

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH )  
WARRANT OBTAINED FROM )  
THE LANCASTER COUNTY )  
SHERIFF'S OFFICE/ LINCOLN )  
POLICE DEPARTMENT )  
ELECTRONICS EVIDENCE UNIT, 605 )  
SOUTH 10<sup>TH</sup> STREET, LINCOLN, )  
LANCASTER COUNTY, NE- )  
Q2403510 )

CR 24-1

SEARCH WARRANT  
RETURN

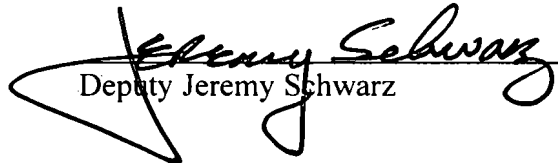
STATE OF NEBRASKA )  
COUNTY OF LANCASTER )

ss.

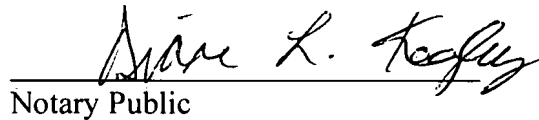
LANCASTER COUNTY  
2024 MAR 19 PM 2:38  
CLERK OF THE  
DISTRICT COURT

The undersigned states that he/she received the search warrant issued herein on the 28th day of February, 2024 and that he/she executed the same on the 8th day of March, 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.

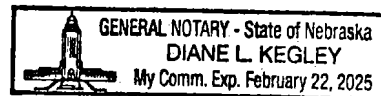
DATE this 18 day of March, 2024.

  
Deputy Jeremy Schwarz

SUBSCRIBED AND SWORN to before me this 18<sup>th</sup> day of March, 2024.

  
Notary Public

C4000263





IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE SEARCH )  
WARRANT OBTAINED FROM )  
THE LANCASTER COUNTY SHERIFF'S )  
OFFICE/ LINCOLN POLICE )  
DEPARTMENT ELECTRONICS )  
EVIDENCE UNIT, 605 SOUTH 10<sup>TH</sup> )  
STREET, LINCOLN, LANCASTER )  
COUNTY, NE- Q2403510 )

INVENTORY

CLERK OF THE  
DISTRICT COURT

2024 MAR 19 PM 2:39

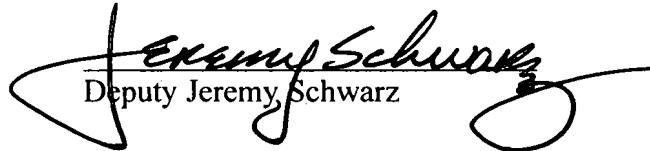
LANCASTER COUNTY

STATE OF NEBRASKA )  
 ) ss.  
County of Lancaster )

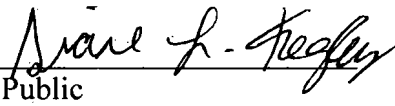
Deputy Jeremy Schwarz being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

- A full file extraction

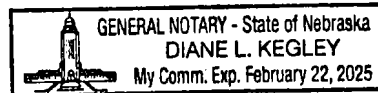
DATED this 18 day of March, 2024.

  
Deputy Jeremy Schwarz

SUBSCRIBED AND SWORN to before me this 18<sup>th</sup> day of March, 2024.

  
Notary Public

C4000263



RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from a black Samsung cellular phone located in the Electronic Evidence Unit located at 605 S. 10<sup>th</sup> Street, Lincoln, Lancaster County, Nebraska and labeled with Property Report number Q2403510:

A full file extraction.

LANCASTER COUNTY  
2024 MAR 19 PM 2:39  
CLERK OF THE  
DISTRICT COURT

DATED this 8<sup>th</sup> day of March, 2024.

  
Law Enforcement Officer

  
WITNESS

C4000263

LANCASTER COUNTY

2024 MAR 19 PM 2:39

CLERK OF THE DISTRICT COURT

IN THE COUNTY OF LANCASTER COUNTY, NEBRASKA

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

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

WHEREAS, Jeremy Schwarz, 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 black Samsung cell phone labeled with Property Report Q2403510 and stored at the Lincoln Police Department Property Division located at 575 S. 10th Street, Lincoln, Lancaster County, Nebraska 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;

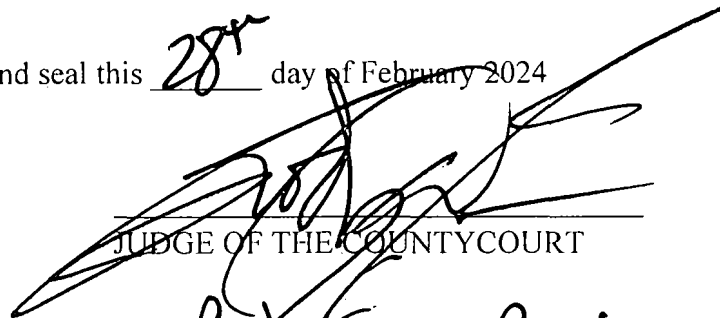
- c) Photographs, images, videos, documents, and related data created, accessed, read, modified, received, stored, sent, moved, deleted or otherwise manipulated;
- d) Evidence of use of the device to conduct internet searches relating to above listed crime(s);
- e) Information that can be used to calculate 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 above listed crime(s);
- l) Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);

- m) Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);
- n) Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, usernames, 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 28<sup>th</sup> day of February 2024



JUDGE OF THE COUNTY COURT

Rodney D. Rents

Printed Name of County Court Judge



LANCASTER COUNTY

2024 MAR 19 PM 2:39

CLERK OF THE DISTRICT COURT

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA )  
 )  
COUNTY OF LANCASTER )

ss. AFFIDAVIT FOR SEARCH WARRANT

Jeremy Schwarz, 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 theft by unlawful taking or disposition N.R.S. 28-511, occurring in Lincoln, Lancaster County, Nebraska. As part of the investigation, AFFIANT has consulted with other involved law enforcement and reviewed case reports. AFFIANT states as follows:

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

A black Samsung cellular phone located in the Lincoln Police Property Evidence Unit at 575 South 10<sup>th</sup>, Lincoln, Lancaster County, NE, labeled with Property Number Q2403510 labeled with Case Number C4000263.

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 Thursday, January 11, 2024, your AFFIANT received a call from Detective 'Chip' Dunlap, an employee of the Putnam County Sheriff's Office, located at 130 Orié Griffin Blvd, Palatka, Florida. Detective Dunlap is assigned to the Criminal Investigation Division and was tasked with investigating a fraud case involving Bitcoin (cryptocurrency).

Through conversations with Detective Dunlap and a review of his investigative reports, your AFFIANT knows victims Fay M and Norbert Slater received a call on August 23, 2023, at 5:31 p.m., from a person reporting to be 'Deputy Park's from the Putnam County Sheriff's Office. The Slater's were told Norbert had an active warrant, and the warrant could be resolved by paying the fine amount of \$9,280.00. Fay Slater was directed to deposit the money in a 'Coinflip' machine. Fay was directed to pay an additional \$4,500.00, however; the caller agreed to an additional \$1,100.00 after Fay claimed she didn't have the additional \$4,500.00. The total loss reported to the Putnam County Sheriff's Office is \$10,380.00.

During the conversation between Fay Slater and the person purporting to be Deputy Parks, she was given the account number 531-220-0699 to deposit the money into.

With a Florida subpoena, Detective Dunlap obtained documents from Coinflip. Detective Dunlap discovered 531-220-6999 is cellular phone number that belongs to Kena Kinnan of Lincoln, Nebraska, and was identified as the person who opened the Coinflip account and called Coinflip customer service. Detective Dunlap requested assistance from your AFFIANT in the interview of Kena Kinnan to determine her level of involvement.

Your AFFIANT knows the photograph and personal information of Kena Kinnan Nebraska's operator's license H13777835 and personal information in the local law enforcement record management system matched the account information provided by Coinflip.

Your AFFIANT reviewed the images provided by Detective Dunlap and discovered Kena Kinnan's driver's license was taken on a glass counter with what appears to be a Nintendo game controller next to it. A Google search of Coinflip ATMs in Lincoln, Lancaster County, Nebraska revealed six locations. Most of the locations appear to be CBD (Cannabidiol) remedy stores, however; one of the locations is Game Stop located at 1713 O Street, Lincoln, Lancaster County. The timestamp of the photo along with a photo of Kena Kinnan at the counter is dated July 30, 2023.

12 images of various unknown individuals were also provided and appeared to be images captured from Coinflip machines. It is your AFFIANT's belief these 12 people are victims of the scam reported by Fay M and Norbert Slater.

According to investigative reports, your AFFIANT knows between August 1<sup>st</sup> and September 1<sup>st</sup>, 2023, Kena Kinnan received eight (8) Coinflip transactions totaling \$36,885.00. Your AFFIANT also knows, a second suspect identified by the initials C.P. with a Georgia driver's license was also identified. Between August 1<sup>st</sup> and September 1<sup>st</sup>, 2023, C.P. received \$42,675.00. Your AFFIANT knows on August 25, 2023, Fay and Norbert Slater used Terminal BT105775 at 4:48 and 5:44 p.m. and conducted two transactions and generated two transaction identification numbers RHXYSU and RSHXU3. Customer identification number "IKD7CVSTDBKMCZI8" identified as Kena Kinnan was used to send the money to the Destination Address "bc1qk.....wzuh." Your AFFIANT also knows nine (9) minutes later at 5:53 p.m., Fay and Norbert Slater initiated a third transaction from the same Terminal and generated a transaction identification number REY4TU. Customer identification number IE8YC4XA7EOU4XY was used to send the money to the same Destination address "bc1qk.....wzuh."

Additionally, I located another photograph of Kena Kinnan with a white female wearing glasses and a tattoo on her right shoulder standing next to her. Your AFFIANT sent the image to the Nebraska Department of Motor Vehicles Fraud Unit for facial recognition. Your AFFIANT received a response from DMV indicating the most likely candidate is Danika Rae Kinnan, Kena's mother. A check of jail book-in information for Danika Kinnan indicated she as a 'Rose' tattoo on a shoulder (shoulder non-specified).

Your AFFIANT researched the local law enforcement record management system and discovered Danika Kinnan's cellular phone number is 402-610-4801.

On January 12, 2024, your AFFIANT knows Z. Windle, Crime Analyst for the Lancaster County Sheriff's Office and assigned to the Criminal Investigative Division, served a signed Lancaster County Subpoena to Verizon Wireless for Kena Kinnan's cellular phone number 531-220-6999. Your AFFIANT knows Verizon Wireless complied with the subpoena and provided the requested records on February 16, 2024.

During investigative follow-up, your AFFIANT analyzed the cellular records and discovered knows between July 1, 2023, and January 11, 2024, Kena and Danika Kinnan communicated 534 times. 171 were cellular calls and 363 were cellular text. Of the 363 cellular texts, 14 were multimedia messaging services. Your AFFIANT also discovered a Georgia area code phone number 404-499-6222. A search of the phone number using law enforcement database indicated the number is used by three people.

On Friday, February 22, 2024, Kena Kinnan voluntarily submitted to an interview at the Lancaster County Sheriff's Office located at 575 S. 10<sup>th</sup> Street, Lincoln, Lancaster County, Nebraska. Kena Kinnan told your AFFIANT her mother, Danika Kinnan has a boyfriend, Tye LNU (last name unknown) who is currently incarcerated in a prison outside Nebraska.

Kena Kinnan admitted she opened a Coinflip account at the direction of her mother and Tye LNU. Kena Kinnan confirmed the personal information provided by Coinflip is her personal information and she and her mother are in the photographs captured by the Coinflip machine.

According to Kena Kinnan, Tye LNU began using her to receive money from people unknown to her toward the end of Spring or early Summer 2023. Kena Kinnan stated when she received the money from Coinflip, she moved the money to a secondary payment system i.e., Cash App, Chime, or Apple Pay. Kena Kinnan stated she would then forward the money at the direction of Tye LNU or her mother, Danika Kinnan to another unknown person. Kena Kinnan told your AFFIANT she stopped doing this in September or October 2023. Kena Kinnan stated the communication between her, and Tye LNU would take place either individually by cellular phone or through a three-way cellular phone call facilitated by her mom, Danika Kinnan. Kena Kinnan believed she conducted between 10 and 20 transactions for approximately \$5,000.00 to \$6,000.00.

Following the interview of Kena Kinnan, your AFFIANT interviewed Danika Kinnan outside her residence located at 3815 NW 53<sup>rd</sup> Street, Lincoln, Lancaster County, Nebraska. Danika Kinnan stated she is engaged to a Tye Brent who is incarcerated in a Georgia State Prison. Danika Kinnan stated she and Tye Brent talk daily by cellular text or voice communication. Danika Kinnan told your AFFIANT Tye Brent calls from the prison and the phone number he calls from vary by which phone he uses.

Danika Kinnan told your AFFIANT she has received money from friends and family members of Tye Brent, and has sent the money to her daughter, Kena Kinnan to deposit onto Tye Brent's prison books. Danika Kinnan stated her bank card is linked to Tye Brent's cellmate whose name she could not recall. Danika Kinnan could not provide a valid explanation why she has a financial card linked to another inmate other than her fiancé.

Danika Kinnan told your AFFIANT in 2023 she received money from random people via Kena Kinnan's Coinflip account. The money was transferred from Coinflip to a secondary payment system owned by Kena Kinnan. Kena Kinnan would then forward it to another person or to her personally where she would place it on her own secondary payment system (i.e., Cash App, Chime, PayPal, or Apply Pay); before it was transferred to another random person. Danika Kinnan stated this was done on behalf of Tye Brent's former cellmate, Joshua Nut, who claimed the money came from online betting. Danika Kinnan stated she

managed all of these secondary payment systems on her cellular phone. Danika Kinnan stated she still sends money to Tye Brent.

Before the interview ended, your AFFIANT seized Danika Kinnan's black Samsung smartphone that was resting on the trunk of a white car parked in the driveway of her residence where your AFFIANT was standing. Your AFFIANT knows Danika Kinnan requested her phone back after she was informed the phone was being seized.

On February 27, 2024, your AFFIANT contacted the Georgia Department of Corrections in an attempt to identify Tye Brent and is awaiting a response.

According to Conflip.tech/faq, your AFFIANT knows "Coinflip is the leading Bitcoin ATM operator in the world with 24/7 customer support and low fees." Your AFFIANT also knows Bitcoin i.e., cryptocurrency, can use a QR Code (Quick Response Code) to send and/receive crypto payments. Lastly, your AFFIANT knows when a crypto QR code generator is used, the image can be saved in the phone's image gallery.

### **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.

AFFIANT has been involved in investigations and has received training in various types of criminal investigations to include theft by unlawful taking. Through your AFFIANT's training and past experience, your AFFIANT is aware that cellular telephone data can provide valuable insight for theft by unlawful taking 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.

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 10<sup>th</sup> 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 a black Samsung cell phone labeled with Property Report Q2403510 and stored at the Lincoln Police Department Property Division located at 575 S. 10<sup>th</sup> Street, Lincoln, Lancaster County, Nebraska, 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;

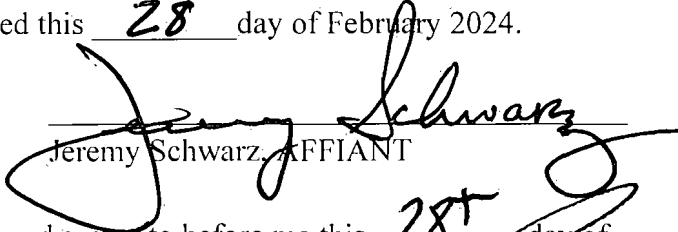
- d) Evidence of use of the device to conduct internet searches relating to above listed crime(s);
- e) Information that can be used to calculate the position of the device between the above dates, including location data; GPS satellite data; GPS coordinates for routes and destination queries between 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 above listed crime(s);
- l) Evidence of purchases, such as items used in planning or carrying out above listed crimes(s);
- m) Internet research history conducted while planning, executing, or covering up to commit above listed crimes(s);

- n) Any live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, account names, usernames, 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.

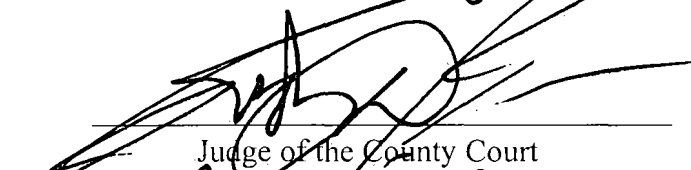
Your AFFIANT would also like to advise the court that the examination of digital devices is a lengthy process requiring special steps to ensure the integrity of the electronic evidence. Therefore, it may not be possible to complete a return for the court within the 10 days normally required by the court

Further AFFIANT saith not;

Dated this 28 day of February 2024.

  
\_\_\_\_\_  
Jeremy Schwarz, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 28<sup>th</sup> day of February 2024.

  
\_\_\_\_\_  
Judge of the County Court  
Rodney D. Reuter  
\_\_\_\_\_  
Printed Name of Judge

