

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE)
SEARCH WARRANT FOR)
PROPERTY LOCATED IN THE)
LINCOLN POLICE)
DEPARTMENT PROPERTY)
UNIT, 575 SOUTH 10TH)
STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2328372)

CR 24-1

SEARCH WARRANT
RETURN

CLERK OF THE
DISTRICT COURT

2024 JAN 24 PM 3:15

LANCASTER COUNTY

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

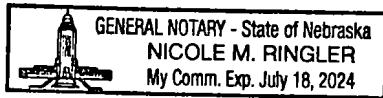
ss.

The undersigned states that he/she received the search warrant issued herein on the 10th day of January, 2024 and that he/she executed the same on the 10th day of January, 2024 and on the 24th day of January, 2024 seized the property/person described in the inventory filed herein and by delivering a copy of the said order for said property/person at the place from which the property/person was taken.

DATE this 24th day of January, 2024.

[Signature] 2/4/24
Inv. Jarod Brabec

SUBSCRIBED AND SWORN to before me this 24th day of January, 2024.



[Signature]
Notary Public

C3009533



[Signature]

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE)
SEARCH WARRANT FOR)
PROPERTY LOCATED IN THE)
LINCOLN POLICE DEPARTMENT)
PROPERTY UNIT, 575 SOUTH)
10TH STREET, LINCOLN,)
LANCASTER COUNTY, NE)
Q2328372)

INVENTORY.

LANCASTER COUNTY
2024 JAN 24 PM 3:16
CLERK OF THE
DISTRICT COURT

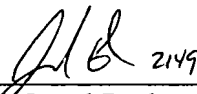
STATE OF NEBRASKA)
) ss.
County of Lancaster)

Inv. Jarod Brabec being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

Attempted device extractions from the following devices (device unable to be extracted):

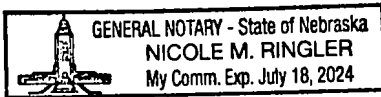
- White iPhone in a clear case which was tagged into LPD Property under Property Q2328372 under LSO case #C3009533

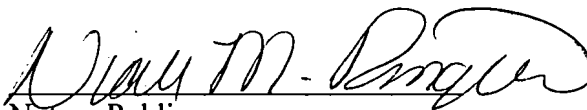
DATED this 24th day of January, 2024.



Inv. Jarod Brabec

SUBSCRIBED AND SWORN to before me this 24th day of January, 2024.





Notary Public

C3009533

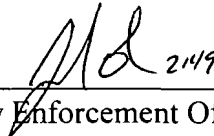
RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from 575 S 10th St Lincoln, Lancaster County, Nebraska:

Attempted device extractions from the following devices (device unable to be extracted):

- white iPhone in a clear case which was tagged into LPD Property under Property #Q2328372 under LSO case #C3009533

DATED this 24th day of January, 2024.



Law Enforcement Officer

WITNESS

LANCASTER COUNTY
2024 JAN 24 PM 3:16
CLERK OF THE
DISTRICT COURT

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

TO: Jarod Brabec, a Deputy Sheriff with the Lancaster County Sheriff's Office (LSO), Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Jarod Brabec, has filed an Affidavit before the undersigned Judge of the County Court of Lancaster County, Nebraska, a copy of which affidavit is attached hereto and made a part hereof; 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 a white iPhone in a clear case which was tagged into LPD Property under Property # Q2328372 under LSO Case #C3009533, for the following items:

Evidence to be searched for includes:

- a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging "app" accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;
b. Evidence of use of the device to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;
c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
d. Evidence of use of the device to conduct internet searches relating to [specify subject of suspected searches and any terms that would have been used in internet searches];
e. Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; "app" data or usage

information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;

f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;

g. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;

h. Records showing a relationship with victim(s), location(s), other suspects, etc.;

i. Names, nicknames, account ID's, phone numbers, or addresses of specific persons;

j. Records showing a relationship to particular areas or locations.;

k. Photographs, images, videos, documents that contain or are evidence of crime(s);

l. Evidence of purchases, such as items used in planning or carrying out crimes;

m. Internet research history conducted while planning, executing, or covering up to commit crimes;

n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;

o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the logs and data associated with the applications, programs or software, and any device backup files;

p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.

Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Given under my hand and seal this 10th day of January, 2024



JUDGE OF THE COUNTY COURT

Rodney D. Reutz
Printed Name of County Court Judge



IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA)
)
COUNTY OF LANCASTER)

ss. AFFIDAVIT FOR SEARCH WARRANT

Jarod Brabec, being first duly sworn upon oath deposes and states that he is a Investigator for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. AFFIANT further states he is currently involved in the investigation of Possession of a controlled substance w/ intent to deliver (marijuana/psilocybin mushrooms) NRS 28-416 and Possession of a controlled substance without tax paid (NRS 77-4302) occurring at NW 48th St/W O St, Lancaster County, Nebraska. Investigator Jarod Brabec, has also reviewed case reports regarding these investigations by all Lancaster County Sheriff Deputies and other involved law enforcement.

The item(s) to be searched for digital evidence are particularly described as:

- a. 1 each, white iPhone in a clear case located in the Lincoln Police Property Evidence Unit at 575 South 10th, Lincoln, Lancaster County, NE, labeled with Property Number Q2328372 labeled with Case Number C3009533;

The items to be searched are currently located at the Lincoln Police Department Property Unit, 575 South 10th, Lincoln, Lancaster County, State of Nebraska. The item(s) to be searched shall be delivered to the Electronic Evidence Unit located at 605 South 10th, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis. The Electronic Evidence Unit forensic examiners may designate additional forensic services, as they may deem necessary to complete the analysis. Once examination and analysis has been completed, the listed evidence shall be returned to the Lincoln Police Department Property Unit, where it will be held until any final disposition by the Court

Facts:

On 12-19-23 at approximately 0914 hrs Amanda McCandless was contacted in a white Chevy Malibu bearing California plates 9JAH337 at Shoemaker's Truck Stop located at MM 395 in Interstate 80 for the traffic violation of driving on the shoulder (NRS 60-6,142) by LSO Deputy Jason Henkel #902135. McCandless provided Deputy Henkel with an Iowa driver's license, and he observed she was the lone occupant of the vehicle.

McCandless stated the vehicle was a rental vehicle and she began pulling up the rental agreement on her cell phone. Deputy Henkel was able to observe the rental agreement and noticed McCandless was the renter of the vehicle and she had rented the vehicle on 12-17-23 in Los Angeles and it was due back on 12-20-23. Deputy Henkel asked McCandless if she lived in California, and she stated she lived in Iowa and had flown to California. During this time, Deputy Henkel noticed McCandless was exhibiting increased nervousness, including excessive blinking, labored breathing, and a visible pulse.

Deputy Henkel then asked McCandless to step out of her vehicle and come back to his cruiser for the enforcement portion of the traffic stop. McCandless questioned the reason for the traffic stop and Deputy Henkel then explained the probable cause for the traffic stop. McCandless stood at Deputy Henkel's open passenger side window of his cruiser. Deputy Henkel then engaged in conversation with McCandless while he completed the enforcement portion of the traffic stop. Deputy Henkel asked McCandless what part of California she was visiting, and she stated she was in Los Angeles. McCandless explained that she had a dog breeding business, where she breeds Frenchies and a friend of hers had a stud dog that she went to Los Angeles to look at for breeding purposes with her female Frenchie. McCandless continued talking about dog breeding and stated she had a family member that lived in Northern California that had another breed of dog that she was interested in breeding and pulled up a picture on her phone, where Deputy Henkel saw that McCandless had her maps function on and running on her phone.

McCandless continued talking with Deputy Henkel and she mentioned she does body modifications, owned a tattoo parlor in Iowa and she does human suspension activities. Human suspension involves placing hooks in the skin and swinging around in the air. Deputy Henkel noticed that McCandless' nervousness had subsided as they continued talking. Deputy Henkel eventually asked McCandless if there was anything illegal in her car and she shook her head "no". Deputy Henkel specifically asked if there were any narcotics, including marijuana, or currency in the vehicle and McCandless stated "no". Deputy Henkel asked McCandless if he could open the trunk on her vehicle to make sure and McCandless indicated she would prefer Deputy Henkel to not open the trunk. Deputy Henkel could tell McCandless' nervousness had increased at this time as she had a visible pulse in her neck, and she started blinking excessively again.

Deputy Henkel explained to McCandless that travelers who fly to California usually end up flying home and don't typically rent a vehicle and McCandless stated she had missed her flight and had gotten pulled over in Colorado on her return trip. Deputy Henkel later confirmed that McCandless was not being truthful about her travel plans as she had flown into California on the 12-17-23 and had rented the car the same day to return to Iowa. McCandless also produced a business card for a Colorado State Trooper that had pulled her over on her way back to Iowa. Deputy Henkel asked for consent to search McCandless' vehicle and she denied consent to search. Deputy Henkel then asked for consent to deploy his trained police dog around the vehicle and McCandless consented to the dog deployment.

Deputy Henkel then returned McCandless' driver's license and traffic warning to her, and McCandless returned to her vehicle and began pumping fuel into the vehicle. Deputy Henkel told McCandless if she only had a small amount of marijuana in the vehicle, it would be no big deal and McCandless said something to the effect of all "cops are mean" or something of that nature. Deputy Henkel noticed McCandless was starting to get upset and her nervousness was increasing again, due to labored breathing and a visible pulse.

At this point, Deputy Henkel believed McCandless was involved in criminal activity due to her abrupt exit at MM 395 on I-80, pulling into a gas station to get fuel when she had half a tank of fuel in her vehicle, visible signs of increased

nervousness, one-way rental from California to Iowa, implausible travel plans and her portrayal of law enforcement as bad people. Deputy Henkel continued to observe McCandless at the fuel pump, where she made a phone call and then was asked to step over and stand by Deputy Henkel's cruiser.

Deputy Henkel then deployed his trained police dog "Koda" to conduct a free-air sniff of the McCandless' rental vehicle, where LSO K9 Koda alerted and indicated to the odor of narcotics emitting from the vehicle. McCandless was detained in the back seat of Deputy Henkel's cruiser and her cell phone was seized at this time. Deputy Henkel noted that McCandless was on a phone call with her husband when the phone was seized, and Deputy Henkel was able to set the phone to the "never lock" function at this time.

A probable cause search of the rental vehicle produced 18 lbs of high-grade marijuana buds, 3.6 lbs of THC oil (1628 THC vape cartridges), 2 lbs of THC hash (32 one oz containers), and 10.62 lbs of psilocybin mushroom chocolate bars (100 1.7 oz bars) in the trunk. Additionally, two boxes of vacuum sealer bags, a blue money bag, a tan money bag, an empty large black odor proof duffel bag were also located. McCandless was read her Miranda Rights by Deputy Henkel and made a comment about it just being "marijuana" in her vehicle, leading Deputy Henkel to believe she knew what the narcotics were that were in her vehicle. McCandless' white iPhone was seized as evidence and tagged into LPD Property under this case number and property #Q2328372. McCandless was lodged at the Lancaster County ADF for possession of a controlled substance with intent to deliver (marijuana/psilocybin mushrooms) (NRS 28-416) and cited for possession of a controlled substance w/out tax paid (NRS 77-4302).

Digital Storage Devices

Your AFFIANT knows from training and experience that digital media devices and related digital storage devices, such as cell phones, can be used to create, edit, delete, share, and store files and other data including, live and deleted documents, photographs, videos, electronic mail (e-mail), search history and other relevant user information.

Your AFFIANT also knows from training and experience that computers and mobile devices, such as cell phones, connected to the Internet, are used to search

the World Wide Web for content and such access can allow users to access and control data such as pictures, videos, documents, and other files.

Your AFFIANT also knows that such devices are often used to communicate and share data with other users and that such digital data can be transferred between various devices. Your AFFIANT knows that information associated with such data may show evidence of current, on-going, future, and past criminal activity. Your AFFIANT knows that this type of information can be used to identify and locate potential victims, witnesses, and co-conspirators.

Your AFFIANT also knows that data associated with these devices can often include user attribution data that can help identify the person(s) who sent, received, created, viewed, modified, or otherwise had control over particular content.

Your AFFIANT has been employed by the Lancaster County Sheriff's Office (LSO) since 2010. Your AFFIANT is currently an Investigator assigned to the LSO Criminal Interdiction Unit and has been in that unit since 2013. Your AFFIANT received law enforcement training at the Nebraska Law Enforcement Training Academy (NLETC) in Grand Island, NE and has attended numerous other trainings since receiving my law enforcement certification at NLETC in 2011. Your AFFIANT has been trained in various types of criminal investigations to include narcotic, weapons, money laundering, fraud, theft and a variety of other criminal investigations. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for all of the above-mentioned investigations. Cellular telephones are used by the general public for communication, access to and sharing of information, research, socialization, entertainment, mapping, shopping, note taking and other functionality.

Your AFFIANT knows from training and criminal investigation experience that individuals also use cellular telephones for the aforementioned purposes, and as a tool for facilitating criminal activity. The data contained on cellular telephones seized in investigations can provide a wealth of information that can assist investigators 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. As such, a cellular telephone 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. Cellular telephones contain location data that can assist in an investigation by both corroborating and disproving statements. Cellular telephones can also show any possible relationships between parties involved through past communications, location data, and contact information stored.

Your AFFIANT is aware from past criminal investigation experience of numerous instances where cellular telephones were used by criminal participants to communicate via voice, text messaging, social media or other communication applications; instances in which criminal participants utilized cellular telephones to photograph themselves, associates and co-conspirators; instances in which cellular telephones were used by criminal participants to create videos of their criminal activity; instances where criminal participants have used cellular based internet applications to research crimes they have or intend to participate in; instances in which criminal participants have maintained notes within cellular telephones and instances in which criminal participants used global positioning, mapping and other location services to facilitate in- person meetings with co-conspirators or a victim;

Through your AFFIANT's training and criminal investigation experience examining cellular telephones, your AFFIANT is aware cellular telephones typically contain electronic records concerning calls made to, from, or missed by the cellular telephone. In addition, cellular telephones typically contain electronic records of text messages sent to and from the telephone, and other types of communication between persons. Cellular telephones typically contain a "phone book" of stored names and telephone numbers.

AFFIANT knows for the year 2023, members of the Lancaster County Sheriff's Office Interdiction Unit has seized and searched 34 cellular phones. Of these phones searched, 29 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is 85.29%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain

evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT knows for the year 2022, members of the Lancaster County Sheriff's Office Interdiction Unit has seized and searched 61 cellular phones. Of these phones searched, 60 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is 98.36%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT knows for the year 2021, members of the Lancaster County Sheriff's Office Interdiction Unit has seized and searched 46 cellular phones. Of these phones searched, 45 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is 97.82%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT knows for the year 2020, members of the Lancaster County Sheriff's Office Interdiction Unit had seized and searched 104 cellular phones. Of these phones searched, 99 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is 95.19%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT knows for the year 2019, members of the Lancaster County Sheriff's Office Interdiction Unit had seized and searched 131 cellular phones. Of these phones searched, 128 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is 97.7%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT knows that for 2018, members of the Lancaster County Sheriff's Office Interdiction Unit had seized and searched 88 cellular phones. Of these phones searched, 85 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is approximately 96.59%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

AFFIANT Knows that for the full year of 2017, members of the Lancaster County Sheriff's Office Interdiction Unit had seized and searched 140 cellular phones. Of these phones searched, 139 phones were found to contain evidence related to narcotic sales, manufacturing and other evidence that related to the Lancaster County Sheriff's Office cases. The percentage of phones seized, to phones searched that contained narcotic related activity is approximately 99.28%. This percentage shows a strong correlation between cellular phones that are in the possession of those who are arrested, with the probability that the cellular phones contain evidence related to the narcotic investigation the Deputies are conducting on these individuals.

Through your AFFIANT's training and experience with examining digital devices, your AFFIANT is aware cellular telephones typically contain electronic records concerning calls made to, from, or missed by cellular telephone. In

addition, digital devices typically contain electronic records of messages sent to and from the device, and other types of communications between persons. Digital devices typically contain a “contact list” of stored names, telephone numbers, usernames, and accounts.

Your AFFIANT know evidence can remain on the device or media for indefinite periods of time after the communication originally took place, even if deleted by the user. A forensic examiner may be able to recover information deleted by the user throughout the working life span of the device.

Your AFFIANT knows digital data can be found in numerous locations, and formats. Evidence can be embedded into unlikely files for the type of evidence, such as a photo included in a document or converted into a PDF file or other format in an effort to conceal their existence. Information on devices and media can be stored in random order; with deceptive file names; hidden from normal view; encrypted or password protected; and stored on unusual devices for the type of data, such as routers, printers, scanners, game consoles, or other devices that are similarly capable of storing digital data.

Your AFFIANT knows, that, wholly apart from user-generated files and data, digital devices and media typically store, often without any conscious action by the user, electronic evidence pertaining to virtually all actions taken on the digital device, and often information about the geographic location at which the device was turned on and/or used. This data includes logs of device use; records of the creation, modification, deletion, and/or sending of files; and uses of the internet, such as uses of social media websites and internet searches/browsing.

Your AFFIANT knows device-generated data also includes information regarding the user identity at any particular date and time; usage logs and information pertaining to the physical location of the device over time; pointers to outside storage locations, such as cloud storage, or devices to which data may have been removed, and information about how that offsite storage is being used. If the device is synced with other devices, it will retain a record of that action. Digital device users typically do not erase or delete this evidence, because special software or use of special settings are usually required for the task. However, it is technically possible to delete this information.

Your AFFIANT knows digital devices can also reveal clues to other locations at which evidence may be found. For example, digital devices often maintain logs of connected digital or remote storage devices. A scanner or printer may store information that would identify the digital device associated with its use. Forensic

examination of the device can often reveal those other locations where evidence may be present.

Your AFFIANT knows, 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 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 the forensic examiner may also need the following items in order to conduct a thorough and accurate search of the devices: computer hardware, software, peripherals, internal or external storage devices, power supplies, cables; internet connection and use information; security devices; software; manuals; and related material.

Your AFFIANT knows, that searching the digital device itself would irreversibly alter data and/or evidence on the device. The commonly accepted best practice method to search a digital device for evidence involves creating a digital image of the device and then searching that image for the responsive evidence. Creating a forensic image does not alter any evidence on the device; it only copies the data into a searchable format. The image is then searched using search tools to locate and identify that evidence whose seizure is authorized by this warrant. The unaltered device and the image are then preserved in evidence.

Your AFFIANT knows modern digital devices and media can contain many gigabytes and even terabytes of data. Due to the potential for an extremely large volume of data contained in devices and media, and that fact that evidence can be stored/located in unanticipated locations or formats and/or embedded in other items stored on the device/media, investigators typically need to use specialized equipment in their search. Such large volumes of data also mean that searches can take days or even weeks to complete.

Your AFFIANT also requests authority to obtain assistance from a technical specialist, to review the digital device(s) and digital media for the best and least intrusive method of securing digital evidence that this warrant authorizes for seizure, and to assist in securing such evidence.

Based on all the foregoing information, there is probable cause to believe that evidence of the above-listed crimes exists in the above-described digital devices and that there is probable cause to search those devices for the evidence of the above crimes.

Your AFFIANT knows from my training and experience, and from information provided to me by Electronic Evidence Unit Personnel that it is necessary to search live and deleted data recovered from digital devices from the time when the device was first used through the time when the device was seized. This is specifically necessary to establish associations between a particular device and associated applications and files to a particular user (or users). This scope of time is necessary to identify potential inculpatory and exculpatory evidence during the planning, execution and post event activities of potential criminal activity. These activities may include communication, contact, calendar entries, pictures, videos, location information (including GPS, navigation, and maps), This scope of time is also necessary to determine accurate device date and time settings, including time zone changes, and allow for the analysis any associated data within a proper context. I know from my training and experience that it is important to understand events of a particular day and time in proper context that may exist before and to attribute particular users of a device and associated applications.

For the technical reasons described, the digital evidence listed above shall be submitted to the Electronic Evidence Unit located at 605 South 10th St, Lincoln, Lancaster County, State of Nebraska for digital forensic processing and analysis.

The above does constitute grounds of probable cause for the issuance of a Search Warrant for:

- Black iPhone which was tagged into LPD Property under Property # Q2319192

Evidence to be searched for includes:

- a. Evidence of other accounts associated with this device including email addresses, social media accounts, messaging “app” accounts, and other accounts that may be accessed through the digital device that will aid in determining the possessor/user of the device;
- b. Evidence of use of the device to communicate with others about the above-listed crime(s), via email, chat sessions, instant messages, text messages, app communications, social media, internet usage, and other similar digital communications;

- c. Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
- d. Evidence of use of the device to conduct internet searches relating to [specify subject of suspected searches and any terms that would have been used in internet searches];
- e. Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between the above-listed dates; “app” data or usage information and related location information; IP logs or similar internet connection information, and images created, accessed or modified between the above-listed dates, together with their metadata and EXIF tags;
- f. Evidence of the identity of the person in possession of the device(s) and the associated times and dates. Such evidence may be found in digital communications, photos and video and associated metadata, IP logs, documents, social media activity, and similar data;
- g. Records linking the suspect(s), co-conspirators, victim(s), witness(es) to a certain screen name, handle, email address, Social media identity, etc.;
- h. Records showing a relationship with victim(s), location(s), other suspects, etc.;
- i. Names, nicknames, account ID’s, phone numbers, or addresses of specific persons;
- j. Records showing a relationship to particular areas or locations.;
- k. Photographs, images, videos, documents that contain or are evidence of crime(s);
- l. Evidence of purchases, such as items used in planning or carrying out crimes;
- m. Internet research history conducted while planning, executing, or covering up to commit crimes;
- n. Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, user names, screen names, remote data storage accounts, documents, files, calendars, metadata, recycle bin files, and any other information and evidence that may demonstrate attribution to a particular user or users;
- o. Any live and deleted applications, programs, or software, used to facilitate the creation, storage, display, or transmission of digital visual recordings and the

logs and data associated with the applications, programs or software, and any device backup files;

p. Any live and deleted audio or visual recording files including files bearing file extensions jpg, jpeg, png, gif, tif, wav, aiff, mp3, mp4, avi, mpg, mpeg, flv, mp4, mov, and wmv along with any descriptive metadata within or associated with the visual recording files, which may include date and time the recording was created, the device used to create the recording and location the recording was made;

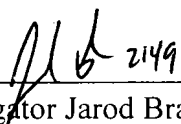
q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user(s) of the computers or digital devices including web browser history; temporary Internet files; cookies, bookmarked or favorite web pages; e-mail addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; e-mails, instant messages, text messages (SMS/MMS), application data and other electronic communications; address books; contact lists; records of social networking and online service usage; calendar entries, notes, journals, and any software that would allow others to control the digital device such as viruses, Trojan horses, malware, and other forms of malicious software.

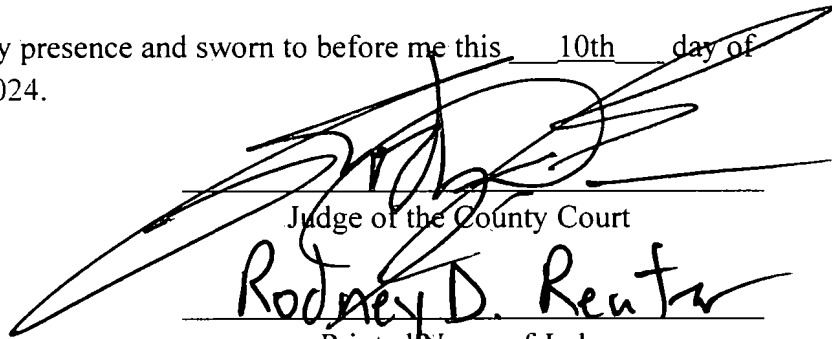
Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Further AFFIANT saith not;

Dated this 10th day of January, 2024.


Investigator Jarod Brabec, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 10th day of
January, 2024.



Judge of the County Court

Rodney D. Reuter
Printed Name of Judge

