

IN THE DISTRICT COURT OF THE FOURTH JUDICIAL DISTRICT OF THE STATE OF
OKLAHOMA SITTING IN AND FOR KINGFISHER COUNTY

Kingfisher County Oklahoma
FILED

OCT 28 2023

IN RE: SEARCH WARRANT

CF-2022-72

LISA MARKUS, COURT CLERK
BY  DEPUTY.

**APPLICATION FOR ORDER TO TRANSFER REDACTED SEARCH WARRANTS TO
CRIMINAL FILE**

COMES NOW the State of Oklahoma by and through District Attorney Michael J. Fields and makes application to the Court for an order transferring the **attached redacted** search warrants, affidavits for search warrant, returns of search warrant, and transcripts of oral testimony, if any, from case numbers SW-2023-11, SW-2-23-49, SW-2023-39, SW-2023-10, SW-2023-41, SW-2023-38, and SW-2023-40 to the following criminal case(s):

CF-2022-72 STATE OF OKLAHOMA V. CHEN WU

In support of this application, the State informs the Court that the contents of are evidence in these prosecutions and pursuant to Title 22 O.S. 1224.2 should be transferred, but transferal of the complete, unredacted search warrants, affidavits for search warrants, returns of search warrant, and transcripts of oral testimony, if any, would jeopardize an ongoing criminal investigation.

Dated this 19th day of October, 2023.

MICHAEL J. FIELDS
DISTRICT ATTORNEY

By: 

Austin T. Murrey
Assistant District Attorney

ORDER

NOW on this 19 day of October, 2023, the Court finds for good cause shown, that the State of Oklahoma's Application for Order to Transfer **Redacted** Search Warrant to Criminal File should be granted.

The Court Clerk is directed to file the contents of in each of the cases enumerated above. The Court Clerk is further directed to designate which court case received the original and which cases received copies of the original contents.

The Court Clerk is further directed to file this Order in the Search Warrant file while keeping the unredacted search warrants in the Search Warrant file to establish the redacted nature of the documents transferred to the criminal case(s).

Dated this 19 day of October, 2023.


LANCE SCHNEITER
Judge of the District Court

FILED**APR 19 2023**LISA MARKUS, COURT CLERK
BY Lisa Markus
DEPUTYIN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMAAPPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO VERIZON WIRELESS)
TELEPHONE NUMBER [REDACTED])SW-2022-10³**AFFIDAVIT FOR SEARCH WARRANT**
PURSUANT TO 18 U.S.C. § 2703

NOW COMES The State of Oklahoma, by and through Agent Phillip Ott, an Agent with the Oklahoma State Bureau of Investigation, and being duly sworn and upon Oath, states as follows:

Your Affiant is Phillip Ott, a certified and commissioned police officer in and for the State of Oklahoma, for approximately 17 years, and is currently employed as a Special Agent for the Oklahoma State Bureau of Investigation (OSBI). Your Affiant was previously employed by the Department of Human Services- Office of Inspector General and the Waukomis Police Department. Your Affiant's training and education have included a Bachelor Degree in Criminal Justice from Northwestern Oklahoma State University, OSBI Agent's Academy, Oklahoma Basic Peace Officer Academy and currently has an Advance Certification through the Oklahoma Council of Law Enforcement Education and Training.

Your Affiant, on behalf of the Oklahoma State Bureau of Investigation, respectfully applies to this Court for an Order requiring Cello Partnership dba: Verizon Wireless, located at 180 Washington Valley Road Bedminster, NJ 07921 to furnish to your Affiant the following information concerning telephone number [REDACTED]

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 22, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 22, 2022, at 2359 hours (CST) and to include date,

time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.

3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Verizon Custom Experience (Verizon Selects):** All records associated with the technology known as Verizon Selects, Verizon Custom Experience, and Custom Experience Plus, to include device location information specific to the network, regardless of the device location services settings, as well as device location information specific to Verizon apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate

Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from Verizon applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), to include all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of Verizon telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top level domain and subdomain of the URL) visited, to include a list of all Verizon applications used on the mobile device, and any records related to information about Verizon Fios services. If no records are located associated with Verizon Selects, Verizon Custom Experience and Custom Experience Plus, or Verizon Fios, provide detailed information associated with the subscriber opting out of said services, to include opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.

- h. Activation date and termination date of each device associated with the account and the above-listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

Your Affiant further requests this court to order **Cellco Partnership dba: Verizon Wireless** to provide any technical assistance requested by your Affiant or any other employee of the Oklahoma State Bureau of Investigation.

In support of this warrant, your Affiant respectfully submits to this Court as follows:

1. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
2. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
3. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

Further, your Affiant states, in support of this application and for showing that there is probable cause for the issuance of a search warrant; and in conformity with Title 18 U.S.C. § 2703 (d) of the United States Code, your Affiant makes known to the Court the facts which indicate that the requested records and information are relevant and material to an ongoing criminal investigation.

THAT, cellular telephone providers, such as **Cellco Partnership dba: Verizon Wireless**, is an electronic communication service that maintains records of individuals who are assigned their telephone numbers. These records include telephone number, account number, name of the subscriber, address(s) associated with the account, inception of service, source of payment for service, and associated telephone numbers of the account.

THAT, cellular telephone providers, such as **Cellco Partnership dba: Verizon Wireless**, maintain call detail records, SMS (text message) detail records, and data (internet/application usage, not content, which was routed through a cell tower) records for their telephone numbers. These records include, but not limited to: dates, times, direction and duration of call activity; and the cellular telephone towers, including the locations of said towers, the calls were routed through.

THAT, network-based triangulation is a technique to locate the mobile device using a particular telephone number. The service provider continually measures signal strength and the time it takes for a signal to travel from a mobile device to the cell tower site. The providers also measures the direction from the site in contact with the mobile device. By measuring the signal, the provider can estimate the distance and direction from the mobile device to the cell tower site, and therefore estimate the location of the device. Cellular telephone service providers refer to these differently, depending on the service provider. For example, AT&T refers to this data as NELOS (Network Event Location System); Sprint and US Cellular refers to this data as PCMD (Per Call Measurement Data) data; T-Mobile refers to this data as TDOA (Time Distance of Arrival), and Verizon Wireless refers to this as RTT (Round-Trip Time) data.

THAT, handset-based geolocation is a technique to locate mobile devices. Many mobile devices are equipped with a Global Positioning System (GPS) feature known as Assisted GPS (A-GPS), so that applications, such as Google Maps, can properly work. When the mobile device has contact with the GPS satellite constellation, this information is available to the provider of the mobile device.

PROBABLE CAUSE:

THAT, the statements in this affidavit are based on information obtained during your Affiant's investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant did not include each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed that are necessary to establish probable cause.

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual, later identified as YIFEI LIN with gunshot wounds inside a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QIRONG LIN, HE CHUN CHEN, HE QIANG CHEN, and FANG LEE.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend (FANG LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, AKA: WU CHEN, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was WU, and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YIFEI was able to escape the building and hide. YI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YI was part owner of LIN & CHEN LLC and had previously employed WU. YI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

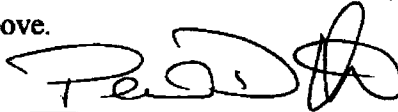
On November 22, 2022, your affiant was notified that CHEN WU AKA: WU CHEN, was located and arrest in Miami Beach, Florida. When WU was arrested, his cell phone was located after he dropped it. A search warrant was later obtained to search WU'S cell phone and Agents were able to determine the phone number to be [REDACTED] during that search.

[REDACTED] WU sent his intended location to individuals while he was traveling to Miami Beach, Florida.

THAT, It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Your Affiant also submits that the disclosure of this Affidavit or the Warrant will cause **CHEN WU, AKA: WU CHEN** or anyone involved in this criminal investigation to potentially flee from prosecution, the destruction of or tampering with evidence, and would seriously jeopardize the above described criminal investigation. Therefore, pursuant to 18 U.S.C. § 2705, your Affiant request that this Court to seal this Affidavit and the Warrant; and order **Cellco Partnership dba: Verizon Wireless** do not disclose the existence of this order to their customer.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search for the items set forth above.



Phillip Ott, Special Agent

Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 19 day of December, 2022.


JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

APR 19 2023

LISA MARKUS, COURT CLERK
BY LISA MARKUS
-DEPUTY

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO VERIZON WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-202³~~2~~-10

SEARCH WARRANT PURSUANT
TO 18 U.S.C. § 2703

In the name of the State of Oklahoma: To any Sheriff, Deputy, Peace Officer, Constable, Marshal, Police Officer, Highway Patrolman, Agent of the Oklahoma State Bureau of Investigation, Agent of the Oklahoma Bureau of Narcotics and Dangerous Drugs, or other law enforcement officer thereof, in the County of Kingfisher, State of Oklahoma:

THIS COURT, having considered the affidavit of Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT for the disclosure of certain records or information pertaining to **Cellco Partnership dba: Verizon Wireless** telephone assigned telephone number [REDACTED] finds as follows:

4. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
5. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
6. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

The Court hereby directs **Cellco Partnership dba: Verizon Wireless**, located at 180 Washington Valley Road Bedminster, NJ 07921 to provide Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT with the following records:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-

referenced number for the period of November 1, 2022, 2400 hours (CST) through November 22, 2022, 2359 hours (CST).

2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 22, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Verizon Custom Experience (Verizon Selects):** All records associated with the technology known as Verizon Selects, Verizon Custom Experience and Custom Experience Plus, to include device location information specific to the network, regardless of the device location services settings, as well as device location

information specific to Verizon apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above referenced number. The responsive data shall also include all numbers listed above, collected from Verizon applications and/or URLs and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), to include all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of Verizon telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top level domain and subdomain of the URL) visited, to include a list of all Verizon applications used on the mobile device, and any records related to information about Verizon Fios services. If no records are located associated with Verizon Selects, Verizon Custom Experience and Custom Experience Plus, or Verizon Fios, provide detailed information associated with the subscriber opting out of said services, to include opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contain the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell-sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.

- c. Credit information obtained or used by the company to grant account status.
- d. All numbers associated with account.
- e. Billing records.
- f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
- g. All Authorized users on the associated account.
- h. Activation date and termination date of each device associated with the account and the above listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

THIS court understands that these technical records can take more than ten days to be compiled and made available pursuant to this Order. You are commanded to make a proper return of the records received, to this Court, when those records are made available to you and you have had time to compile a return as required by law.

IT IS ORDERED that **Celco Partnership dba: Verizon Wireless** provide any technical assistance requested by the Oklahoma State Bureau of Investigation.

IT IS FURTHER ORDERED that **Celco Partnership dba: Verizon Wireless** not disclose to the customer(s) or subscriber(s) the existence of this Order, or the affidavit for this Order, pursuant to 18 U.S.C. § 2705.

DATED THIS 19 DAY OF December, 2022 at 135 am/pm

[Signature]
JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

APR 19 2023

LISA MARKUS, COURT CLERK
BY Lisa Markus
DEPUTY

STATE OF OKLAHOMA)

COUNTY OF KINGFISHER)

SW - 2023-10

OFFICER'S RETURN

I received the above styled warrant of search and seizure to search the following described property, to wit:

Cellco Partnership dba: Verizon Wireless, located at 180 Washington Valley Road Bedminster, NJ 07921 to furnish to your Affiant the following information concerning telephone number [REDACTED]

Your Affiant received this warrant on the 19th day of December 2022, and executed the same on the 23rd day of December 2022, by entering the above-described premises and seizing the following property, all of which was found within these premises, to wit:

Notified on April 4, 2023 that Verizon Wireless would not comply with this warrant. No information was obtained.

I hereby swear that the above inventory contains a true and detailed account of all property taken by me or any Peace Officer aiding or assisting me in the execution of this warrant and hereby make a return to you as directed by law.



Phillip D. Ott, Affiant

Subscribed and Sworn to before me this 19 day of April,
2023


Judge of the District Court

**IN THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT
SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA**

STATE OF OKLAHOMA

)

)

NO. SW-2023-11

COUNTY OF KINGFISHER

)

Kingfisher County Oklahoma

FILED

APR 19 2023

AFFIDAVIT FOR SEARCH WARRANT

LISA MARKUS COURT CLERK
BY Lisa Markus
DEPUTY

The undersigned affiant, being duly sworn, upon oath deposes and says that the following described property:

See Attachment A and Attachment B

Constitutes evidence that an offense was committed and that the person in possession thereof participated in the commission of said offense, to-wit:

Murder 21 O.S. §701-7

This warrant applies to information and data associated with the Apple ID described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), an electronic communications company headquartered at One Apple Park Way, Cupertino, California 95014.

Affiant states that there is probable cause for the issuance of a search warrant because,

I, Phillip Ott, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Apple, Inc. ("Apple"), an electronic communications company headquartered at One Apple Park Way, Cupertino, California 95014. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a),

2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed with the Oklahoma State Bureau of Investigation since May 2022. I am a law enforcement officer as defined at *13 O.S. §176.2 (11)*. I am certified and commissioned through the Oklahoma Council on Law Enforcement Education and Training (CLEET). I have been employed as a full-time peace officer since 2004. During my tenure as a criminal investigator, I have participated as a case agent and support agent in numerous investigations, covering various areas of criminal law. During these investigations, I have participated in interviewing witnesses and sources regarding these various crimes, and I have read official reports of similar interviews by other officers. I have participated in surveillance operations, observing and recording movements of persons involved in criminal activity. I have authored search warrants, seizure warrants, and other court orders in furtherance of criminal investigations. Additionally, I have spoken to other agents who have experience with murder and other violent crimes. As a result, I have learned that people who engage in violent crimes, maintain data and other documentation on their electronic devices for substantial periods of time.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 O.S. §701-7, Murder, committed by CHEN WU, AKA: WU CHEN. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes as further described in Attachment B.

JURISDICTION

3. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants." 18 U.S.C. § 2711(3)(B).

PROBABLE CAUSE

4. The Oklahoma State Bureau of Investigation is investigating WU CHEN for his role in the Murder of FANG HUI LEE, CHUN HE CHEN, QIRONG CHEN, and CHEN HE QIANG. The victims were all workers at a Marijuana Farm near Lacy, Oklahoma.

5. On November 20, 2022, The Kingfisher County Sheriff's Office received a call from YEFEI LIN who attempted to tell them about a hostage situation located at 2372 N. 2760 Rd. Hennessey, Oklahoma. There was a language barrier between the dispatcher and YEFEI. Deputies arrived on the scene to find YEFEI in a black in color F150 suffering from multiple gunshot wounds. A search of the farm located four deceased individuals inside a garage on the property as well as a large amount of marijuana. Kingfisher County Sheriff's Office requested the assistance of the Oklahoma State Bureau of Investigation.
6. Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the farm for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend (FANG HUI LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO, and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.
7. Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information that he lived and worked on the marijuana farm for approximately two years. JINBU had received a phone call from FANG LEE'S brother, SHAN FENG LIN, stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU went in hid on the property. JINBU heard numerous gunshots and he witnessed someone run

out of the garage. JINBU saw WU CHEN, who used to work on the marijuana farm approximately a year prior to the homicide. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. OSBI Agent DEREK WHITE showed JINBU a photograph of WU. JINBU confirmed the person in the picture was WU and the same individual who shot at him.

8. On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YI was able to escape the building and hide. YIFEI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YIFEI was part owner of LIN & CHEN LLC and had previously employed WU. YIFEI described having phone conversations with WU during and after his employment at LIN & CHEN LLC
9. On November 23, 2022, Agents interviewed FANG HUI LEE'S brother, SHAN FENG LIN. LIN provided information that on November 20, 2022, at 1748 hours, he received messages from LEE stating CHEN WU was there with a gun and wanted \$300,000.
10. WU was subsequently arrested in Miami Beach, Florida on November 22, 2022.
11. It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the

Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

12. I am seeking evidence of association. I know that establishing the association of co-conspirators is important in proving a concert of action between multiple persons. In my training and experience some of the best ways of linking co-conspirators together is by searching the calendar, contacts, photo gallery, communications, application data, call logs, and social networking connections. In my training and experience, a comparison of the social media posts of multiple individuals can show an intent to act together and dispel the notion of an accidental meeting. In my training and experience when two or more individuals are in private social media communities together it demonstrates a mutual relationship. In my training and experience associates communicate together via phone calls, text messages and emails, therefore I am seeking the communications evidence to demonstrate the associations of the individuals in this case. In my training and experience a user's "connections," "buddies," and/or "friends," on social networking sites is indicative of who their associates are. Because this evidence is intended to be used to show associations of the user/owner of the device and co-participants, I am seeking the above items regardless of the dates the information was created.
13. I am seeking evidence of communications. In my training and experience, associates communicate together via phone calls, text messages, emails, and social network posts. These communications often contain direct and indirect statements about crimes. Furthermore, I know that communications rarely explicitly mention an intent to commit a crime. Instead, they often allude to intent. In my training and experience individuals often use digital devices and cellular devices to post messages to others on social networking applications. In my

training and experience, it is possible for cellular phone users to use a variety of messaging platforms including SMS, MMS, iChat, WhatsApp, call logs, and others. Therefore, I seek to search all communications of evidence on the device to understand not only what was said, but what was intended and to whom. Therefore, I am seeking all evidence to establish communications between co-conspirators related to the investigation.

INFORMATION CONCERNING APPLE ID AND ICLOUD

1. In my training and experience, I have learned that Apple is a United States company that produces the iPhone, iPad, and iPad Touch, all of which use the iOS operating system, as well as desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of on-line 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:
 - a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
 - b. 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.
 - c. 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.
 - d. 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.

- e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
 - f. 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.
 - g. 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.
 - h. 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.
2. 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.
 3. 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.
 4. 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.

5. 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.
6. In general, an email that is sent to an Apple subscriber is stored in the subscriber's "mail box" on Apple servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Apple servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Apple's servers for a certain period of time.
7. 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.
8. 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.

9. Chat messages may also contain evidence, which can provide a chronological depiction of criminal acts. Specifically, these chat messages can be in the form of SMS text messages, iMessage, or third-party chatting applications such as WeChat. Messages sent in proximate to those from WU could further define the criminal act and identify if others were involved with WU.
10. Other evidence of criminal activity is often found in the form of emails. Correspondence of evidentiary value conducted via e-mail may be with co-conspirators relating to criminal acts, or with innocent third parties in preparation of the criminal activity, such as booking airline tickets, renting a vehicle or reserving a hotel room. In iMessages sent from WU'S phone and subsequent conversations with other co-conspirators. Stored email and chat messages could further define those involved and identify evidence and correspondence related to the matter.
11. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

12. Based on the forgoing, I request that the Court issue the proposed search warrant.
13. **Delayed Notice and Sealing of the Order.** Pursuant to *13 O.S. § 177.4(C)(1) & (2)*, I submit to the Court that based on the information contained in this application, that immediate notice to CHEN WU, AKA: WU CHEN, or anyone associated with the WU, if required, would seriously jeopardize the investigation. Therefore, I request that Apple, Inc. be ordered to not disclose the existence of this search warrant, application, order, or the existence of the investigation to the

listed subscriber, or to any other person, unless or until otherwise ordered by the Court. For that reason, I would further request that this application and the Court's order be sealed until further order of the Court.

14. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

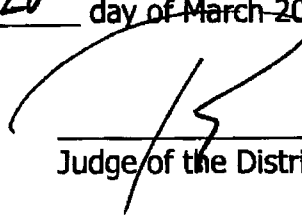
FURTHER YOUR AFFIANT SAYETH NOT.

WHEREFORE, Affiant asks that a search warrant be issued according to law, directed to any OSBI Special Agent, sheriff, policeman, or law enforcement officer in Kingfisher County, Oklahoma, commanding that he search said persons, premises and/or vehicle described and detain the same as provided by law.



Special Agent Phillip Ott
Oklahoma State Bureau of Investigation

Subscribed and sworn to before me this 20th day of ~~March~~ 2023.



Judge of the District Court

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following accounts ("the accounts"):

CHEN WU, AKA: WU CHEN

[REDACTED]

Phone number: [REDACTED]

IMEI: [REDACTED]

Phone Number: [REDACTED]

Email address(es): [REDACTED]

that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Apple, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) and 2703(h)(5)(B), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period starting January 01, 2021 to October 18, 2021.

a. 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);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic

Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. 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;

d. 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;

e. 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;

f. 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, MMS, and WeChat 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);

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

h. All records pertaining to the types of service used; and

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

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of Murder 21 O.S. §701-7, involving CHEN WU, AKA: WU CHEN, since at least January 01, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The identity of the person(s) who created or used the Apple ID, subscriber records, including records that help reveal the historical whereabouts of such person(s);
- (b) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the planning, preparation and actions taken to facilitate human smuggling.
- (c) Communications to, from and between CHEN WU AKA: WU CHEN, along with known and unknown co-conspirators.
- (d) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Oklahoma State Bureau of Investigation may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**IN THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT
SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA**

STATE OF OKLAHOMA

COUNTY OF KINGFISHER

)
)
)

NO. SW-2023-11

SEARCH WARRANT

Kingfisher County Oklahoma

FILED

APR 19 2023

LISA MARKUS, COURT CLERK
BY Lisa Markus
DEPUTY

IN THE NAME OF THE STATE OF OKLAHOMA:

To any OSBI Agent, Sheriff, Policeman or Law Enforcement Officer in Kingfisher County, Oklahoma:

Probable cause having been shown on this date before me, by Special Agent Phillip Ott for believing the following described property:

See Attachment A and Attachment B

The property is located at, and is now being kept, possessed and on the premises, of the above named defendant, and is now located in Kingfisher County, Oklahoma, at, upon or within a certain vehicle, and/or house, building or premises, the curtilage thereof and the appurtenances thereunto, belonging, described as follows:

This warrant applies to Information and data associated with the Apple ID described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), an electronic communications company headquartered at One Apple Park Way, Cupertino, California 95014.

The affidavit being positive that the above described property is on or in the premises described above and there being a likelihood that said property is of important and probative value,

YOU ARE THEREFORE COMMANDED at any time of the day to make a search of said premises for described property and seize the same and safely keep it, and make return hereof within ten days in accordance with the subsequent order of the court, and make a return hereof within ten days.

Further, this Court finds:

1. This Court is a court of competent jurisdiction to issue such orders as defined by Title 18 Section 2711 and Section 3127 of the United States Code, and Title 13 Section 177.1 of the Oklahoma Statutes.

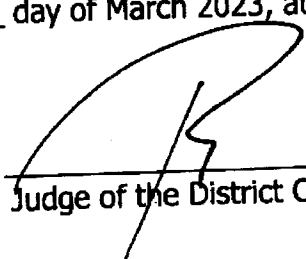
2. As a court of competent jurisdiction, this Court has the authority to order the disclosure of the above Information, pursuant to Title 18 of the United States Code, Section 2703(b) and (d).

ORDER FOR DELAYED NOTICE

3. Pursuant to 13 O.S. § 177.4(C)(1) & (2), the Court finds, based on the information contained in OSBI Special Agent Phillip Ott's application, that immediate notice to Chen Wu AKA: WU CHEN, or his associates, if necessary, would seriously jeopardize the investigation. Therefore, this application and the Court's order shall be sealed pursuant to 13 O.S. § 177.4(C)(1) until further order of the Court. Apple, Inc., its agents and employees shall not disclose to the subscriber or to any other person, the existence of this application or order, or the existence of this investigation or of the devices used to accomplish the aforementioned registering and/or line identification, unless and until otherwise ordered by the Court. *The affidavit and Warrant are sealed until May 1, 2023 unless extended by further order of the court. PKW*

4. Additionally, in accordance with 18 U.S.C. 2703(g), this Court directs Apple, Inc. to execute this warrant without requiring the presence of the Affiant or any officer and deliver the contents of communications, records, or other information as specified in this affidavit to the Affiant by the most expedient and reasonable means.

Whereof Witness My Hand this 20th day of March 2023, at 3:25 am/pm



Judge of the District Court

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following accounts ("the accounts"):

CHEN WU, AKA: WU CHEN

[REDACTED]

Phone number: [REDACTED]

IMEI: [REDACTED]

Phone Number: [REDACTED]

Email address(es): [REDACTED]

that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Apple, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) and 2703(h)(5)(B), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period starting January 01, 2021 to October 18, 2021.

- a. 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);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic

Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. 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;

d. 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;

e. 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;

f. 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, MMS, and WeChat 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);

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

h. All records pertaining to the types of service used; and

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

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of Murder 21 O.S. §701-7, involving CHEN WU, AKA: WU CHEN, since at least January 01, 2022, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The identity of the person(s) who created or used the Apple ID, subscriber records, including records that help reveal the historical whereabouts of such person(s);
- (b) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the planning, preparation and actions taken to facilitate human smuggling.
- (c) Communications to, from and between CHEN WU AKA: WU CHEN, along with known and unknown co-conspirators.
- (d) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Oklahoma State Bureau of Investigation may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

APR 19 2023

LISA MARKUS, COURT CLERK
BY Lisa Markus
DEPUTY

STATE OF OKLAHOMA)

SW - 2023-11

COUNTY OF KINGFISHER)

OFFICER'S RETURN

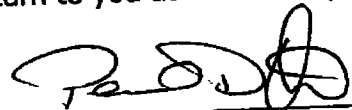
I received the above styled warrant of search and seizure to search the following described property, to wit:

This warrant applies to information and data associated with the Apple ID described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc. ("Apple"), an electronic communications company headquartered at One Apple Park Way, Cupertino, California 95014.

Your Affiant received this warrant on the 20th day of March 2023, and executed the same on the 24th day of March 2023, at approximately 3:46, by entering the above-described premises and seizing the following property, all of which was found within these premises, to wit:

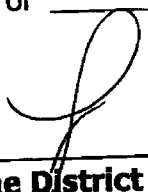
Account Information
Bookmarks
Calendars
Facetime
iCloud Drive
iCloud Log
iMessage Log
Production

I hereby swear that the above inventory contains a true and detailed account of all property taken by me or any Peace Officer aiding or assisting me in the execution of this warrant and hereby make a return to you as directed by law.



Phillip D. Ott, Affiant

Subscribed and Sworn to before me this 19 day of April
2023



Judge of the District Court

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma
FILED

AUG 16 2023

LISA MARKS, COURT CLERK
BY *[Signature]*
DEPUTY

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T-MOBILE WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-38

AFFIDAVIT FOR SEARCH WARRANT
PURSUANT TO 18 U.S.C. § 2703

NOW COMES The State of Oklahoma, by and through Agent Phillip Ott, an Agent with the Oklahoma State Bureau of Investigation, and being duly sworn and upon Oath, states as follows:

Your Affiant is Phillip Ott, a certified and commissioned police officer in and for the State of Oklahoma, for approximately 18 years, and is currently employed as a Special Agent for the Oklahoma State Bureau of Investigation (OSBI). Your Affiant was previously employed by the Department of Human Services- Office of Inspector General and the Waukomis Police Department. Your Affiant's training and education have included a Bachelor Degree in Criminal Justice from Northwestern Oklahoma State University, OSBI Agent's Academy, Oklahoma Basic Peace Officer Academy and currently has an Advance Certification through the Oklahoma Council of Law Enforcement Education and Training.

Your Affiant, on behalf of the Oklahoma State Bureau of Investigation, respectfully applies to this Court for an Order requiring T-Mobile, 4 Sylvan Way, Parsippany, New Jersey 07054 to furnish to your Affiant the following information concerning telephone number [REDACTED]

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up,

- bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
 4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
 5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
 6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive

data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).

- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

Your Affiant further requests this court to order T-Mobile to provide any technical assistance requested by your Affiant or any other employee of the Oklahoma State Bureau of Investigation.

In support of this warrant, your Affiant respectfully submits to this Court as follows:

1. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
2. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
3. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

Further, your Affiant states, in support of this application and for showing that there is probable cause for the issuance of a search warrant; and in conformity with Title 18 U.S.C. § 2703 (d) of the United States Code, your Affiant makes known to the Court the facts which indicate that the requested records and information are relevant and material to an ongoing criminal investigation.

THAT, cellular telephone providers, such as T-Mobile, is an electronic communication service that maintains records of individuals who are assigned their telephone numbers. These records include telephone number, account number, name of the subscriber, address(s) associated with the account, inception of service, source of payment for service, and associated telephone numbers of the account.

THAT, cellular telephone providers, such as T-Mobile, maintain call detail records, SMS (text message) detail records, and data (internet/application usage, not content, which was routed through a cell tower) records for their telephone numbers. These records include, but are not limited to: dates, times, directions, and duration of call activity; and the cellular telephone towers, including the locations of said towers, the calls were routed through.

THAT, network-based triangulation is a technique to locate the mobile device using a particular telephone number. The service provider continually measures signal strength and the time it takes for a signal to travel from a mobile device to the cell tower site. The providers also measure the direction from the site in contact with the mobile device. By measuring the signal, the provider can estimate the distance and direction from the mobile device to the cell tower site, and therefore estimate the location of the device. Cellular telephone service providers refer to these differently, depending on the service provider. For example, AT&T refers to this data as NELOS (Network Event Location System); Sprint and US Cellular refer to this data as PCMD (Per Call Measurement Data) data; T-Mobile refers to this data as TDOA (Time Distance of Arrival), and Verizon Wireless refers to this as RTT (Round-Trip Time) data.

THAT, handset-based geolocation is a technique to locate mobile devices. Many mobile devices are equipped with a Global Positioning System (GPS) feature known as Assisted GPS (A-GPS), so that applications, such as Google Maps, can properly work. When the mobile device has contact with the GPS satellite constellation, this information is available to the provider of the mobile device.

PROBABLE CAUSE:

THAT, the statements in this affidavit are based on information obtained during your Affiant's investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant did not include each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed that are necessary to establish probable cause.

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, at approximately 7:24 p.m. (CST) Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual, later identified as YIFEI LIN with gunshot wounds inside a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QIRONG LIN, HE CHUN CHEN, HE QIANG CHEN, and FANG LEE.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend

(FANG LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO, and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, AKA: WU CHEN, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was WU and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YIFEI was able to escape the building and hide. YIFEI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YIFEI was part owner of LIN & CHEN LLC and had previously employed WU. YIFEI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

On November 22, 2022, your affiant was notified that CHEN WU AKA: WU CHEN, was located and arrested in Miami Beach, Florida. When WU was arrested, his cell phone was located after he dropped it. A search warrant was later obtained to search WU'S cell phone and Agents were able to determine the phone number to be [REDACTED] during that search.

[REDACTED] WU sent his intended location to individuals while he was traveling to Miami Beach, Florida.

[REDACTED]

THAT, It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Your Affiant also submits that the disclosure of this Affidavit or the Warrant will cause CHEN WU, AKA: WU CHEN or anyone involved in this criminal investigation to potentially flee from prosecution, the destruction of or tampering with evidence, and would seriously jeopardize the above described criminal investigation. Therefore, pursuant to 18 U.S.C. § 2705, your Affiant request that this Court to seal this Affidavit and the Warrant; and order T-Mobile Wireless do not disclose the existence of this order to their customer.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search for the items set forth above.



Phillip Ott, Special Agent

Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 6 day of July, 2023.


JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

AUG 16 2023

LISA MARKUS, COURT CLERK
BY LISA MARKUS
-SECURITY

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T-MOBILE WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-38

SEARCH WARRANT PURSUANT
TO 18 U.S.C. § 2703

In the name of the State of Oklahoma: To any Sheriff, Deputy, Peace Officer, Constable, Marshal, Police Officer, Highway Patrolman, Agent of the Oklahoma State Bureau of Investigation, Agent of the Oklahoma Bureau of Narcotics and Dangerous Drugs, or other law enforcement officer thereof, in the County of Kingfisher, State of Oklahoma:

THIS COURT, having considered the affidavit of Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT, and in doing so find probable cause for the search and for the disclosure of certain records or information pertaining to and housed by T-Mobile Records for the assigned telephone number [REDACTED] finds as follows:

4. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
5. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
6. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

The Court hereby directs T-Mobile, 4 Sylvan Way, Parsippany, New Jersey 07054 to provide Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT with the following records:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-

referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).

2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time,

direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contain the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell-sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.

- f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
- g. All Authorized users on the associated account.
- h. Activation date and termination date of each device associated with the account and the above listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:
1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

THIS court understands that these technical records can take more than ten days to be compiled and made available pursuant to this Order. You are commanded to make a proper return of the records received, to this Court, when those records are made available to you and you have had time to compile a return as required by law.

IT IS ORDERED that T-Mobile provide any technical assistance requested by the Oklahoma State Bureau of Investigation.

IT IS FURTHER ORDERED that this order and the associated Application be sealed by the Clerk of the District Court and shall be unsealed only upon Order of this Court of competent jurisdiction.

IT IS FURTHER ORDERED that T-Mobile not disclose to the customer(s) or subscriber(s) the existence of this Order, or the affidavit for this Order, pursuant to 18 U.S.C. § 2705.

DATED THIS 6 DAY OF July, 2023 at 225 am/pm

[Signature]
JUDGE OF THE DISTRICT COURT

FILED

AUG 16 2023

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMALISA MARKUS, COURT CLERK
BY LISA MARKUS
DEPUTYAPPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T-MOBILE)
TELEPHONE NUMBER [REDACTED])

SW-2023-38

SEARCH WARRANT RETURNI RECEIVED THE ABOVE STYLED WARRANT OF SEARCH AND SEIZURE TO OBTAIN
THE FOLLOWING:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID

authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.

4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with

T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.


7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
 - j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
 - k. All customer service and account notes.
 - l. Any and all number and/or account number changes prior to and after the cell number was activated.
 - m. Any other records and other evidence relating to phone number [REDACTED]

- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

Your affiant received this warrant on the 6th day of July 2023, and executed the same on the 11th day of July 2023, by serving T-Mobile with a copy of the search warrant. Your affiant received the following information on the 24th day of July 2023, from T-Mobile:

1. Call detail records for telephone number (617) 320-6888 from November 1, 2022, through November 30, 2022.
2. Subscriber information including account numbers, names, addresses, and date of account establishment.

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO YOU AS DIRECTED BY LAW.


Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN TO THIS 16 DAY OF July, 2023


JUDGE OF THE DISTRICT COURT

FILED**AUG 16 2023**LISA MARKUS, COURT CLERK
BY ALISA MARKUS
DEPUTYIN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMAAPPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO AT&T WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-39

AFFIDAVIT FOR SEARCH WARRANT
PURSUANT TO 18 U.S.C. § 2703

NOW COMES The State of Oklahoma, by and through Agent Phillip Ott, an Agent with the Oklahoma State Bureau of Investigation, and being duly sworn and upon Oath, states as follows:

Your Affiant is Phillip Ott, a certified and commissioned police officer in and for the State of Oklahoma, for approximately 18 years, and is currently employed as a Special Agent for the Oklahoma State Bureau of Investigation (OSBI). Your Affiant was previously employed by the Department of Human Services- Office of Inspector General and the Waukomis Police Department. Your Affiant's training and education have included a Bachelor Degree in Criminal Justice from Northwestern Oklahoma State University, OSBI Agent's Academy, Oklahoma Basic Peace Officer Academy and currently has an Advance Certification through the Oklahoma Council of Law Enforcement Education and Training.

Your Affiant, on behalf of the Oklahoma State Bureau of Investigation, respectfully applies to this Court for an Order requiring ATT Wireless, ATT Wireless National Compliance Center, 11760 US Highway 1, Suite 300, North Palm Beach, Florida 33408 to furnish to your Affiant the following information concerning telephone number [REDACTED]

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up,

bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.

3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to ATT apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive

data shall also include all numbers listed above, collected from ATT applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of ATT telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about ATT services. If no records are located associated with ATT services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).

- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

Your Affiant further requests this court to order **AT&T Wireless** to provide any technical assistance requested by your Affiant or any other employee of the Oklahoma State Bureau of Investigation.

In support of this warrant, your Affiant respectfully submits to this Court as follows:

1. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
2. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
3. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

Further, your Affiant states, in support of this application and for showing that there is probable cause for the issuance of a search warrant; and in conformity with Title 18 U.S.C. § 2703 (d) of the United States Code, your Affiant makes known to the Court the facts which indicate that the requested records and information are relevant and material to an ongoing criminal investigation.

THAT, cellular telephone providers, such as **AT&T Wireless**, is an electronic communication service that maintains records of individuals who are assigned their telephone numbers. These records include telephone number, account number, name of the subscriber, address(s) associated with the account, inception of service, source of payment for service, and associated telephone numbers of the account.

THAT, cellular telephone providers, such as AT&T Wireless, maintain call detail records, SMS (text message) detail records, and data (internet/application usage, not content, which was routed through a cell tower) records for their telephone numbers. These records include, but are not limited to: dates, times, directions, and duration of call activity; and the cellular telephone towers, including the locations of said towers, the calls were routed through.

THAT, network-based triangulation is a technique to locate the mobile device using a particular telephone number. The service provider continually measures signal strength and the time it takes for a signal to travel from a mobile device to the cell tower site. The providers also measure the direction from the site in contact with the mobile device. By measuring the signal, the provider can estimate the distance and direction from the mobile device to the cell tower site, and therefore estimate the location of the device. Cellular telephone service providers refer to these differently, depending on the service provider. For example, AT&T refers to this data as NELOS (Network Event Location System); Sprint and US Cellular refer to this data as PCMD (Per Call Measurement Data) data; T-Mobile refers to this data as TDOA (Time Distance of Arrival), and Verizon Wireless refers to this as RTT (Round-Trip Time) data.

THAT, handset-based geolocation is a technique to locate mobile devices. Many mobile devices are equipped with a Global Positioning System (GPS) feature known as Assisted GPS (A-GPS), so that applications, such as Google Maps, can properly work. When the mobile device has contact with the GPS satellite constellation, this information is available to the provider of the mobile device.

PROBABLE CAUSE:

THAT, the statements in this affidavit are based on information obtained during your Affiant's investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant did not include each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed that are necessary to establish probable cause.

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, at approximately 7:24 p.m. (CST) Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual, later identified as YIFEI LIN with gunshot wounds inside a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QIRONG LIN, HE CHUN CHEN, HE QIANG CHEN, and FANG LEE.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend

(FANG LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO, and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, AKA: WU CHEN, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was WU and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YIFEI was able to escape the building and hide. YIFEI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YIFEI was part owner of LIN & CHEN LLC and had previously employed WU. YIFEI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

On November 22, 2022, your affiant was notified that CHEN WU AKA: WU CHEN, was located and arrested in Miami Beach, Florida. When WU was arrested, his cell phone was located after he dropped it. A search warrant was later obtained to search WU'S cell phone and Agents were able to determine the phone number to be [REDACTED] during that search.

[REDACTED] WU sent his intended location to individuals while he was traveling to Miami Beach, Florida.

[REDACTED] Your affiant reviewed data associated with the video that was provided from JINBU'S cell phone. The time the video started was at approximately 5:57 p.m. (CST) on November 20, 2022. During the interview with WINBO, he reported that WU had a phone call and became "amped up" prior to the shooting. [REDACTED]

[REDACTED]

THAT, It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Your Affiant also submits that the disclosure of this Affidavit or the Warrant will cause CHEN WU, AKA: WU CHEN or anyone involved in this criminal investigation to potentially flee from prosecution, the destruction of or tampering with evidence, and would seriously jeopardize the above described criminal investigation. Therefore, pursuant to 18 U.S.C. § 2705, your Affiant request that this Court to seal this Affidavit and the Warrant; and order AT&T Wireless do not disclose the existence of this order to their customer.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search for the items set forth above.


Phillip Ott, Special Agent

Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 6 day of July, 2023.


JUDGE OF THE DISTRICT COURT

FILED**AUG 16 2023**LISA MARKUS COURT CLERK
BY LISA MARKUS
DEPUTYIN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMAAPPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO VERIZON WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023- 39

SEARCH WARRANT PURSUANT
TO 18 U.S.C. § 2703

In the name of the State of Oklahoma: To any Sheriff, Deputy, Peace Officer, Constable, Marshal, Police Officer, Highway Patrolman, Agent of the Oklahoma State Bureau of Investigation, Agent of the Oklahoma Bureau of Narcotics and Dangerous Drugs, or other law enforcement officer thereof, in the County of Kingfisher, State of Oklahoma:

THIS COURT, having considered the affidavit of Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT, and in doing so find probable cause for the search and for the disclosure of certain records or information pertaining to and housed by AT&T Wireless Records for the assigned telephone number [REDACTED] finds as follows:

4. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
5. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
6. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

The Court hereby directs ATT Wireless, ATT Wireless National Compliance Center, 11760 US Highway 1, Suite 300, North Palm Beach, Florida 33408 to provide Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT with the following records:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in

relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).

2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to ATT apps when permission has been provided by the subscriber to share such information via the device settings.

Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from ATT applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of ATT telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about ATT services. If no records are located associated with ATT services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contain the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell-sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.

- f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
- g. All Authorized users on the associated account.
- h. Activation date and termination date of each device associated with the account and the above listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

THIS court understands that these technical records can take more than ten days to be compiled and made available pursuant to this Order. You are commanded to make a proper return of the records received, to this Court, when those records are made available to you and you have had time to compile a return as required by law.

IT IS ORDERED that AT&T Wireless provide any technical assistance requested by the Oklahoma State Bureau of Investigation.

IT IS FURTHER ORDERED that this order and the associated Application be sealed by the Clerk of the District Court and shall be unsealed only upon Order of this Court of competent jurisdiction.

IT IS FURTHER ORDERED that AT&T Wireless not disclose to the customer(s) or subscriber(s) the existence of this Order, or the affidavit for this Order, pursuant to 18 U.S.C. § 2705.

DATED THIS 6 DAY OF July, 2023 at 225 am/pm



JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO ATT WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-39

Kingfisher County Oklahoma
FILED

AUG 16 2023

LISA MARKUS COURT CLERK
BY Lisa Markus
DEPUTY

SEARCH WARRANT RETURN

I RECEIVED THE ABOVE STYLED WARRANT OF SEARCH AND SEIZURE TO OBTAIN
THE FOLLOWING:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of **November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST)**.
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from **November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST)** and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID

authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.

4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the **"Time on Tower" and/or Sector**, to include information with the start and end date and time for each time the connection was involved in a **"hand-off"** to another cell-site and/or sector, to include the elapsed time (in seconds) for each **"hand-off"**, that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to ATT apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from ATT applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of ATT telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about ATT services. If no records are located associated with ATT services, provide detailed

information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
 - j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
 - k. All customer service and account notes.
 - l. Any and all number and/or account number changes prior to and after the cell number was activated.
 - m. Any other records and other evidence relating to phone number [REDACTED]

- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

Your affiant received this warrant on the 6th day of July 2023, and executed the same on the 11th day of July 2023, by serving ATT Wireless, ATT Wireless National Compliance Center with a copy of the search warrant. Your affiant received the following information on the 16th day of July 2023, from ATT Wireless:

1. Call detail records for telephone number [REDACTED] from November 1, 2022, through November 30, 2022.
2. Subscriber information including account numbers, names, addresses, and date of account establishment.
3. Location Information for telephone number [REDACTED] from November 1, 2022, through November 30, 2022.
4. Payment Information

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO YOU AS DIRECTED BY LAW.



Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN TO THIS 16 DAY OF August, 2023



JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County, Oklahoma

FILED

AUG 16 2023

LISA MARKUS, COURT CLERK
BY LISA MARKUS
DEPUTY

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO VERIZON WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023- 40

AFFIDAVIT FOR SEARCH WARRANT
PURSUANT TO 18 U.S.C. § 2703

NOW COMES The State of Oklahoma, by and through Agent Phillip Ott, an Agent with the Oklahoma State Bureau of Investigation, and being duly sworn and upon Oath, states as follows:

Your Affiant is Phillip Ott, a certified and commissioned police officer in and for the State of Oklahoma, for approximately 17 years, and is currently employed as a Special Agent for the Oklahoma State Bureau of Investigation (OSBI). Your Affiant was previously employed by the Department of Human Services- Office of Inspector General and the Waukomis Police Department. Your Affiant's training and education have included a Bachelor Degree in Criminal Justice from Northwestern Oklahoma State University, OSBI Agent's Academy, Oklahoma Basic Peace Officer Academy and currently has an Advance Certification through the Oklahoma Council of Law Enforcement Education and Training.

Your Affiant, on behalf of the Oklahoma State Bureau of Investigation, respectfully applies to this Court for an Order requiring Celco Partnership dba: Verizon Wireless, located at 180 Washington Valley Road Bedminster, NJ 07921 to furnish to your Affiant the following information concerning telephone number [REDACTED]

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 22, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 22, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up,

bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.

3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Verizon Custom Experience (Verizon Selects):** All records associated with the technology known as Verizon Selects, Verizon Custom Experience, and Custom Experience Plus, to include device location information specific to the network, regardless of the device location services settings, as well as device location information specific to Verizon apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and

sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from Verizon applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), to include all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of Verizon telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top level domain and subdomain of the URL) visited, to include a list of all Verizon applications used on the mobile device, and any records related to information about Verizon Fios services. If no records are located associated with Verizon Selects, Verizon Custom Experience and Custom Experience Plus, or Verizon Fios, provide detailed information associated with the subscriber opting out of said services, to include opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.

- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

Your Affiant further requests this court to order **Cellco Partnership dba: Verizon Wireless** to provide any technical assistance requested by your Affiant or any other employee of the Oklahoma State Bureau of Investigation.

In support of this warrant, your Affiant respectfully submits to this Court as follows:

1. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
2. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
3. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

Further, your Affiant states, in support of this application and for showing that there is probable cause for the issuance of a search warrant; and in conformity with Title 18 U.S.C. § 2703 (d) of the United States Code, your Affiant makes known to the Court the facts which indicate that the requested records and information are relevant and material to an ongoing criminal investigation.

THAT, cellular telephone providers, such as **Cellco Partnership dba: Verizon Wireless**, is an electronic communication service that maintains records of individuals who are assigned their telephone numbers. These records include telephone number, account number, name of the subscriber, address(s) associated with the account, inception of service, source of payment for service, and associated telephone numbers of the account.

THAT, cellular telephone providers, such as **Cellco Partnership dba: Verizon Wireless**, maintain call detail records, SMS (text message) detail records, and data (internet/application usage, not content, which was routed through a cell tower) records for their telephone numbers. These records include, but not limited to: dates, times, direction and duration of call activity; and the cellular telephone towers, including the locations of said towers, the calls were routed through.

THAT, network-based triangulation is a technique to locate the mobile device using a particular telephone number. The service provider continually measures signal strength and the time it takes for a signal to travel from a mobile device to the cell tower site. The providers also measures the direction from the site in contact with the mobile device. By measuring the signal, the provider can estimate the distance and direction from the mobile device to the cell tower site, and therefore estimate the location of the device. Cellular telephone service providers refer to these differently, depending on the service provider. For example, AT&T refers to this data as NELOS (Network Event Location System); Sprint and US Cellular refers to this data as PCMD (Per Call Measurement Data) data; T-Mobile refers to this data as TDOA (Time Distance of Arrival), and Verizon Wireless refers to this as RTT (Round-Trip Time) data.

THAT, handset-based geolocation is a technique to locate mobile devices. Many mobile devices are equipped with a Global Positioning System (GPS) feature known as Assisted GPS (A-GPS), so that applications, such as Google Maps, can properly work. When the mobile device has contact with the GPS satellite constellation, this information is available to the provider of the mobile device.

PROBABLE CAUSE:

THAT, the statements in this affidavit are based on information obtained during your Affiant's investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant did not include each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed that are necessary to establish probable cause.

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual, later identified as YIFEI LIN with gunshot wounds inside a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QIRONG LIN, HE CHUN CHEN, HE QIANG CHEN, and FANG LEE.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within

the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend (FANG LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, AKA: WU CHEN, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was WU, and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YIFEI was able to escape the building and hide. YI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YI was part owner of LIN & CHEN LLC and had previously employed WU. YI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

On November 22, 2022, your affiant was notified that CHEN WU AKA: WU CHEN, was located and arrest in Miami Beach, Florida. When WU was arrested, his cell phone was located after he dropped it. A search warrant was later obtained to search WU'S cell phone and Agents were able to determine the phone number to be [REDACTED] during that search. [REDACTED]

[REDACTED] WU sent his intended location to individuals while he was traveling to Miami Beach, Florida.

THAT, It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application.

Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Your Affiant also submits that the disclosure of this Affidavit or the Warrant will cause **CHEN WU, AKA: WU CHEN** or anyone involved in this criminal investigation to potentially flee from prosecution, the destruction of or tampering with evidence, and would seriously jeopardize the above described criminal investigation. Therefore, pursuant to 18 U.S.C. § 2705, your Affiant request that this Court to seal this Affidavit and the Warrant; and order **Celco Partnership dba: Verizon Wireless** do not disclose the existence of this order to their customer.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search for the items set forth above.



Phillip Ott, Special Agent

Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 19 day of April, 2023.



JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

AUG 16 2023

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO VERIZON WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-40

LISA MARKUS, COURT CLERK
BY Lisa Markus
DEPUTY

SEARCH WARRANT PURSUANT
TO 18 U.S.C. § 2703

In the name of the State of Oklahoma: To any Sheriff, Deputy, Peace Officer, Constable, Marshal, Police Officer, Highway Patrolman, Agent of the Oklahoma State Bureau of Investigation, Agent of the Oklahoma Bureau of Narcotics and Dangerous Drugs, or other law enforcement officer thereof, in the County of Kingfisher, State of Oklahoma:

THIS COURT, having considered the affidavit of Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT, and in doing so find probable cause for the search and for the disclosure of certain records or information pertaining to and housed by **Cellco Partnership dba: Verizon Wireless** Records for the assigned telephone number [REDACTED] finds as follows:

4. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
5. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
6. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

The Court hereby directs **Cellco Partnership dba: Verizon Wireless**, located at 180 Washington Valley Road Bedminster, NJ 07921 to provide Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT with the following records:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-

referenced number for the period of November 1, 2022, 2400 hours (CST) through November 22, 2022, 2359 hours (CST).

2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 22, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Verizon Custom Experience (Verizon Selects):** All records associated with the technology known as Verizon Selects, Verizon Custom Experience and Custom Experience Plus, to include device location information specific to the network, regardless of the device location services settings, as well as device location information specific to Verizon apps when permission has been provided by the

subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above referenced number. The responsive data shall also include all numbers listed above, collected from Verizon applications and/or URLs and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), to include all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of Verizon telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top level domain and subdomain of the URL) visited, to include a list of all Verizon applications used on the mobile device, and any records related to information about Verizon Fios services. If no records are located associated with Verizon Selects, Verizon Custom Experience and Custom Experience Plus, or Verizon Fios, provide detailed information associated with the subscriber opting out of said services, to include opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contain the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell-sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.

- f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
- g. All Authorized users on the associated account.
- h. Activation date and termination date of each device associated with the account and the above listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

THIS court understands that these technical records can take more than ten days to be compiled and made available pursuant to this Order. You are commanded to make a proper return of the records received, to this Court, when those records are made available to you and you have had time to compile a return as required by law.

IT IS ORDERED that **Cellco Partnership dba: Verizon Wireless** provide any technical assistance requested by the Oklahoma State Bureau of Investigation.

IT IS FURTHER ORDERED that **Cellco Partnership dba: Verizon Wireless** not disclose to the customer(s) or subscriber(s) the existence of this Order, or the affidavit for this Order, pursuant to 18 U.S.C. § 2705.

DATED THIS 19 DAY OF April, 2023 at 1100 (C) am/pm



JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

AUG 16 2023

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO ATT WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW 2023-40

LISA MARKUS COURT CLERK
BY: Lisa Markus
DEPUTY

SEARCH WARRANT RETURN

I RECEIVED THE ABOVE STYLED WARRANT OF SEARCH AND SEIZURE TO OBTAIN
THE FOLLOWING:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of **November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST)**.
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from **November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST)** and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID

authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.

4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to ATT apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from ATT applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of ATT telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about ATT services. If no records are located associated with ATT services, provide detailed

information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

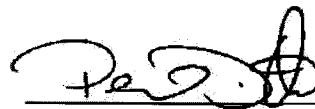
7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
 - j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
 - k. All customer service and account notes.
 - l. Any and all number and/or account number changes prior to and after the cell number was activated.
 - m. Any other records and other evidence relating to phone number [REDACTED]

- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

Your affiant received this warrant on the 19th day of April 2023, and executed the same on the 19th day of April 2023, by serving Celco Partnership dba: Verizon Wireless with a copy of the search warrant. Your affiant received the following information on or about the 15th day of May 2023, from Verizon Wireless:

1. Call detail records for telephone number [REDACTED] from November 1, 2022, through November 22, 2022.
2. Subscriber information including account numbers, names, addresses, and date of account establishment.
3. Location Information for telephone number [REDACTED] from November 1, 2022, through November 22, 2022.
4. Payment Information

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO YOU AS DIRECTED BY LAW.



Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN TO THIS 16 DAY OF June, 2023


JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County Oklahoma

FILED

AUG 16 2023

LISA MARKUS, COURT CLERK
BY: *[Signature]*
DEPUTY

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T-MOBILE WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-41

AFFIDAVIT FOR SEARCH WARRANT
PURSUANT TO 18 U.S.C. § 2703

NOW COMES The State of Oklahoma, by and through Agent Phillip Ott, an Agent with the Oklahoma State Bureau of Investigation, and being duly sworn and upon Oath, states as follows:

Your Affiant is Phillip Ott, a certified and commissioned police officer in and for the State of Oklahoma, for approximately 18 years, and is currently employed as a Special Agent for the Oklahoma State Bureau of Investigation (OSBI). Your Affiant was previously employed by the Department of Human Services- Office of Inspector General and the Waukomis Police Department. Your Affiant's training and education have included a Bachelor Degree in Criminal Justice from Northwestern Oklahoma State University, OSBI Agent's Academy, Oklahoma Basic Peace Officer Academy and currently has an Advance Certification through the Oklahoma Council of Law Enforcement Education and Training.

Your Affiant, on behalf of the Oklahoma State Bureau of Investigation, respectfully applies to this Court for an Order requiring T-Mobile, 4 Sylvan Way, Parsippany, New Jersey 07054 to furnish to your Affiant the following information concerning telephone number [REDACTED]

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up,

bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.

3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive

data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).

- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

Your Affiant further requests this court to order T-Mobile to provide any technical assistance requested by your Affiant or any other employee of the Oklahoma State Bureau of Investigation.

In support of this warrant, your Affiant respectfully submits to this Court as follows:

1. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
2. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
3. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

Further, your Affiant states, in support of this application and for showing that there is probable cause for the issuance of a search warrant; and in conformity with Title 18 U.S.C. § 2703 (d) of the United States Code, your Affiant makes known to the Court the facts which indicate that the requested records and information are relevant and material to an ongoing criminal investigation.

THAT, cellular telephone providers, such as T-Mobile, is an electronic communication service that maintains records of individuals who are assigned their telephone numbers. These records include telephone number, account number, name of the subscriber, address(s) associated with the account, inception of service, source of payment for service, and associated telephone numbers of the account.

THAT, cellular telephone providers, such as **T-Mobile**, maintain call detail records, SMS (text message) detail records, and data (internet/application usage, not content, which was routed through a cell tower) records for their telephone numbers. These records include, but are not limited to: dates, times, directions, and duration of call activity; and the cellular telephone towers, including the locations of said towers, the calls were routed through.

THAT, network-based triangulation is a technique to locate the mobile device using a particular telephone number. The service provider continually measures signal strength and the time it takes for a signal to travel from a mobile device to the cell tower site. The providers also measure the direction from the site in contact with the mobile device. By measuring the signal, the provider can estimate the distance and direction from the mobile device to the cell tower site, and therefore estimate the location of the device. Cellular telephone service providers refer to these differently, depending on the service provider. For example, AT&T refers to this data as NELOS (Network Event Location System); Sprint and US Cellular refer to this data as PCMD (Per Call Measurement Data) data; T-Mobile refers to this data as TDOA (Time Distance of Arrival), and Verizon Wireless refers to this as RTT (Round-Trip Time) data.

THAT, handset-based geolocation is a technique to locate mobile devices. Many mobile devices are equipped with a Global Positioning System (GPS) feature known as Assisted GPS (A-GPS), so that applications, such as Google Maps, can properly work. When the mobile device has contact with the GPS satellite constellation, this information is available to the provider of the mobile device.

PROBABLE CAUSE:

THAT, the statements in this affidavit are based on information obtained during your Affiant's investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant did not include each and every fact known concerning this investigation. Your Affiant has set forth only the facts believed that are necessary to establish probable cause.

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, at approximately 7:24 p.m. (CST) Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual, later identified as YIFEI LIN with gunshot wounds inside a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QIRONG LIN, HE CHUN CHEN, HE QIANG CHEN, and FANG LEE.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend

(FANG LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO, and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, AKA: WU CHEN, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was WU and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YIFEI LIN at OU Hospital in Oklahoma City, Oklahoma. YIFEI provided the following information to Agent VANHOESEN: YIFEI was at the LIN & CHEN LLC. facility when WU walked into a garage where YIFEI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YIFEI attempted to stop WU from hurting anyone else. WU shot YIFEI two different times and YIFEI was able to escape the building and hide. YIFEI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YIFEI was part owner of LIN & CHEN LLC and had previously employed WU. YIFEI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

On November 22, 2022, your affiant was notified that CHEN WU AKA: WU CHEN, was located and arrested in Miami Beach, Florida. When WU was arrested, his cell phone was located after he dropped it. A search warrant was later obtained to search WU'S cell phone and Agents were able to determine the phone number to be [REDACTED] during that search. [REDACTED]

[REDACTED] WU sent his intended location to individuals while he was traveling to Miami Beach, Florida.

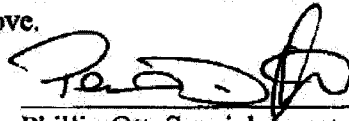
[REDACTED]

[REDACTED]

THAT, It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Your Affiant also submits that the disclosure of this Affidavit or the Warrant will cause CHEN WU, AKA: WU CHEN or anyone involved in this criminal investigation to potentially flee from prosecution, the destruction of or tampering with evidence, and would seriously jeopardize the above described criminal investigation. Therefore, pursuant to 18 U.S.C. § 2705, your Affiant request that this Court to seal this Affidavit and the Warrant; and order T-Mobile Wireless do not disclose the existence of this order to their customer.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search for the items set forth above.


Phillip Ott, Special Agent

Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 6 day of July, 2023.


JUDGE OF THE DISTRICT COURT

Kingfisher County Oklahoma
FILED

AUG 16 2023

LISA MARKUS, COURT CLERK
BY *Lisa Markus*
DEPUTY

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T_MOBILE WIRELESS)
TELEPHONE NUMBER [REDACTED])

SW-2023-41

SEARCH WARRANT PURSUANT
TO 18 U.S.C. § 2703

In the name of the State of Oklahoma: To any Sheriff, Deputy, Peace Officer, Constable, Marshal, Police Officer, Highway Patrolman, Agent of the Oklahoma State Bureau of Investigation, Agent of the Oklahoma Bureau of Narcotics and Dangerous Drugs, or other law enforcement officer thereof, in the County of Kingfisher, State of Oklahoma:

THIS COURT, having considered the affidavit of Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT, and in doing so find probable cause for the search and for the disclosure of certain records or information pertaining to and housed by T-Mobile Records for the assigned telephone number [REDACTED] finds as follows:

4. The Oklahoma State Bureau of Investigation, as an agency of the State of Oklahoma, is a governmental entity pursuant to 18 U.S.C. § 2711 (4).
5. This Court is a Court of competent jurisdiction as defined by Title 18 U.S.C. § 2711 (B) and by Title 13 § 177.1 et seq. of the Oklahoma State Statutes, which has the authority to issue search warrants.
6. As a Court of competent jurisdiction, this Court also has the authority to order the disclosure of the above information, pursuant to Title 22 O.S. § 1222 and Title 18 U.S.C. § 2703; as well as facts set forth in the Affidavit.

The Court hereby directs T-Mobile, 4 Sylvan Way, Parsippany, New Jersey 07054 to provide Oklahoma State Bureau of Investigation Special Agent PHILLIP OTT with the following records:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows

GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST).

2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST) and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.
4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the "Time on Tower" and/or Sector, to include information with the start and end date and time for each time the connection was involved in a "hand-off" to another cell-site and/or sector, to include the elapsed time (in seconds) for each "hand-off", that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has

been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, web site and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contain the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell-sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.

- f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
- g. All Authorized users on the associated account.
- h. Activation date and termination date of each device associated with the account and the above listed number.
- i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
- j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
- k. All customer service and account notes.
- l. Any and all number and/or account number changes prior to and after the cell number was activated.
- m. Any other records and other evidence relating to phone number [REDACTED]
- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

All of which is subject to being lawfully seized for the following criminal act (s), to wit:

1. Murder 1st Degree, Title 21, Ch. 24, Sec. 701.7, Para. A

THIS court understands that these technical records can take more than ten days to be compiled and made available pursuant to this Order. You are commanded to make a proper return of the records received, to this Court, when those records are made available to you and you have had time to compile a return as required by law.

IT IS ORDERED that T-Mobile provide any technical assistance requested by the Oklahoma State Bureau of Investigation.

IT IS FURTHER ORDERED that this order and the associated Application be sealed by the Clerk of the District Court and shall be unsealed only upon Order of this Court of competent jurisdiction.

IT IS FURTHER ORDERED that T-Mobile not disclose to the customer(s) or subscriber(s) the existence of this Order, or the affidavit for this Order, pursuant to 18 U.S.C. § 2705.

DATED THIS 6 DAY OF July, 2023 at 125 am/pm

[Signature]
JUDGE OF THE DISTRICT COURT

IN THE DISTRICT COURT OF KINGFISHER COUNTY
STATE OF OKLAHOMA

Kingfisher County, Oklahoma

FILED

AUG 16 2023

APPLICATION FOR SEARCH WARRANT)
FOR CERTAIN RECORDS OR INFORMATION)
PERTAINING TO T-MOBILE)
TELEPHONE NUMBER [REDACTED])

SW-2023-41

LISA MARKUS, COURT CLERK
BY MISA [Signature]
DEPUTY

SEARCH WARRANT RETURN

I RECEIVED THE ABOVE STYLED WARRANT OF SEARCH AND SEIZURE TO OBTAIN
THE FOLLOWING:

1. **Specialized Location Records:** All call(s), voice, text (SMS & MMS), and data connection location information and transactions (registration of network events), related to all specialized carrier records that may be referred to as LOCDBOR (Location Database of Record), Historical Precision Location Information, Historical Mobile Locate (HML), vMLC (Virtual Mobile Locate - vLMC3, vMLC4, vMLC5), NELOS (Network Event Location System), RTT (Round Trip Time/Return Trip Time/Real Time Tool), PCMD (Per Call Measurement Data), TDOA (Time Difference of Arrival) or Timing Advance Information, Mediation Records, E9-1-1, and/or Historical GPS/Mobile Locate Information which shows GPS location (longitude and latitude) and Cell-Site and sector of the device in relationship to the network when connected to the network for the above-referenced number for the period of **November 1, 2022, 2400 hours (CST) through November 30, 2022, 2359 hours (CST)**.
2. All records associated with the identified mobile number [REDACTED] relating to all delivered and undelivered inbound and outbound calls, text messages SMS & MMS), and text message content to the above-listed number, all voice mail, and all data connections from **November 1, 2022, 2400 hours (CST) through November 30, 2022, at 2359 hours (CST)** and to include date, time, direction, duration, number called or text to and/or received from, bytes up, bytes down, cell-site and sector information related to each call, text, web site and/or application activity (name of web site or application visited and/or accessed) or data connection, all text message content, and voicemails.
3. **FCC TRACED Act STIR/SHAKEN Authentication Standard:** All records associated with the identified mobile number [REDACTED] related to the FCC TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, STIR/SHAKEN caller identification framework, identifying all incoming Voice, Text Message Service (SMS) and Multi-Media Service (MMS) traffic, whether or not the caller ID passed or failed authentication. The report shall include the date, time (with time zone), originating and terminating numbers in their original state prior to Stir/Shaken authentication, the status of whether it passed or failed authentication, the Attestation type, and the originating and terminating verified number that was used to validate Stir/Shaken Caller ID

authentication. The report shall provide all usage events, even if the incoming usage event was blocked and flagged by the service provider (or other third-party entities), prior to delivery to the identified target mobile number.

4. **Time on Tower and/or Sector:** Also provide all cell-site and sector information related to each number called to and/or received from, and data connections, specific to the **"Time on Tower" and/or Sector**, to include information with the start and end date and time for each time the connection was involved in a **"hand-off"** to another cell-site and/or sector, to include the elapsed time (in seconds) for each **"hand-off"**, that was used during and throughout each voice call (whether completed or not), and/or which was used during and throughout each data session.
5. All records associated with the identified mobile number [REDACTED] to include all stored communications or files, including voice mail, text messages (including numbers text to and received from and all related content), e-mail, digital images (e.g. pictures), contact lists, video calling, web activity (name of the web site or application visited or accessed), domain accessed, data connections (to include Internet Service Providers (ISPs), Internet protocol (IP) addresses, IP Session data, IP Destination Data, bookmarks, data sessions, name of web sites and/or applications accessed, date and time when all web sites, applications, and/or third party applications were accessed and the duration of each web site, application, and/or third party application was accessed, and any other files including all cell site and sector information associated with each connection and/or record associated with cell number identified as: [REDACTED]
6. **Custom Experience:** All records associated with device location information specific to the network, regardless of the device location services settings, as well as device location information specific to T-Mobile apps when permission has been provided by the subscriber to share such information via the device settings. Device Location information shall include Cell-site and sector, date, time, direction, duration, number called, or text to and/or received from, and bytes up/down, information related to each call, and text or data connections. The responsive data shall also include all specialized carrier records that may be referred to as RTT (Round Trip Time/Return Trip Time/Real Time Tool), and/or Historical GPS/Mobile Locate Information, which shows GPS location (longitude and latitude) and cell-site and sector of the device in relationship to the network when connected to the network for the above-referenced number. The responsive data shall also include all numbers listed above, collected from T-Mobile applications and/or URLs, and all numbers that communicate with the target number related to the Customer Proprietary Network Information (CPNI), including all delivered and undelivered inbound and outbound calls, text messages, quantity, type, destination, location and amount of use of T-Mobile telecommunications and interconnected voice over internet protocol (VoIP) services and related billing information. All responsive records associated with websites/URLs/domains (top-level domain and subdomain of the URL) visited, include a list of all applications used on the mobile device and any records related to information about T-Mobile services. If no records are located associated with

T-Mobile services, provide detailed information associated with the subscriber opting out of said services, including the opt-out date, time, and associated opt-out IP address.

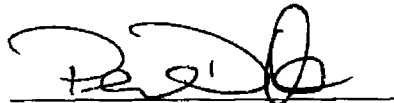
7. Carrier Key related to call detail, text messages, data connections, IP logs, IP Sessions, website and/or application connections, and cell site information. The "carrier key" is a legend related to the types of responsive data received from the service provider, which contains the record column header labels and their definitions of what each cell value represents in the spreadsheet. Carrier keys are required to decipher what the values represent in these cells, as many of these values may be presented in codes only known to the service provider.
8. Content stored in remote storage or 'cloud accounts' associated with the target device including, but not limited to, contacts, call logs, SMS, and MMS messages with associated content including audio, video, and image files, digital images and videos, and files or documents.
9. List of all cell sites as of **November 2022** site lists to include switch, cell-site number, name, physical address, longitude and latitude, all sectors associated with each cell-site, sector beam width, tower height, and azimuth of each sector associated with each cell-site. If multiple technologies (CDMA, UMTS, GSM, LTE etc.) are referenced in the records all appropriate corresponding cell site lists will also be preserved.
10. Subscriber information for the following mobile number [REDACTED]
[REDACTED] including:
 - a. All Subscriber information to include name, tax identification number (social security number or employer identification number).
 - b. Physical address, mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.
 - c. Credit information obtained or used by the company to grant account status.
 - d. All numbers associated with account.
 - e. Billing records.
 - f. All payments to include method, date and time of payments, and location (store name, address, and phone number of location where payment(s) were made).
 - g. All Authorized users on the associated account.
 - h. Activation date and termination date of each device associated with the account and the above-listed number.
 - i. Types of service subscriber utilized (e.g. A-list, AT&T Messages, friends and family).
 - j. Make, model, serial number, IMEI, ESN, MEID, and MAC address associated with the above listed number, including any and all equipment or SIM card changes for the life of the account.
 - k. All customer service and account notes.
 - l. Any and all number and/or account number changes prior to and after the cell number was activated.
 - m. Any other records and other evidence relating to phone number [REDACTED]
[REDACTED]

- n. If any outgoing calls were made to 9-1-1, provide the call details to include date and time, duration, and cell-site and sector information, by querying any other tools (e.g. Sable, ANI/ALI, etc...) necessary to identify the outgoing call(s), whether or not it was the specific carrier network equipment associated with this search warrant, or the 9-1-1 call was carried by a different service provider based on the best signal available from another service provider at the time of the 9-1-1 call.

Your affiant received this warrant on the 6th day of July 2023, and executed the same on the 11th day of July 2023, by serving T-Mobile with a copy of the search warrant. Your affiant received the following information on the 20th day of July 2023, from T-Mobile:

1. No Records provided

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO YOU AS DIRECTED BY LAW.


Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN TO THIS 16 DAY OF July, 2023


JUDGE OF THE DISTRICT COURT

FILED

SEP 13 2023

**THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT
SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA**

ALISA MARKUS, COURT CLERK
[Signature]
 DEPUTY

STATE OF OKLAHOMA)
)
 COUNTY OF KINGFISHER)

SW-2023- 49

AFFIDAVIT FOR SEARCH WARRANT

COMES NOW Phillip Ott, a duly and regularly appointed, qualified, and acting Agent for the Oklahoma State Bureau of Investigation for the State of Oklahoma, who having been first duly sworn upon oath deposes and says:

During your Affiant's employment with the Oklahoma State Bureau of Investigation, and with the Department of Human Services – Office of Inspector General and the Waukomis Police Department, your Affiant has participated in specialized training concerning the investigation of illegal drug offenses, homicides, and frauds. Affiant is an advanced certified Police Officer in the State of Oklahoma is so certified by the Oklahoma Council on Law Enforcement Education and Training for over 18 years; Affiant has attained a Bachelor's Degree in Criminal Justice. Your Affiant has conducted and participated in numerous criminal investigations, these investigations have resulted in the arrest and conviction of individuals involved in the substantive and conspiratorial criminal offenses of murder, shooting with intent to kill, fraud, and other serious felony offenses.


This search warrant is made pursuant to 18 § 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(c)(2) and 22 O.S. §§ 1222 et seq. Your affiant believes probable cause exists for the crime(s) of Murder in the First Degree, 21 O.S. 701.7.

THAT, this Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 USC § 2711. Specifically, a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants, 18 USC § 2711 (3)(B). A District Court of the United States that has jurisdiction over the offenses listed above. 18 USC § 2711 (3)(A)(i).

THAT, Pursuant to 18 USC § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

THAT, California Penal Code 1524.2(4)(c) (2006) states that all California Corporations must honor legal process from foreign states when the foreign states are seeking electronic evidence under terms of the Electronic Communications Privacy Act, 18 USC § 2701 et seq. The affiant has learned that Google, Inc. is a California Corporation subject to the terms of this California Penal Code 1524.2

Your Affiant states that he has reason to believe that housed within the below-listed Google, Inc. Account known as:


located at Google Inc., 1600 Amphitheater Parkway, City of Mountainview, State of California, where there is now being concealed certain property, namely:

1. **Account Information:** User name, primary email address, secondary email addresses, contacted applications and sites, and account activity, including account sign-in locations, browser information, platform information, and Internet protocol (IP) addresses;
2. **Android Information:** Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;
3. **User attribution:** Accounts, email accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voicemail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);
4. **Calendar:** All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;
5. **Contacts:** All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
6. **Documents:** All user created documents stored by Google;
7. **Gmail:** All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the "cc" (carbon copy) or the "bcc" (blind carbon copy), the message content or body, and all attached files;
8. **Google Photos:** All images, graphic files, video files, and other media files stored in the Google Photos service;
9. **Location History:** All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Semantic Location History (SLH) data including activity, start and end location, latitude and longitude for each, duration (epoch time), distance, activity type, confidence level and probability, waypoints including latitude and longitude, places visited including latitude and longitude, place ID, address, name, source info, location confidence, duration, and other candidate locations. Such data shall include the GPS

- coordinates and the dates and times of all location recordings;
10. **Play Store:** All applications downloaded, installed, and/or purchased by the associated account and/or device;
 11. **Search History:** All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;
 12. **Voice:** All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device;
 13. **Google Home (Smart Speaker & Home Assistant):** All information related to Google Home, including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings;
 14. **Android Audio:** All information related to Android Auto including device names, serial numbers and identification numbers, devices, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location data;
 15. **Google Drive or Google One:** All user content stored in Google Drive or Google One including associated metadata.

Based on Affiant's training, experience, and facts tending to establish your Affiant's belief that said items are contained at the said location are as follows:

On November 20, 2022, the Oklahoma State Bureau of Investigation received a request for investigative assistance from the Kingfisher County Sheriff's Office Sheriff DENNIS BANTHER.

On November 20, 2022, Kingfisher County Sheriff's Office responded to a reported hostage situation at the LIN & CHEN LLC. marijuana grow, located at 2372 N 2760 Road near the Town of Hennessey, County of Kingfisher, State of Oklahoma. Upon arrival, Deputies found one individual with gunshot wounds inside of a black in color Ford F150. As Deputies searched the property, they located four deceased individuals in the garage. Three males and one female were later identified as QUIRONG LIN, CHUN CHEN HE, QUIANG CHEN HE, and FANG HUI LEE.

Agents obtained a search warrant for the crime scene and processed the scene for evidence. While processing the scene, OSBI Crime Scene Agent ELI TURLEY collected the above-described cellular telephones from the crime scene in the garage. The above-described phones are believed to have belonged to the deceased victims. The phones were secured and placed into evidence at the OSBI North Central Regional Office, 701 S. Lewis St. Stillwater, Payne County, Oklahoma.

Deputies located three individuals that were present or on the property at the time of the shooting. Agents interviewed WENBO LIN, who provided information he had

been working at the grow for the past ten days. WENBO said on November 20, 2022, WENBO was working in the garage when an unidentified male came into the garage and shot the "Boss" in the leg. The suspect held multiple people inside the garage at gunpoint. The suspect demanded money within the next half hour or he was going to kill everyone in the garage. The "Boss" told his girlfriend (FANG HUI LEE), who was inside the garage to call her brother (SHAN FENG LIN) to get the money. As time went by, the "Boss" was not doing very well and told the suspect to finish him off and the suspect shot the "Boss". Two males inside the garage attempted to rush the suspect and the suspect shot one of the males. The other male ran out of the garage and the suspect chased after the male that ran. The suspect came back into the garage, passed by WENBO and pointed the gun at the female inside the garage. WENBO ran out of the garage and as WENBO was running away, he heard gunshots.

Agents interviewed JINBU LIN who was not inside the garage during the shooting. JINBU provided information, he has lived and worked on this marijuana farm for approximately two years. JINBU received a phone call from the deceased female's little brother (SHAN FENG LIN) stating someone was at the farm to rob them and they had guns. JINBU went to the front of the property to look around. JINBU did not see anyone so he set up his phone to record the garage door. JINBU then went and hid. JINBU heard numerous gunshots and he witnessed someone run out of the garage. JINBU saw CHEN WU, who used to work on the marijuana farm approximately a year prior to this incident. JINBU said WU saw him and started shooting at him. JINBU ran from the property and went to get help. Oklahoma State Bureau of Investigation Special Agent DEREK WHITE showed JINBU a picture of WU. JINBU confirmed the person in the picture was CHEN WU, also known as WU CHEN, and the same individual who shot at him.

On November 22, 2022, Oklahoma State Bureau of Investigation Special Agent CHAD VANHOESEN interviewed YI FEI LIN at OU Hospital in Oklahoma City, Oklahoma. YI provided the following information to Agent VANHOESEN: YI was at the LIN & CHEN LLC. facility when WU walked into a garage where YI and several other victims were working. WU immediately shot the "Boss" in the leg and then shot a dog that was also in the building. WU was demanding money and told everyone they had thirty minutes to get him money or he was killing everyone inside. After 30 minutes to an hour, WU was becoming aggravated and YI attempted to stop WU from hurting anyone else. WU shot YI two different times and YI was able to escape the building and hide. YI heard multiple shots after fleeing the building and presumed WU had killed everyone inside. YI was part owner of LIN & CHEN LLC and had previously employed WU. YI described having phone conversations with WU during and after his employment at LIN & CHEN LLC.

On November 23, 2022, Agents interviewed FANG HUI LEE'S brother, SHAN FENG LIN. LIN provided information that on November 20, 2022, at 1748 hours, he

received messages from LEE stating CHEN WU was there with a gun and wanted \$300,000.

Your affiant conducted a search of WU CHEN'S cellular phone that was found on his person during his arrest, pursuant to a search warrant. Your affiant located information for the Google account under the name of [REDACTED]

Your affiant is aware that Google, Inc., is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, a search engine (Chrome), cloud computing (Drive), software, and hardware. Google, Inc. is considered one of the Big Four technology companies, alongside Amazon, Google, and Microsoft.

Googleplex is Google's corporate headquarters located at 1600 Amphitheater Parkway, Mountain View, California, 94043. Google also maintains data centers (servers) around the world and across the United States including the states of Oregon, Nevada, Oklahoma, Tennessee, Nebraska, South Carolina, North Carolina, Iowa, Georgia, Alabama, Virginia, Ohio, and Texas.

Google offers a large number of products including Gmail, Chrome Web Browser, Waze, YouTube, Chromecast, Google Home, Android, Google Auto, Google Maps, Gmail, photo hosting platforms, and many others. Google collects a tremendous amount of user data from user web activity, application activity, location history, device information, and search history. In addition to information Google obtains from a user using their services, Google collects data on a user from other companies doing business on the internet. They amalgamate user data in order to sell advertising aimed at the specific user and improve the user experience.

Google identifies accounts in a variety of ways, primarily by a user-created Gmail account. However, Google also associates user accounts but the telephone number, or IMEI (International Mobile Equipment Identity) number of an Android device. Basic subscriber-related data Google Stores about users include subscriber name, gender, date of birth, email address(es), telephone number(s), websites visited web searches, searches made on Google, preferences, YouTube video search history, and recently watched videos, and location history.

Use location data is collected and stored by Google. Google uses preparatory advanced location recognition technology in order to routinely calculated a user's location. Android phones, which operate using Google's services, and Pixel Google's own phone devices, track and record a user's location through several means, including Wi-Fi, GPS, Bluetooth, and cellar networks. Similar data is collected about Google device users who are running Google apps.

When a user connects and navigates the Word Wide Web using their connected

device via the Internet (connected infrastructure), the user leaves an Internet Protocol (IP) address that identifies the account user associated by an account and Internet Service Provider (ISP). An IP address, together with the date and time of a communication is unique to each communication. IP addresses are assigned to Internet Service Providers who in turn assign specific addresses to individual users. In some cases, IP addresses are shared with many users. In such situations, users are assigned a Port number that, combined with the IP address and time and date of use, can uniquely identify the user.

Internet Service Providers and others who are assigned ranges of IP addresses typically maintain a record of their sub-assignment of individual IP addresses to individual users. When such records are maintained it is possible to identify the specific date and time, and the specific physical computer and location from which the communication is transmitted.

Other more specific types of information collected and stored by Google include the following:

1. **Account Information:** Username, primary email address, secondary email addresses, connected applications and sites, and account activity, including account sign-in locations, browser information, platform information, and internet protocol (IP) addresses.

Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account as a password login, and account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

2. **Android Information:** Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device.

Google Stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account

and/or known device(s).

3. **User attribution data:** Accounts, emails accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voicemail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).

I know that Google may not verify the true identity of an account creator, account user, or any other person who accesses a user's account using login credentials. For these reasons, it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons, it may be necessary to search and analyze data from when the Google account was initially created to the most current activity.

4. **Calendar:** All calendar feature that allows users to schedule identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees.

Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third-party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. I believe this information will identify dates and appointments relevant to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence.

5. **Contacts:** all contacts stored by Google including name, all contact phone numbers, emails, social network links, and images.

When a user links the Android device or iPhone to their Google account, the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process is continuously updated so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. I believe this information is pertinent to the investigation as it will assist with identifying previously unknown co-conspirators and/or witnesses. Doc (Documents)- All Google documents

including by way of example and not limitation, Docs (a web-based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web-based presentation program). Documents will include all files whether created, shared, or downloaded.

6. **Documents:** All user-created documents stored by Google. Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. I believe this information may contain notes, files, and/or spreadsheets containing information relevant to this investigation including recordation of sales, communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation.
7. **Gmail:** All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the "cc" (carbon copy) or the "bcc" (blind carbon copy), the message content or body, and all attached files.

As noted previously, when the user of an Android device first activates the device they are prompted to associate the device with Google mail, commonly referred to as Gmail account. The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account, they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages.

Messages deleted from Gmail are not actually deleted. They are moved to a folder labeled "Trash" and are stored there until the user empties the "trash" file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. I believe these messages would reveal motivations, plans and intentions, associates, and other co-conspirators.

8. **Google Photos:** All images, graphic files, video files, and other media files stored in the Google Photos service.

Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device.

In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. Your affiant believes a review of these images would provide evidence depicting the suspect, his/her associates, and others performing incriminating acts, and victims. I also believe these image files may assist investigators in determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation.

9. **Location History:** All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Semantic Location History (SLH) data including activity, start and end location, latitude, and longitude for each, duration (epoch time), distance, activity type, confidence level, and probability, waypoints including latitude and longitude, places visited including latitude and longitude, place ID, address, name, source info, location confidence, duration, and other candidate locations. Such data shall include the GPS coordinates and the dates and times of all location recordings.

Google collects and retains location data from Android enables mobile devices. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from Global Positioning Systems (GPS), cell site and cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text message, internet access, or email access.

Your affiant is aware Google Location History may also include a subset of data known as Semantic Location History (SLH). This subset consists of additional contextual information in addition to the date, time, latitude, longitude, uncertainty/display radius, and technology used to find the Location History. Semantic Location History includes the activity type (examples: walking, riding in a vehicle) waypoints, a unique Place ID, physical or street address, location confidence, and other possible location candidates at the same place.

Your affiant believes this data will show the movements of the suspect's mobile device and assist investigators with establishing patterns of movement and identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigations.

10. **Play Store:** All applications downloaded, installed, and/or purchased by the associated account and/or device.

Google operates an inline marketplace whereby Google and other third-party

vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi.

These various applications facilitate communication via voice using voice over Internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service networks there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants.

Furthermore, identifying the user's applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications will assist in locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous-appearing programs, but in reality, are used to conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal.

11. **Search History:** All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance.

Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user-selected results. Furthermore, the specific type of search a user performed into categories differentiates these searches. These categories include a general web search and specialty searches where the results are focused on a particular group such as images, news, videos, and shopping.

Your affiant believes a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it.

12. **Voice:** All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device. Google offers users access to a free voice-over internet protocol (VoIP)

communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user's actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages.

Google Voice also has a voicemail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as any saved voicemail messages and the associated transcriptions.

13. **Google Home (Smart Speaker & Home Assistant):** All information related to Google Home, including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings.

Google Home is a brand of smart speaker development by Google, Inc. Google Home Speakers have microphones that are always listening. It enables users to speak voice commands to interact with services through Google's intelligent personal assistant called Google Assistant. A large number of services, both in-house and third-party, are integrated, allowing users to listen to music, control the playback of videos and photos, and receive news updates entirely by voice. Google Home devices also have integrated support for home automation, letting users control smart home appliances with their voice. Multiple Google Home devices can be placed in different rooms in a home for synchronized connectivity. The data collected by Google Home devices are stored remotely on Google servers.

Users can access their Google Home account and associated data by way of a connected smartphone application or through their Google account. Your affiant believes Google Home data, including the archived audio recordings may be used to refute and corroborate statements, and may be important in identifying potential witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing a timeline and provide context and intent.

14. **Android Audio:** All information related to Android Auto including device names, serial numbers and identification numbers, devices, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location data.

Android Auto is a mobile device application developed by Google that allows

enhanced use of an Android device within a vehicle equipped with a compatible head unit. Once the Android device is connected to the head unit, the system enables it to broadcast applications (apps) with a simple, driver-friendly user interface onto the vehicle's dash display, including GPS mapping/navigation, music playback, text messages (SMS), voice calls, and web search. The system supports both touchscreen and button-controlled head unit displays, although hands-free operation through voice commands is encouraged. Once the user's Android device is connected to the vehicle, the Android mobile device will have access to several of the vehicle's sensors and inputs, such as GPS, steering-wheel-mounted controls (buttons), the sound system, directional microphones, wheel speed, compass, and other vehicle data.

Your affiant believes the Android Auto related data, including the historical geo-location data (GPS, compass, speed, direction) may be important in establishing locations and activities of possible witnesses, victims, co-conspirators, and suspect(s). This information may also be important in establishing the driver and occupants of a particular vehicle, refute and corroborate statements, and can be used to establish a timeline and provide context and intent.

15. **Google Drive or Google One:** All user content stored in Google Drive or Google One including associated metadata. Google Drive is a file storage and synchronization service developed by Google. Google One is a subscription service developed by Google that offers expanded cloud storage and is intended for the consumer market. Every Google Account starts with 15 GB of free storage that is shared across Google Drive, Gmail, and Google Photos. Google One paid plans offer cloud storage starting at 100 GB, up to a maximum of 30 TB.

Google Drive allows users to store files on their servers, synchronize files across devices, and share files. In addition to a website, Google Drive offers apps with offline capabilities for Windows and macOS computers, and Android and iOS smartphones and tablets. Google Drive encompasses Google Docs, Google Sheets, and Google Slides, which are part of an office suite that permits collaborative editing of documents, spreadsheets, presentations, drawings, forms, and more. Files create and edited through the Office suite are saved in Google Drive. Any type of file can be stored and accessed by the user.

Your affiant believes the Google Drive or Google One related data, including the files stored there and the associate metadata maybe important in establishing evidence and knowledge of crimes and may refute and corroborate statements, and may be used to establish a timeline and provide context and intent.

For the reasons outlined above, your affiant believes that probably cause exists to seize and examine the specified records held by Google, Inc. associated with

the listed account.

Your affiant is requesting this search warrant to obtain evidence of the crime of Murder in the First Degree, 21 O.S. 701.7.

It is respectfully requested that this court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Based upon my training and experience, I have learned that criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other criminals as they deem appropriate, e.g., by posting them publicly online through forums. Further information within this application relates to illegal gang activity, which poses a danger to witnesses named within the said application. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. It is requested that these documents be sealed for a period of no less than 90 days from the date of issuance.

WHEREFORE, your Affiant prays that this Honorable Court issue a Warrant authorizing the daytime search of the Google account belong to [REDACTED] located at Google Inc., 1600 Amphitheater Parkway, City of Mountainview, State of California. That this Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 USC § 2711. Specifically, a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants, 18 USC § 2711 (3)(B). A District Court of the United States has jurisdiction over the offenses listed above. 18 USC § 2711 (3)(A)(i).



Phillip Ott, Special Agent
Oklahoma State Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 8 day of August, 2023.



JUDGE OF THE DISTRICT COURT

FILED

SEP 13 2023

**THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT
SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA**

LISA MARKUS, COURT CLERK
[Signature]
 DEPUTY

STATE OF OKLAHOMA)
)
 COUNTY OF KINGFISHER)

SW-2023- 49

SEARCH WARRANT

In the name of the State of Oklahoma:

To any Sheriff, Constable, Marshal, Policeman, OSBI Agent, or other Law Enforcement Officer who is authorized to serve or execute warrants in Kingfisher County, Oklahoma:

Proof by Affidavit having been made before me by Phillip Ott, a duly and regularly appointed, qualified and acting Agent with the Oklahoma State Bureau of Investigation for the State of Oklahoma, that he has reason to believe that housed within the below-listed Google, Inc. Account known as:

[REDACTED]

located at Google Inc., 1600 Amphitheater Parkway, City of Mountainview, State of California, where there is now being concealed certain property, namely:

AND THEREIN SEARCH FOR, SEIZE, SECURE, TABULATE, AT ANYTIME OF DAY BETWEEN THE HOURS OF 6:00 AM AND 10:00 PM AND MAKE RETURNS ACCORDING TO LAW, THE FOLLOWING PROPERTY AND EVIDENCE:

1. **Account Information:** User name, primary email address, secondary email addresses, contacted applications and sites, and account activity, including account sign-in locations, browser information, platform information, and internet protocol (IP) addresses;
2. **Android Information:** Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;
3. **User attribution:** Accounts, email accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voicemail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);

4. **Calendar:** All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;
5. **Contacts:** All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
6. **Documents:** All user created documents stored by Google;
7. **Gmail:** All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the "cc" (carbon copy) or the "bcc" (blind carbon copy), the message content or body, and all attached files;
8. **Google Photos:** All images, graphic files, video files, and other media files stored in the Google Photos service;
9. **Location History:** All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Semantic Location History (SLH) data including activity, start and end location, latitude, and longitude for each, duration (epoch time), distance, activity type, confidence level and probability, waypoints including latitude and longitude, places visited including latitude and longitude, place ID, address, name, source info, location confidence, duration, and other candidate locations. Such data shall include the GPS coordinates and the dates and times of all location recordings;
10. **Play Store:** All applications downloaded, installed, and/or purchased by the associated account and/or device;
11. **Search History:** All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;
12. **Voice:** All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with the target account/device;
13. **Google Home (Smart Speaker & Home Assistant):** All information related to Google Home, including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings;
14. **Android Audio:** All information related to Android Auto including device names, serial numbers and identification numbers, devices, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location data;
15. **Google Drive or Google One:** All user content stored in Google Drive or Google One including associated metadata.

IT IS FURTHER ORDERED that based on the exigency of these circumstances, the search of the property comply as soon as is reasonably possible after receipt of this search

warrant.

IT IS FURTHER ORDERED that this order and the associated Application be sealed by the Clerk of the District Court, and shall be unsealed only upon Order of this Court of competent jurisdiction.

THEREFORE, I am presently satisfied that there is probable cause to believe that the evidence, property, or items so described are presently being concealed in the above-described Google, Inc. Account and that the foregoing grounds for the issuance of this Search Warrant do exist.

YOU ARE FURTHER COMMANDED to search the above-described property for the items so described, serve a copy of the Warrant upon the owner and operator of the property, and make a return of the items seized pursuant to this Warrant within ten (10) days of this date.

Dated this 8 day of August, 2023 at 130 am/pm



JUDGE OF THE DISTRICT

FILED

SEP 13 2023

LISA MARKUS, COURT CLERK

DEPUTY

THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT**SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA**

IN THE MATTER OF THE APPLICATION OF)
 THE OKLAHOMA STATE BUREAU OF)
 INVESTIGATION, A GOVERNMENTAL ENTITY,)
 FOR AN ORDER/SEARCH WARRANT REQUIRING)
 THE DISCLOSURE OF CERTAIN RECORDS OR)
 INFORMATION PERTAINING GOOGLE ACCOUNT)

SW-2023- 49**SEARCH WARRANT RETURN**

I RECEIVED THE ABOVE-STYLED WARRANT OF SEARCH AND SEIZURE TO
 OBTAIN THE FOLLOWING FOR GOOGLE ACCOUNT [REDACTED]

1. Account Information
2. Android Information
3. User Attribution
4. Calendar
5. Contacts
6. Documents
7. Gmail
8. Google Photos
9. Location History
10. Play Store
11. Search History
12. Voice Records
13. Google Home
14. Android Audio
15. Google Drive or Google One

Your affiant received the following information on the 22nd day of August 2023
 from SAMUEL LE CESENE, Support Manager, Kami Vision:

1. Subscriber Information
2. Contact
3. Google Drive
4. Google Chat

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED
 ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR

ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO
YOU AS DIRECTED BY LAW.



Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN ON THIS 13 DAY OF SEPTEMBER 2023.



JUDGE OF THE DISTRICT COURT

THE DISTRICT COURT FOR THE FOURTH JUDICIAL DISTRICT

Kingfisher County Oklahoma

SITTING IN AND FOR KINGFISHER COUNTY, OKLAHOMA

FILED

SEP 25 2023

LISA MARKUS, COURT CLERK
BY LISA MARKUS
DEPUTY

IN THE MATTER OF THE APPLICATION OF)
THE OKLAHOMA STATE BUREAU OF)
INVESTIGATION, A GOVERNMENTAL ENTITY,)
FOR AN ORDER/SEARCH WARRANT REQUIRING)
THE DISCLOSURE OF CERTAIN RECORDS OR)
INFORMATION PERTAINING GOOGLE ACCOUNT)

SW-2023- 49

SEARCH WARRANT RETURN (Amended)

I RECEIVED THE ABOVE-STYLED WARRANT OF SEARCH AND SEIZURE TO
OBTAIN THE FOLLOWING FOR GOOGLE ACCOUNT [REDACTED]


1. Account Information
2. Android Information
3. User Attribution
4. Calendar
5. Contacts
6. Documents
7. Gmail
8. Google Photos
9. Location History
10. Play Store
11. Search History
12. Voice Records
13. Google Home
14. Android Audio
15. Google Drive or Google One

Your affiant received the following information on the 29th day of August 2023,
through the Google Law Enforcement Portal:

1. Subscriber Information
2. Contact
3. Google Drive
4. Google Chat

I HEREBY SWEAR THAT THE ABOVE INVENTORY CONTAINS A TRUE AND DETAILED
ACCOUNT OF ALL PROPERTY TAKEN BY ME OR ANY PEACE OFFICER AIDING OR

ASSISTING ME IN THE EXECUTION OF THIS WARRANT AND HEREBY MAKE RETURN TO
YOU AS DIRECTED BY LAW.


Phillip D. Ott, Affiant

SUBSCRIBED AND SWORN ON THIS 25 DAY OF SEPTEMBER 2023.


JUDGE OF THE DISTRICT COURT