

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)
Q2406399)

CR 24-1

SEARCH WARRANT
RETURN

LANCASTER COUNTY
2024 JUN -5 PM 2:57
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

ss.

The undersigned states that he/she received the search warrant issued herein on the 14th day of May, 2024 and that he/she executed the same on the 28th day of May, 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 30th day of MAY, 2024.

[Signature]
Inv. Tyler Loos

SUBSCRIBED AND SWORN to before me this 30th day of May, 2024.

[Signature]
Notary Public

C4002487



247

[Handwritten mark]

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)
Q2406399)

INVENTORY

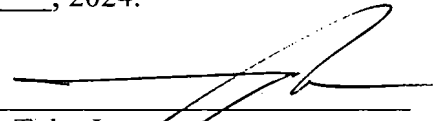
LANCASTER COUNTY
2024 JUN - 5 PM 2: 57
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
County of Lancaster) ss.
County of Lancaster)

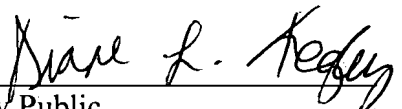
Inv. Tyler Loos being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

- User data, including photos/videos, text messages, call logs, contacts, web search history, network connections, notes, user accounts

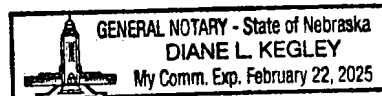
DATED this 30th day of MAY, 2024.


Inv. Tyler Loos

SUBSCRIBED AND SWORN to before me this 30th day of May, 2024.


Notary Public

C4002487



RECEIPT

The undersigned hereby acknowledges receipt of the following described data seized from the Apple iPhone, labeled with property number Q2406399 and case number C4002487, Lincoln, Lancaster County, Nebraska:

-User data, including photos/videos, text messages, call logs, contacts, web search history, network connections, notes, user accounts

LANCASTER COUNTY

2024 JUN -5 PM 2: 57

CLERK OF THE
DISTRICT COURT

DATED this 28th day of May, 2024.


Law Enforcement Officer


WITNESS

C4002487

LANCASTER COUNTY
2024 JUN -5 PM 2:57

CLERK OF THE
DISTRICT COURT

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

TO: Tyler Loos, a Deputy Sheriff with the Lancaster County Sheriff's Office,
Lancaster County, Nebraska, and any and all law enforcement officers.

WHEREAS, Tyler Loos, 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 the following device(s) in the
custody of the Lincoln Police Department Property Unit, 575 South 10th, Lincoln,
Lancaster County, Nebraska:

- 1. Apple iPhone, labeled with Property Number Q2406399 and Case Number
C4002487.

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 aforementioned
crimes, 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 the
aforementioned crimes;
- e. Information that can be used to calculate the position of the device, including
location data; GPS satellite data; GPS coordinates for routes and destination queries;
application data or usage information and related location information; IP logs or similar

internet connection information; and images created, accessed or modified, 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 Michael Glaser, victims, and/or witnesses to a certain screen name, handle, email address, social media identity, etc.;

h. Records showing a relationship with Michael Glaser, co-conspirator(s), victim(s), witness(es), and/or location(s), etc.;

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

j. Records showing a relationships to particular areas or locations associated with the aforementioned crimes;

k. Photographs, images, videos, documents that contain or are evidence of the aforementioned crimes;

l. Evidence of purchases, such as items used in planning or facilitating the aforementioned crimes;

m. Internet research history conducted while planning, executing, or covering up the aforementioned 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;


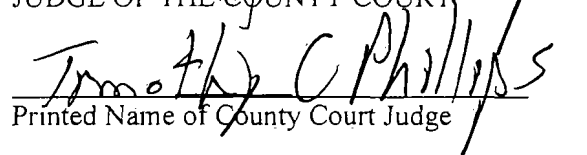
q. Any live and deleted passwords, password files, keys, encryption codes, or other information necessary to access the digital device, software or data stored on the digital device;

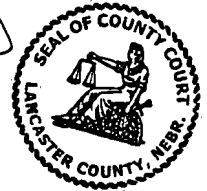
r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this affidavit, that show the actual user of the computers or digital devices including web browser history; temporary Internet files; 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.

This Court, being duly advised that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence, finds 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 14th day of May, 2024.


JUDGE OF THE COUNTY COURT

Printed Name of County Court Judge



IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

Tyler Loos, being first duly sworn upon oath deposes and states that he is a Deputy Sheriff for the Lancaster County Sheriff's Office, Lancaster County, Nebraska. Your Affiant further states he is currently involved in the investigation of Attempted 2nd Degree Assault on a Peace Officer, Terroristic Threats, Use of a Weapon to Commit a Felony, Possession of a short shotgun, and intimidation by telephone or electronic device, occurring at Casey's Gas Station at 2500 NW 12th, Lincoln, Lancaster County, Nebraska. As part of the investigation, your Affiant has consulted with other law enforcement and reviewed case reports. Your Affiant states as follows:

The item to be searched for digital evidence is particularly described as:

- 1. Apple iPhone, labeled with Property Number Q2406399 and Case Number C4002487.

The item to be searched is in the custody of the Lincoln Police Department Property Unit, 575 South 10th, Lincoln, Lancaster County, Nebraska. The item(s) to be searched shall be delivered to the Electronic Evidence Unit, located at 605 South 10th, Lincoln, Lancaster County, Nebraska for digital forensic processing and analysis. The Electronic Evidence Unit forensic examiners may designate additional forensic services, as deemed 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.

RELEVANT FACTS

On April 2nd, 2024, Officers with the Lincoln Police Department were notified of a male, later identified as Michael Glaser, at Casey's gas station at 2500 NW 12th with a firearm. When officers arrived on location Glaser discharged a firearm at officers, who returned fire. Officers attempted communication with Glaser for approximately 30 minutes and he refused to comply with their commands. Glaser then fired his weapon again at the officers, who again returned fire. Glaser was struck twice and ultimately taken into custody.

Your Affiant is aware Investigator Tim Cronin, an employee of the Lincoln Police Department, interviewed Kiarra Oliver who is an employee of Casey's gas station. Oliver stated she was outside smoking with another coworker, Andrew Jones, when she saw a black SUV pull into the lot and park at an awkward angle. Oliver observed a male exiting the vehicle that she recognized as Glaser. Oliver was aware that Glaser was previously in an intimate dating relationship with another Casey's employee, Stormy Tackett. Oliver saw that Glaser was carrying a handgun and a box of ammunition when he approached her and asked if Tackett was at work. When Oliver said Tackett was not there, Glaser forced Oliver and Jones back into the store.

Your Affiant knows Investigator O'Connor interviewed Glaser about the events leading up to his arrival at Casey's gas station. Approximately five days prior, Glaser's wife Stormy Tackett returned to his apartment at 2737 A St #2 to try to work on the marriage with Glaser. However, on April 2nd, 2024, Tackett ended it. Glaser said he had been consuming alcohol since 10:00 AM and felt he wanted to die. Glaser said he had WWII guns inside of this residence and he had an extra box of ammunition that he brought with him to Casey's.

Your Affiant knows Stormy Tackett was interviewed by investigators. Tackett stated she moved into the apartment at 2737 A St #2 in November of 2023. In January 2024, Tackett moved out after ending the relationship, however she returned approximately five days to try to work on the relationship. On April 2nd, 2024, Tackett went to her job at Casey's gas station at 2500 NW 12th. At or about 1:36 PM, Tackett sent a text message to Glaser stating she wanted to end the relationship. Tackett then resumed working and did not look at her phone again until Glaser contacted the store phone looking for her. Tackett then saw that she had multiple text messages from Glaser, and she subsequently blocked his number from her cellphone and the store phone. Tackett ended her shift at 6:30 PM and left Casey's. Tackett said around 18 months to two years ago she and Glaser purchased several firearms together. Tackett named a .45, two 9MMs, and a shotgun. Tackett did not take any of the firearms with her when she moved out. Tackett had reported to law enforcement on February 7th, 2024, Glaser was sending text messages to Tackett that she felt were threatening. Glaser said that he would make Tackett 'pay.' Glaser also stated he was going to show up at Tackett's job and cause a scene so that he could go to jail. Glaser sent another text stating, 'Only I have nothing to lose...And I want to fucking die, and I am not afraid of the police...You have taken every inch of my fucking life you bitch...I hope you call them on me tonight, so I can fucking shoot at them.' Tackett also told law enforcement that Glaser regularly consumes alcohol and uses cocaine.

Your Affiant knows a residential search warrant was served at Glaser's residence in Lincoln, Nebraska in the early morning hours following his apprehension. During that time, an illegal short shotgun was located and seized.

Your Affiant knows Tackett informed Inv. Kelly that Glaser has an Apple iPhone. Your Affiant also knows an iPhone was recovered by crime scene technicians on the floor behind the counter at the Casey's gas station. During review of in store surveillance footage showing an overhead view of the store's counter, Glaser was observed to fall over. Prior to falling over, no cellphone was observed on the floor near him. After Glaser fell over and got back up, a cellphone is observed on the floor next to him. The phone is observed via footage to have a lit background with a small blue design element. Your Affiant knows the iPhone recovered by crime scene technicians also has the same background.

Due to the above foregoing information, it is obvious the iPhone recovered by crime scene technicians belongs to Glaser.

INVESTIGATOR BACKGROUND

Your Affiant is a certified law enforcement officer in the State of Nebraska with 11 years of experience investigating crimes including, but not limited to domestic violence, narcotics, theft, sexual assaults, and homicides. Your AFFIANT is a Technical Investigator assigned to the Lancaster County Sheriff's Office Criminal Investigations Division and has received training and experience in technologically advanced investigative tools, including cellular devices. Through such training and experience, your Affiant understands the capabilities of cellular devices and the valuable information contained within pertaining to criminal investigations. Furthermore, most people possess cellular telephones and other connected devices (tablets, watches, laptops, etc.) used to communicate electronically. It can be generally recognized that cellular devices tend to accompany their users everywhere, and thus, it may be inferred that a suspect's cellular phone accompanied the suspect at the time of the crime.

Your Affiant knows from his training and experiences that dedicated GPS devices store large amounts of data. Location data including waypoints, search history, home location and routes of travel all are stored on the device. GPS devices record location points while powered on, and this data is also stored on the device. GPS devices can also be used as

removable media, with the capability of storing any digital data. GPS devices record location points while powered on, and this data is also stored on the device.

Your Affiant knows from his training and experiences that SIM cards, or Subscriber Identification Module, are used in GSM cellular networks. SIM cards can contain subscriber identification numbers, text messages, and contacts, among other identifying information.

Your Affiant knows from his training and experiences that images and data captured on cellular devices or tablets are easily transferred. Data or data files can be transferred from device to device via storage cards, and wireless technologies. Data can also be transferred to computers via data cables or wireless technology.

Your Affiant knows that cellular devices and tablets can contain data in memory such as email, text messages, calendar events, contacts, photographs, videos, and call records.

Your Affiant also knows from his training and experiences that cellular devices, especially 'smart phones', and tablets can access the internet in the same capacity as a desktop computer. Smart phones and tablets have internet web browsers, email clients, and software to enable the same functionality as a traditional desktop or laptop computer.

Your Affiant knows from his training and experience those cellular devices, especially 'smart phones' and tablet devices using the Android and Apple iOS operating systems, create and store GPS (Global Positioning System) data. This data can be stored for the lifetime of the phone or tablet.

Your Affiant also has knowledge in the forensic analysis of computers, cellular devices, and other digital media. Your AFFIANT advises that the examination of computer files, documenting the examination, and making evidentiary and discovery copies of evidence found on a computer and storage devices is a lengthy, technical process. It is necessary to determine that no security devices are in place, which causes the destruction of evidence during the search. In some cases, it is impossible to even conduct a search without expert technical assistance.

Electronic device data search protocols are exacting procedures designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Using these procedures, it is also possible to recover evidence from "slack space" and/or "unallocated space" of the storage media. The data in these areas is not controlled by the user of a computer and can exist on a computer for

extended periods of time. In theory, it can exist for several years. It is possible that evidence is contained within the data stored in the slack space and/or unallocated space.

Your Affiant also advises the Court that technical expertise is necessary to complete examination of electronic evidence. Because of the possibility that files may be hidden, or codes put in place to prevent the retrieval of data, it may become necessary to request assistance of an individual/s who are not commissioned law enforcement officers but who are trained and/or learned in the retrieval of data stored in a computer or related devices.

Your Affiant also advises that an examination requires all peripheral devices, software and documentation, printed and handwritten, be seized since it would be impossible without examination to determine that it is standard, commercially available software and/or hardware. In some instances, it is necessary to have the software used to create data files and records in order to read the files and records. In addition, without examination, it is impossible to determine that the disks purporting to contain standard commercially available software program has not been used to store records instead.

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 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 within applications on cellular devices.

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 criminal activity.

Your Affiant advises that it has been recognized by the Nebraska Supreme Court that law enforcement cannot predict where evidence of a crime will be located in a cellular device, or call records, or in what format, such as texts, videos, photographs, emails, or applications. And it has been further stated that there is no way for law enforcement to know where in the digital information associated with cell phones it will find evidence of the specified crime. Consequently, a brief examination of all electronic data associated with a cell phone is usually necessary to find where the information to be seized is located, and such examination is reasonable under the Fourth Amendment.

No wire communications or electronic communications will be intercepted. There is no reason to believe that any of the computers operate in any way as a server of an electronic bulletin board service. As such, the provisions of the Wire and Electronic Communications Interception Act would not apply. Should information of this type be discovered, it would be set aside, unopened.

There is no indication that there is any "work product" or "documentary" material stored on the computers with the purpose of disseminating to the public a newspaper, broadcast, or other similar form of public communication. Should officers become aware of any such materials, they shall be returned as quickly as circumstances permit.

Furthermore, your Affiant advises that the examination of an electronic device is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, your AFFIANT would like to advise the Court that it may not be possible to complete a return to the Court within the 10 days normally required by the Courts.

Your Affiant believes that the information presented to him is factual and that there is reason to believe that the below-mentioned property has location and communication data, along with other evidence related to this case.

The above does constitute grounds of probable cause for the issuance of a Search Warrant for the following device(s):

1. Apple iPhone, labeled with Property Number Q2406399 and Case Number C4002487.

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 aforementioned crimes, 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 the aforementioned crimes;

e. Information that can be used to calculate the position of the device, including location data; GPS satellite data; GPS coordinates for routes and destination queries; application data or usage information and related location information; IP logs or similar internet connection information; and images created, accessed or modified, 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 Michael Glaser, victims, and/or witnesses to a certain screen name, handle, email address, social media identity, etc.;

h. Records showing a relationship with Michael Glaser, co-conspirator(s), victim(s), witness(es), and/or location(s), etc.;

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

j. Records showing a relationships to particular areas or locations associated with the aforementioned crimes;

k. Photographs, images, videos, documents that contain or are evidence of the aforementioned crimes;

l. Evidence of purchases, such as items used in planning or facilitating the aforementioned crimes;

m. Internet research history conducted while planning, executing, or covering up the aforementioned 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;

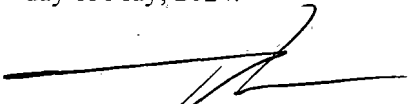
r. Any live and deleted records, documents, programs, applications, information, or materials created, modified, or stored in any form on the digital devices listed in this

affidavit, that show the actual user 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 14th day of May, 2024.

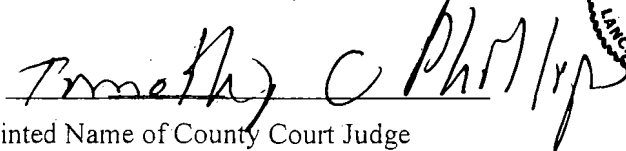


Tyler Loos, Affiant

SUBSCRIBED to in my presence and sworn to before me this 14th day of May, 2024.



JUDGE OF THE COUNTY COURT



Printed Name of County Court Judge

