

AUG 14 2023

THE 8TH JUDICIAL DISTRICT OF MARION COUNTY, KANSAS

8:23 AM PM

MN 2023MR65

IN RE: SEARCH WARRANT FOR: the premises commonly known as 117 S 3rd Street, Marion, Marion County, Kansas. The premise is described as a two-story building that has a red brick facade facing street to the east. There are steps going into a glass door area on the north side of the front of the building. Above the glass is a sign that says, "Marion County Record."

APPLICATION FOR SEARCH WARRANT

State of Kansas, Marion County, ss:

Gideon Cody, of lawful age, after first being duly sworn on oath, on information and belief states:

Affiant has probable cause to believe and does believe that an offense against the laws of the State of Kansas, **K.S.A. 21-6107 - Identity theft** and **K.S.A. 21-5839 - Unlawful acts concerning computers**, has been committed and that certain contraband, fruits, instrumentalities, and evidence of such offense are located in or upon the above-described person, place, thing or means of conveyance. Those items are as follows:

1. Forensically process and analyze in a controlled setting all listed electronic media, for the purpose of viewing and or retrieving for evidentiary purposes all data including electronic images, documents and stored electronic communications.
2. Digital communications devices allowing access to the Internet or to cellular digital networks which were or have been used to access the Kansas Department of Revenue records website.
3. Any computer or digital device that has been used to access the Kansas Department of Revenue records website.
4. Documents and records pertaining to Kari Newell
5. Conduct a preview search of all located digital communications devices and digital storage media to exclude from seizure those which have not been involved in the identity theft, by use of manual or automated preview tools.
6. Digital storage media and the digital content which are, or have been, used to store documents and items of personal information as defined by K.S.A. 21-6107.
7. Digital software and application software installation and operation media.

8. Computer software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.
9. If computers or other digital devices are found in a running state, the investigator may acquire evidence from the devices prior to shutting the devices off. This acquisition may take several hours depending on the volume of data. This will include the contents of volatile memory related to computers and other digital communication devices that would tend to show the current and recent use of the computer, use of encryption, use of other communications devices, routes of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details necessary to preserve the true state of running evidence.
10. Manuals and other documents (whether digital or written) which describe operation of items or software seized.
11. Items containing or displaying passwords, access codes, usernames, or other identifiers necessary to examine or operate items, software or information seized.
12. Correspondence or other documents (whether digital or written) pertaining to Kari Newell
13. Items or digital information that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts and cellular digital networks to participate in the identity theft of Kari Newell.
14. Items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements, and other identification documents.
15. Pictures of the exterior and interior of the premises.

That the basis of affiant's probable cause is:

I, Gideon Cody, of lawful age, being first duly sworn on oath, state:

Affiant is the Chief of Police with Marion Kansas Police Department. I began my law enforcement career in June of 1999 and worked as a police officer for the Kansas City Missouri Police Department. I completed the requirements for basic law enforcement training at the Kansas City Missouri Police Department and certified in the State of Missouri as a police officer and currently hold my provisional Law Enforcement certification with the state of Kansas. My law enforcement career included training in judicial custody, juvenile interrogation, crime scene processing and investigation, narcotics investigation, county and municipal offense investigation, interrogation processes, DWI investigation, accident investigation, and fraud and counterfeiting.

As a commander with the Kansas City Missouri Police Department I was in charge of investigations units. I have investigated several cases of identity theft and fraud.

Affiant is assisted in this investigation by Detective Aaron Christner with the Marion County, Kansas Sheriff's Office. Detective Christner was first a patrol deputy starting in February 2019 and worked as a police officer at Anthony, KS Police Department from June 2016 to June 2018. Detective Christner completed the requirements for basic law enforcement training at the Kansas Law Enforcement Training Center (KLETC), September 30, 2016 and is a certified Law Enforcement Officer in the State of Kansas. Detective Christner has attended The Vital Role of Preservation Letters in Investigations training from the National White-Collar Crime Center (NW3C) and Basic Internet Investigations from KLETC. Detective Christner has completed the Obtaining & Understanding Cloud-Based Evidence training at KLETC in June 2022. Detective Christner has also been a co-instructor for the Obtaining & Understanding Cloud-Based Evidence training through KLETC. Detective Christner has also attended the Introduction and Basic Courses for osTriage in 2023. Detective Christner has also completed the FBI First Responder Course as part of the Cyber Investigator Certificate Program in November 2022. While working as a law enforcement officer, Detective Christner is an affiliate with the Internet Crimes Against Children Task Force. As a member of the Task Force Detective Christner conducts investigations involving electronic storage and sharing of child sexual exploitation material via computers, electronic devices and the internet.

During the investigation, your Affiant has learned and been advised of the following:

SEARCH AND SEIZURE

Affiant knows from training and experienced Detectives that searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction, both from external sources and from destructive code imbedded in the system as a "booby trap", the controlled environment of a laboratory is essential to its complete and accurate analysis.

Affiant knows from experienced Detectives that searches and seizures of evidence from computers and other Internet access devices require law enforcement to seize most or all electronic items (hardware, software, passwords, and instructions) to be processed later by a qualified digital evidence expert in a controlled environment. Digital storage media may include but is not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical, solid state or mechanical storage which can be accessed by computers or other electronic devices to store or retrieve data or images, which can store the equivalent of thousands of pages of information. Users may store information in random order with deceptive file names, which requires searching authorities to

examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.

Affiant knows from experienced Detectives that computers and other digital communications devices contain volatile memory that contains information only while the device is in a powered on and/or running state. Your affiant knows that powering off the device may result in the loss of the volatile information. Your affiant also knows that adding an external evidence storage device will cause minor changes to the state of the computer but will allow for the best effort in fully capturing the state of the running evidence. Your affiant knows that this capture of information requires technical expertise to ensure the resulting data can be examined by all subsequent investigators. Your affiant knows that this captured information may include current and recent use of the computer, use of encryption, use of other communications devices, routers of Internet and other digital communications traffic and passwords, encryption keys or other dynamic details relevant to use the system.

Affiant knows from training and experienced Detectives that when entering businesses, that it is common to find multiple devices capable of accessing or storing evidence. It is common to encounter devices which may be used by persons other than the person(s) suspected of identity theft. Due to the large number of devices that may be on the premise, your affiant knows that law enforcement officers can conduct a preview of these devices on scene. This preview can be conducted in a manner which preserves the integrity of the device and its digital information. This preview can be conducted either manually or by use of automated preview tools, such as OS Triage, TUX 4N6 (TUX Forensics) or Internet Evidence Finder. This preview can be accomplished in as little as a few minutes and will allow investigators to release certain items at the scene.

Affiant knows from training and experienced Detectives that in order to fully retrieve data from a computer or other digital communications system the analyst needs all storage media as well as the storage devices. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware access software or drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

Affiant knows from training and experienced Detectives that files related to identity theft on computers and other digital communications devices are usually obtained from the Internet or from cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the method of location or creation of the, search terms used, exchange, transfer, distribution, possession or origin of the files.

Affiant knows from training and experienced Detectives that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

Affiant knows from training and experienced Detectives that computers or other digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the device as well as ownership and use of Internet service accounts used for the Internet or cellular data network access.

Affiant knows from training and experienced Detectives that digital crime scenes usually include items or digital information that would tend to establish ownership or use of digital devices and Internet access equipment and ownership or use of any Internet service or digital cellular service accounts used to participate in identity theft.

Affiant knows from training and experienced Detectives that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

DETAILS OF THE INVESTIGATION:

That since this Affidavit is being submitted for the limited purpose of securing a search warrant; the Affiant has not included each and every fact known concerning this investigation.

On Tuesday August 1, 2023 at or around 1500 hours I attended a meet-and-greet at Kari's Kitchen located at 301 E Santa Fe Marion, Marion County, Kansas 66861. Marion County Record publisher Eric Meyer and reporter Phyllis Zorn were present. I was asked by the owner of the business, Kari Newell, to remove Eric and Phyllis because she did not want them in her establishment. I informed Eric and Phyllis of Kari's wishes and they left.

On Friday August 4, 2023 at or around 1851 hours I received an email from Eric Meyer. In the email he states that he received a copy of someone's private Department of Revenue Records. In the email he alleged possible police misconduct regarding how the Department of Revenue Record was obtained.

After reading the email on Monday August 7, 2023 at or around 0610 hours, I then contacted Marion City Administrator, Brogan Jones, and told him that an internal investigation should be conducted. Brogan stated he was aware of the Department of Revenue Record (DOR record) because City Council member, Ruth Herbel, sent him a screenshot via email of the DOR record belonging to Kari Newell. Ruth states in the email that she received the DOR record from Pam

Maag. Brogan stated Ruth wanted to deny the renewal of Kari's liquor/caterers' license based on the DOR record and that the license was on the City Council Agenda for a meeting the same afternoon. I asked that he forward those emails so that I can continue my investigation.

Later that morning I received the emails, I saw that it contained a screenshot with a DOR record addressed to the victim, Kari Newell. I then contacted Kari, she stated she did not know how someone was able to access her mail and she gave no one permission to obtain, access, or open her private mail.

My investigation revealed the letter was not stolen from her mailbox, rather it was downloaded directly from the Department of Revenue. The Department of Revenue advised the individuals who downloaded the information were Phyllis Zorn and "Kari Newell". Kari's name was listed three minutes after Phyllis Zorn downloaded the information according to the Kansas Department of Revenue. Downloading the document involved either impersonating the victim or lying about the reasons why the record was being sought. Based on the options available on the Kansas DOR records website.

- A. I am requesting my own record.
- B. I have written consent from the individual to whom the requested information pertains, to obtain records on their behalf.
- C. I work for or am acting on the behalf of a government agency and am requesting this information to fulfill the functions of that agency.
- D. I am requesting this information in connection with matters of: motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
- E. I am an employee, agent or contractor of a legitimate business. I am requesting record information in order to verify the accuracy of personal information submitted by the individual in question. If the information I have is incorrect, I am requesting to obtain corrected information. This information will be used to pursue legal remedies against or recover on a debt or security interest against the individual in question.
- F. I am going to use this information in connection with a civil, criminal, administrative, or arbitral proceeding in a Federal, State, or local court or agency or before a self-regulatory body. This may include the service of process, investigation

in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

- G. I am involved in a research project to produce statistical reports. The personal information obtained will not be published, redisclosed or used to contact the individual in question.
- H. I am an agent, employee or contractor for an insurer; an insurance support organization or I am self-insured. The information requested will be used in connection with a claims investigation, antifraud activities, rating or underwriting.
- I. I am requesting record information to provide notice to owners of towed or impounded vehicles.
- J. I work for a licensed private investigative agency or a licensed security service.
- K. I am an employer or an agent or insurer working on the behalf of an employer of licensed commercial drivers. I am requesting records information in order to obtain or verify information relating to a holder of a commercial driver's license.
- L. I am requesting records of individuals who have given the state the express consent to release personal information by "opting in" their records.
- M. I will use the information requested in a manner that is specifically authorized by Kansas law and is related to the operation of a motor vehicle or public safety.

I again contacted the victim, she stated that she did not download or authorize anyone to download any information from the Department of Revenue and someone obviously stole her identity.

On Wednesday August 9, 2023 Kari provided me with a written statement of the events since we last spoke. In the statement she says that on a phone call from 08/07/2023 at or around 1901 hours Eric Meyer admitted to her an employee of his Phyllis Zorn downloaded the private DOR record information and that is why there would be no story. She stated Eric then threatened her "if you pursue anything I will print the story and will continue to use anything I can to come at you. I will own your restaurant".

In the Marion Record Newspaper with a publish date of August 9, 2023, there is an article written by Eric Meyer. The article is titled "Restaurateur accuses paper, councilwoman". In the article Eric Meyer discusses Kari Newell accusing the Marion Record of illegally obtaining her DOR information. Eric Meyer states that the information was provided by a "source" who contacted Marion Record via social media and also sent the information to the council member.

The third paragraph in the article states, "After verifying that the information was accurate and had been obtained, as the source claimed from a public website, the Record decided not to publish it"

While the initial front page of the website is public, as seen above a selection must be made to show a legal reason to obtain the information according to Drivers' Privacy Protection Act of 1994. To access the records a confidentiality agreement is displayed prior to a user accessing the search function. A section of the confidentiality agreement states "Under the Drivers' Privacy Protection Act of 1994, as amended (DPPA) (18 U.S.C. § 2721), personal information obtained by the Kansas Department of Revenue cannot be released unless the request for information falls within one of the exceptions within the Act"

Under the confidentiality agreement it states "By proceeding past this screen, I declare that I am eligible and have the express authority to receive the requested information pursuant to the Federal Drivers' Privacy Protection Act of 1994, as amended. I further declare that any personal information I receive will not be used to sell or offer for sale any property or service."

The Marion County Record is located at 117 S 3rd St, Marion, Marion County, KS according to the contact information on their website.

I believe that certain contraband, fruits, instrumentalities, and evidence of **K.S.A. 21-6107 - Identity theft** and **K.S.A. 21-5839 - Unlawful acts concerning computers**, are located in or upon the above-described person, place, thing or means of conveyance.

FURTHER AFFIANT SAITH NOT

WHEREFORE, Affiant prays that a search warrant be issued, according to law, to search for, apprehend and seize, the above-described items, if any there be, holding them to be dealt with according to law.


Chief Gideon Cody, Affiant

SUBSCRIBED and SWORN to before me this 11th day of August, 2023.


~~Notary~~ Magistrate Vicar