 Baldwin Avenue in Lincoln, Lancaster County, Nebraska. Investigator Starr questioned Mr. Smith regarding the allegation asking him to explain what had transpired. Mr. Smith stated, "it's really complicated." Upon questioning he stated he had a male friend, Robby, who was kidnapped in Brazil and was being held for ransom sometime in July 2023. He needed \$750,000 to secure his release according to a call he received from "Pablo." Mr. Smith stated he did not contact any law enforcement entities as "Pablo" advised "Robby" would be killed if he did. Mr. Smith stated he did not have that kind of money so he looked to see if he could make a false claim on his policy which he found, that in fact, he could. Smith stated he believes he made nearly 50 false claims totaling nearly \$800,000.

Smith stated he lives with his daughter, Desirae Valentine, and her boyfriend Ethan. The property is titled to a Desirae Valentine. Smith stated he has worked from his home since 2019 when COVID hit. He has a computer, a docking station, and equipment issued by Allstate to handle claims. He denied having a personal computer.

Smith stated he has maintained three separate accounts with financial institutions: Wells Fargo, JP Morgan Chase, and Chime. He had the electronic deposits pertaining to the claims going into his Wells Fargo account. Smith stated he would then make electronic transactions to "Pablo" as directed. Nearly all his banking and communication were done through his personal cellphone, which he would refer to on several occasions during the interview process. Smith stated he has a Samsung S10 Android cellphone through T-Mobile, number 402.570.3087. Smith stated he made cash withdraws from his bank and sent monies through crypto devices at a liquor store on North 48th or vape shop located on 33rd and Pioneer, sending the money to "Pablo." Smith communicated with his cellphone with several individuals during this time period, including a female who identified herself as Kathy, "Robby's" personal assistant.

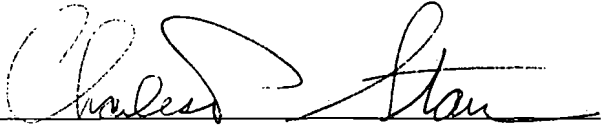
Smith showed Investigator Starr a series of "texts" from his cellphone, one of which was alleged to be a flight schedule for Roberto Diaz Sanchez (Robby). Smith stated he was supposed to arrive in Lincoln; however, he had to go to Brazil to handle his father's affairs at the last minute when he was kidnapped. It was pointed out to Mr. Smith, that this was after the alleged bogus claims started and the amount demanded by the kidnapers exceeded the ransom demand. Mr. Smith appeared to hesitate and again started reviewing texts on his cellphone stating he did "invest" about half, \$500,000, with another friend whom he has never met located in Seattle, Washington. He met this friend, Thomas Wagner, on a dating site and was investing in a business venture hoping to make a profit.

Mr. Smith forwarded several texts to Investigator Starr showing financial transfers to several persons not referenced in the interview. In addition, he forwarded a photograph of an individual whom he advised was "Robby" that was sent to him by "Robby" while recovering from his kidnapping.

The above does constitute grounds of probable cause for the issuance of a search warrant to search and seize the evidence specifically identified in **Attachment A**, to include any specific authorization requested authorization to be ordered by the court.

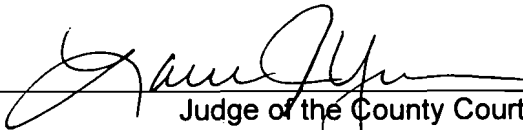
Further AFFIANT saith not:

DATED this 2nd day of January January, 2024.



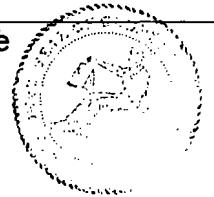
Charles P. Starr, AFFIANT

SUBSCRIBED AND SWORN to before me this 2nd day of Jan January, 2024.



Judge of the County Court
Laurie J Tardif

Printed Name of Judge



ATTACHMENT A: Location and Digital Device(s) to Be Searched

Law enforcement and those assisting law enforcement is directed to seize and search the following:

- 4224 Baldwin Avenue, Lincoln, Lancaster County, Nebraska

for the following evidence:

- Samsung cellphones
- Any/all cellular phones in the possession of Jeffrey Smith
- Computers to include laptops and personal computers.
- Any electronic memory storage device to included CD's, thumb drives, flash cards, external hard drives.
- Evidence of the use of digital currency
- Any cellphone associated with telephone number 402.570.3087
- Cash
- Any and all information related to claims, financial information, communication with or by Jeffrey Smith as it pertains to contacts or money transfers.

And, furthermore, to search any seized electronic evidence as necessary and authorized to accomplish the purposes of this warrant to include any live and/or deleted data for the timeframe of January 1, 2023 to January 1, 2024, specifically for the seizure of the following items:

1. Device identifiers, information, and configurations.
2. User account information and any associated accounts on the device.
3. Call logs.
4. Contact lists.
5. Short Message Service (SMS), Multimedia Messaging Service (MMS) messages and instant messages.
6. Chat messages from installed applications.
7. Email messages.
8. Installed applications and their corresponding accounts and data.
9. Applications containing digital currency wallets and related information.
10. Images and associated metadata.
11. Photographs and/or videos, and associated metadata.
12. Audio files, including voicemails, and associated metadata.
13. Document files and associated metadata.
14. Internet browsing history, including bookmarks, searches, browser cookies and other associated cache files.
15. Memos and notes (typed and voice).
16. Calendar information.
17. Passwords, keychains.
18. Databases and file systems.
19. Device activity logs and application usage logs.

To obtain and search the data from the aforementioned digital device, law enforcement and/or those assisting may:

1. Obtain data from the physical memory of the digital device itself as well as from any data storage devices housed within the digital device, specifically Secure Digital (SD) and Subscriber Identification Module (SIM) cards.

2. Obtain data from the aforementioned digital device's active file system, as well as unallocated space as to recover deleted data and file fragments.
3. Obtain data by making unobtrusive revocable setting changes to permit the digital extraction of the data unless the digital device requires disassembly to obtain the desired data which may render the device inoperable.
4. Copy, forensically image, view, photograph, record, and/or conduct forensic analysis of the data obtained.
5. Enlist the aid of non-law enforcement, who are trained in conducting forensic analysis of the data in retrieving and analyzing the data. When files have been deleted, they can be potentially recovered later using forensic tools. A person with familiarity with how digital devices work may, after examining the data, be able to draw conclusions about how the device was used, the purpose of its use, who used it, where, and when; and/or
6. Be required to examine every file and scan its contents briefly to determine whether it falls within the scope of the warrant. This is necessary as it is difficult to know prior to the search the level of technical ability of the device's user and data can be hidden, moved, encoded, or mislabeled to evade detection.
7. Remove the digital device to another location to conduct the digital forensic examination and/or analysis.

The search of digital devices is a lengthy process requiring special steps to ensure the integrity of the digital devices. In the event the search and/or seizure of evidence is not completed within ten (10) days, law enforcement is authorized to return the search warrant within ten (10) days upon completion of the search and seizure.

ATTACHMENT B: Technical Information Regarding the Search of Digital Devices

Through your Affiant's training and past experience, and from information provided by Electronic Evidence Unit forensic examiners, your Affiant is aware that:

Digital device data can provide valuable insight for criminal investigations. Digital devices are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality. Individuals also use digital devices for the aforementioned purposes, and as a tool for facilitating criminal activity.

Digital devices are often used to communicate via voice, text messaging, social media, or other communication applications; and share data with other users and that such digital data can be transferred between various digital devices. Information associated with such data may show evidence of current, on-going, future, and past criminal activity as well as assist law enforcement in determining identity and culpability of participants, including identifying those with knowledge of a criminal offense or identify those who have aided a criminal participant in the commission of a criminal offense, victims and/or witnesses. As such, digital devices possessed by criminal participants can serve both as an instrument for committing crime as well as a storage medium for evidence of the crime, including communications to plan, execute, and otherwise document the commission of a crime.

There have been numerous instances where criminal participants utilized digital devices to photograph themselves, associates and/or co-conspirators, and victims; instances in which digital devices were used by criminal participants to create videos of their criminal activity; instances where criminals participants have used digital devices' internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within digital devices; and instances in which criminal participants used global positioning, mapping and other location services to facilitate in-person meetings with co-conspirators and/or a victim.

On a digital device, data can be created in a matter of moments because most operations can be performed almost instantly, which would be relevant to the incident being investigated. The data can be created intentionally or accidentally by the user, or automatically by the device itself as a part of its regular functioning.

Electronic evidence can remain on the digital devices for indefinite periods of time after the data was created, even if deleted by the user. Data generally is stored on the physical memory of the digital device, but also can be stored on removable storage devices such as Secure Digital (SD) and Subscriber Identification Module (SIM) cards. A forensic examiner may be able to recover information deleted by the user throughout the working life span of the device.

The following are examples of how types of data on digital devices can assist investigators. A full, all-inclusive list would be impossible due to the ever-increasing development of digital devices and their applications:

1. Phone information, configurations, calendar events, notes and user account information which can be used to identify or confirm who owns or was using a digital device. Because of their small size, digital devices can easily be passed from one person. As such it is necessary to document evidence that reveals or suggests who possessed or used the device. This evidence is akin to the search for venue items when executing a search warrant at a residence.
2. Call logs can establish familiarity between people involved in an incident. These records are consistently stamped with dates and times which can be significant regarding the reconstruction of the timeline of events regarding an investigation. Associated contact lists stored in the device can provide names to correspond with voice calls as well as other forms of communication. Voicemails can indicate the purpose of the phone call when the phone call was not answered.

This information can also be invaluable to establish conspirators, witnesses, and suspect information.

3. Data from associated supplemental software applications (apps), both standard and manually installed, stored on the digital devices can demonstrate the user's association with investigated people, locations, and events. Digital devices can run apps which allow them to increase their functionality. Common programs include social media applications, such as Facebook, as well as messaging applications Snapchat and Facebook Messenger to name a few. These applications are increasingly used as alternative methods for users to communicate from the standard messaging service as they offer additional functionality. Many of these applications can determine the user's geographic location which can be instrumental to completing an investigation.
4. Media files such as images, videos, audio, and documents provide first-hand documentation of actions regarding an event. Additionally, files can contain embedded metadata that show additional information which is valuable to investigators such as when and where the file was created. Digital devices can create, store and exchange media with other devices and computers.

Your Affiant seeks to complete a comprehensive and unbiased examination of the data on the device for information which could aid in the investigation; seeking only prescribed information would jeopardize the completeness of the search as it is typically unknown how the electronic device was used or the technical ability and intent of the user before the device has been examined. As with other types of evidence, the context, location, and data surrounding information in the device data is often necessary to understand whether evidence falls within the scope of the search warrant. This type of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes.

Your Affiant knows that digital devices are constantly changing system data on the device as programmed by their manufacturer. Additionally, your Affiant knows that searching the digital device itself would irreversibly alter data and/or evidence on the device. To search a device for evidence, the commonly accepted best practice of digital forensics is to utilize forensic software to obtain an extraction of the data on the device. Attempts will be made to obtain the devices data by only making unobtrusive revocable changes to the system settings to permit the extraction of the data. If necessary, the digital device may require disassembly to obtain the desired data which may render the device inoperable. These processes do not change or alter any of the user data stored on the device. The extraction is then searched using analysis software to locate, identify, and seize the evidence authorized by this warrant. The device and the image are then preserved in evidence.

The digital device has been stored in a manner in which its/their contents are, to the extent material to this investigation, substantially the same state as when it first came into the possession of law enforcement.