

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

CR24-1

IN THE MATTER OF THE SEARCH)
WARRANT OBTAINED FROM)
APPLE INC., 1 INFINITY LOOP,)
CUPERTINO, CA)

SEARCH
WARRANT RETURN

LANCASTER COUNTY
2024 MAY 16 PM 3:27
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
COUNTY OF LANCASTER)

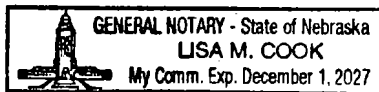
ss.

The undersigned states that he/she received the search warrant issued herein on the 2nd day of May, 2024, and that he/she executed the same on the 10th 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 15 day of May, 2024.


Deputy Colt Lathrop

SUBSCRIBED AND SWORN to before me this 15 day of May, 2024.




Notary Public

C4002884



212



IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

IN THE MATTER OF THE)
SEARCH WARRANT OBTAINED) INVENTORY
FROM APPLE INC., 1 INFINITY)
LOOP, CUPERTINO, CA)

LANCASTER COUNTY
2024 MAY 16 PM 3:27
CLERK OF THE
DISTRICT COURT

STATE OF NEBRASKA)
) ss.
County of Lancaster)

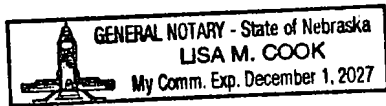
Deputy Colt Lathrop being first duly sworn upon oath, deposes and states the following is an inventory of property seized by virtue of the warrant issued herein:

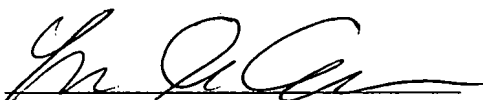
- Complete iCloud Account extraction/download of all data/contents from a black iPhone 14, IMEI #355402932150153, Phone: 17543272385, SIM #: 8901240228193064894 for Juan Carlos Acosta Valdez

DATED this 15 day of May, 2024.


Deputy Colt Lathrop

SUBSCRIBED AND SWORN to before me this 15 day of May, 2024.




Notary Public

C4002884

RECEIPT

The undersigned hereby acknowledges receipt of the following described property seized from the iCloud account attached to a Black Iphone 14, IMEI #355402932150153, Phone: 17543272385, SIM #: 8901240228193064894, for user Juan Carlos Acosta Valdez Lancaster County, Nebraska:

- Complete iCloud Account extraction/download of all data/contents.

LANCASTER COUNTY
2024 MAY 16 PM 3:27
CLERK OF THE
DISTRICT COURT

DATED this 10 day of May 2024


Law Enforcement Officer


WITNESS

account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

All records pertaining to the types of service used;

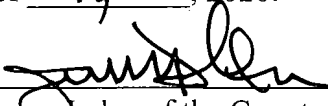
All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

This search warrant shall be executed and returned to a Judge of the County

Court of Lancaster County, Nebraska. It may not be possible to complete a return to the Court within the 10 days normally required by the court.

This Order shall be sealed until otherwise ordered by the Court.

Given under my hand and seal this 2 day of may, ²⁰²⁴2020.



Judge of the County Court





Printed Name of Judge

IN THE COUNTY COURT OF LANCASTER COUNTY, NEBRASKA

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

CLERK OF THE
DISTRICT COURT

LANCASTER COUNTY
2024 MAY 16 PM 3:28

Deputy Lathrop, Colt 902187, being first duly sworn upon oath deposited 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 Theft by Deception - Nebraska Revised Statute 28-512, Theft by Unlawful Taking \$0-\$500 - Nebraska Revised Statute 28-511, and Unauthorized use of a financial transaction device - Nebraska Revised Statute 28-620.

Facts:

On April 17th, 2024 at approximately 1102am CST, I was parked in the turnaround of Nebraska Parkway just east of Rokeby Rd observing westbound Nebraska Parkway traffic when a vehicle pulled up next to me. The driver of the vehicle quickly stated that there was a white Penske rental box truck with a Hispanic male pulled over just east of my location. He stated the vehicle was pulled off near the north side of the ditch of westbound traffic lanes and appeared to be littering. I drove eastbound and passed the Penske truck traveling westbound on Nebraska Parkway. I continued eastbound and found freshly made muddy tracks consistent with a vehicle being recent pulled off the shoulder. I noticed there to be a green box of 'Club' crackers and a large Styrofoam cup in the ditch beside the tracks location. I then proceeded westbound on Nebraska Parkway and locate the same Penske truck pulled now stopped on the shoulder near S 87th/Nebraska Parkway. I initiated a traffic stop of the Penske truck which came to a stop in the north-bound lanes of S 84th St, just south of Eiger Dr. I conducted a traffic stop on a Penske box rental truck (bearing Indiana plate 2830979) for the offense of littering.

I contacted the driver and lone occupant of the Penske truck, who identified himself by his New Mexico driver's license as Juan C Acosta Valdez.

He also provided me with a Penske rental agreement. I identified myself as Deputy Lathrop with the Sheriff's Office and asked why he was littering on the highway. Valdez spoke little English and Google Translate was utilized to communicate. I input in 'Why are you littering on the highway' to which Valdez communicated back in broken English 'My bad' and tried to explain that he stopped on the side to use the restroom and just threw items out. When I asked again why he just didn't keep the trash in his truck, he again replied with 'My bad'. Due to the language barrier, I asked Valdez to exit the vehicle and take a seat in my front passenger seat. Valdez then sat in the front passenger seat of my marked patrol unit 0924.

According to the Penske rental agreement the pick-up date to be April 9th, 2024 with a drop off date of April 10th, 2024. When I pointed out to Valdez he was overdue for the drop off date, he stated his boss 'Frank' had called Penske and made an extension on the rental. This would later be confirmed this with Penske - Fort Myers location who stated the new drop off date was for April 20th, 2024. I also noticed the customer information on the rental agreement was made out to Gonzalez Construction.

While working through Valdez's paperwork and running his license on LPD Channel 16, conversation was made with Valdez about his travels. Valdez claimed to live in New Mexico but was living in Florida for that last 3 months. Valdez stated that he moved to Florida to assist his daughter in moving into her new residence and ended up getting a job from 'Frank'. Valdez stated he left Florida and was coming to Lincoln, NE to pick up vehicle motors and then would turn right back around and head back to Florida. Valdez could not name a business nor give me the address but stated it was written down on paper inside the truck. This address would later be identified as 2414 N St Lincoln Lancaster County Nebraska. A Google search of this address would reveal it to be Lincoln Restaurant Equipment. According to their Facebook page, Lincoln Restaurant Equipment sells new and used restaurant equipment but not vehicle parts.

Valdez claimed to have just left Florida on April 15th, 2024. This would later change to Valdez being in Nebraska since April 15th, 2024. Over the course of speaking with Valdez, his phone continually rang, and Valdez continued to decline the calls. When asked who kept calling him, Valdez stated his boss 'Frank'. When asked why, he stated 'Frank' was just checking up on him. When asked how often 'Frank' calls to check on him, he stated usually at least once in

the morning and once in the afternoon. At this time, LPD Channel 16 would advise that Valdez had an active felony arrest warrant out of Florida.

I then asked if Valdez was aware of his warrant to which he stated no. Valdez made claim that approximately 10 days ago he spoke with his lawyer who spoke with the judge over his case and was granted more time to pay for his fines if he got a job. While discussing his warrant, I observed Valdez to quickly shut his phone off. Valdez was then placed into custody and secured in the rear of my cruiser. A search incident to arrest yielded two wallets were located in Valdez' pockets, spare change, a set Super eight (8) hotel room keys, and various business cards. One wallet contained a Washington state driver's license for David Gonzalez.

When I asked Valdez who Gonzalez was, he stated it was his business partner who was still at the hotel. When I asked which hotel, Gonzalez would originally state something along the lines of 'C' hotel. I believed Valdez to be struggling with English to say Super 8. When I asked if the hotel was in Lincoln, Valdez would originally say yes. Valdez then changed his story to a Hotel 6, about an hour outside of Lincoln. When asked what direction the hotel was from Lincoln, Valdez was unable to answer. A general manager card for 'Jessica' at Super 8 in Percival, IA was located within the wallet with the license belonging to David Gonzalez. I then called the number on the card for Jessica at Super 8. She informed me there was an active room for David Gonzalez that was checked in to on April 15th, 2024, and was due for checkout on April 18th, 2024. Jessica stated she went into the room shortly before and noted no other individuals in the room and only a suitcase and blanket were in the room.

Due to the Penske truck being a rental and Valdez being arrested on an extraditable warrant, the Penske truck was towed by Midwest Towing. An inventory search of the truck revealed numerous pieces of paper of which appeared to be handwritten credit card numbers and receipts from TriMark Foodservice Equipment, Supplies and Design in Omaha, NE. In the storage unit of the box truck, two Polaris VRX iQ+ robotic pool cleaners were located. One box had two receipts attached to it and were identical but separate purchases, as if the transaction was broken into two payments utilizing the same credit card number. These receipts were from Leslie's Cool Springs, TN #939 located at 615 Bakers bridge Ave Ste 170, Franklin, TN 37067. These receipts only showed the last four digits of 9536. A search of all credit cards in Valdez's possession did not

have a matching last four digits to these receipts. Ultimately, Valdez was lodged at the Lancaster County Jail for his Florida extraction warrant and given a written warning for the Littering.

Leslie's would be later contacted and stated the transaction was unusual. The assistant manager Jack, stated a single Hispanic male would come in and make two separate but back to back purchases of these Polaris VRX iQ+. The employee also stated that there was no credit card transaction done but the credit card numbers were manually punched into the computer in order to complete the purchase. This employee also stated it was odd because the Hispanic male stated he would be back to purchase several more items on Monday but never returned.

Due to the circumstance in which the cellular phone was seized in relation to the arrest scene and crime, the statements made by Juan Carlos Acosta Valdez about unusual travel plans and purchase history, statements made by the assistant manager Jack of Leslie's Pro Swimming Equipment about the unusual transaction with manual credit card number inputs for the two Polaris VRX iQ+ pool cleaners, the credit card numbers from the purchase receipts from Leslie's Pro Swimming not matching any credit cards in Valdez's possession, evidence of at least two credit card numbers hand written on separate scratch papers, it is probable the cellular phone was in possession of the person(s) responsible for the Theft by Deception - Nebraska Revised Statute 28-512, Theft by Unlawful Taking \$0-\$500 - Nebraska Revised Statute 28-511, and Unauthorized use of a financial transaction device - Nebraska Revised Statute 28-620; and it is reasonable to believe the device contains information pertinent to this investigation.

Your affiant was granted a cell phone search warrant on April 19th, 2024 and was signed by Judge Dalton at 0842hrs. Lancaster County Sherriff's Office Electronic Evidence Unit were unable to serve said warrant due to the iPhone not being accessible with forensic tools. Your affiant is aware that iPhone users are capable of utilizing an iPhone iCloud backup feature which periodically takes snapshots of phone data and uploads it to iCloud for safe keeping and to restore onto a new device.

Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either

Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including

connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or

controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

Therefore, Apple’s servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple’s services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account’s user or users.

The records which are the subject of this search warrant are material and relevant to a legitimate law enforcement ongoing investigation. Pursuant to Nebraska Revised Statute(s) 86-2,105 to 86-2,108, affiant requests that Apple Inc. shall be ordered NOT to notify any other person of the existence of this search warrant, including the user of the account, or release any information related to this search warrant, as there is reason to believe that notification or other disclosure would impede this ongoing investigation or otherwise cause an adverse result, as defined by law. Specifically, disclosure would likely result in flight

from prosecution, a negative or harmful modification of activities or the activities of those with whom the subject of the investigation communicates and/or associates, the destruction or tampering with evidence; or would otherwise seriously jeopardize the investigation.

The above does constitute grounds of probable cause for the issuance of a search warrant to search Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014, for the following information: Apple Account(s) data associated with Apple ID: iCloud Account data associated with IMEI: 355402932150153, iPhone 14, phone number: 1-754-327-2385, SIM #: 8901240228193064894, for user/owner Juan Carlos Acosta Valdez including:

All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes,

reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

All records pertaining to the types of service used;

All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

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. Apple Inc. will respond to the warrant as soon as possible, according to their legal compliance guide.

WHEREFORE, PREMISES CONSIDERED, Your applicant respectfully requests that an order, consistent with this Application and subsequent technical wording of said Order, be granted and that it be sealed. Pursuant to Nebraska Revised Statute(s) 86-2,105 to 86-2,108, no notice will be given and Apple shall not disclose for a period of 90 days

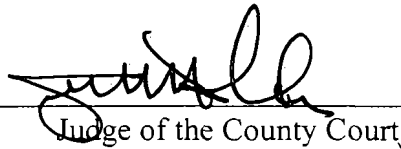
Further AFFIANT saith not;

Dated this 2 day of MAY, ²⁰²⁰2020.

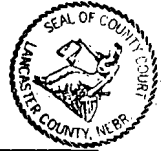


Lathrop, Colt #902187, AFFIANT

SUBSCRIBED to in my presence and sworn to before me this 2 day of may, 2020.



Judge of the County Court



Printed Name of Judge