REDACTED COPY

ISP CASE NUMBER 24ISPC011536
SEARCH WARRANT 5

Probable Cause Affidavit
LIST OF PROPERTY, OBJECTS, THINGS, INFORMATION OR PERSONS SEIZED OR PRODUCED AFFIDAVIT

STATE OF INDIANA)		IN THE DUBOIS COUNTY
)	SS:	SUPERIOR COURT
COUNTY OF DUBOIS)		
IN THE MATTER OF)		CAUSE NUMBER:
A REQUEST FOR THE)		**19D01-2410-MC-001192**
ISSUANCE OF A)		
SEARCH WARRANT)		

Lieutenant Jeffrey C. Hearon, of the Indiana State Police Department, swears or affirms that he believes and has probable cause to believe that certain documents and data, hereinafter described is concealed in, or upon, the following described property, to wit:

Dubois County Security Center
255 Brucke Strasse, Jasper, IN 47546

The property or data to be seized or documented, which constitutes unlawfully obtained property, contraband, property used or possessed with the intent to use in the commission or concealment of an offense of official misconduct is described as follows:

1. **Cellphone utilizing the phone number [redacted].**
2. **Desktop and laptop computer utilized by Tom Kleinhelter.**

The cellphone number [redacted] is known to be associated with:

1. **Thomas "Tom" J. Kleinhelter**
   575 N Weisheit Dr, Jasper, IN 47546
   [redacted]
   Gender: Male
   [redacted]

This search warrant authorizes law enforcement officers to seize and conduct a forensic examination analysis on the above-described device(s), including any identity modules and/or removable media contained therein, using forensic methods described in the attached Affidavit, to search for and seize the following:

1. Records of dialed and/or received phone calls, text messages, voicemails, emails, media messages, media searches, video recordings, audio recordings, photographs, contact logs/address book, and other digital evidence located within the devices related to the Dubai trip and commissary expenditures associated with it;

2. Indicia of ownership or use consisting of telephone number, images, nicknames, and other information which will assist law enforcement in establishing the identity of the person or persons who uses, own, rent, lease, or purchased the devices.

The Court specifically grants permission; in order to locate and retrieve the above-described information and data, the forensic examiners and/or law enforcement officers have:

1. Authority to bypass or remove user locks using software or hardware tools, including methods or modifications which may void the device manufacturer's warranty;

2. Authority to, if necessary, perform a chip-off examination of the device;

3. Authority to repair a damaged device if necessary for the examination, including seeking assistance from non-law enforcement officers with experience in device repair; and

4. Authority to seek assistance from another qualified laboratory, including laboratories with forensic experts who are not sworn law enforcement officers.

STATEMENT OF PROBABLE CAUSE

Affiant's Experience:

I, Indiana State Police Lieutenant Jeffrey C. Hearon, being a duly sworn peace officer for the State of Indiana, have been employed by the Indiana State Police for 36 years.

Your affiant, Jeffrey C. Hearon, a law enforcement officer with the Indiana State Police, being duly sworn, swears and affirms under penalties for perjury that the following statements are true and accurate to the best of my knowledge:

I am a police officer with the Indiana State Police. I have been a police officer with the Indiana State Police since 11/13/1988. I am a "law enforcement officer" as that term is defined in Ind. Code 35-31.5-2-185.

I am currently assigned as a Lieutenant to the Area V Field Investigations of the Indiana State Police. In connection with my official duties, I am involved in investigations relating to violations of the Indiana Criminal Code.

I have received training relating to the enforcement of the Indiana Criminal Code, including the following:

A. My initial training at the Indiana Law Enforcement Academy in 1988. I have satisfied the minimum basic training requirements established by rules adopted by the law enforcement training board under I.C. 5-2-1-9 and described in I.C. 35-37-4

B. I have attended numerous additional training courses; see attached transcripts.

As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection.

Investigation:

In support of affiant's assertion of Probable Cause, the following facts are known to affiant, to wit:

During July 2024, the Indiana State Police became aware of the findings of a regularly scheduled audit of Dubois County. According to the findings of the State Board of Accounts, there were purchases from the Jail Commissary fund that did not fall under the County Sheriff's discretionary spending authority set forth at Indiana Code 36-8-10-21. These unallowable expenditures from the fund were approved by County Sheriff, Thomas “Tom” J. Kleinhelter. Indiana State Board of Accounts (SBOA) auditors determined additional procedures were needed to evaluate expenditures from the fund for the duration of Kleinhelter's term beginning January 1, 2019, through December 31, 2023.

As the County Sheriff, Kleinhelter oversaw the Jail Commissary fund established under Indiana Code 36-8-10-21. All monies received from jail commissary sales are to be deposited into the fund's bank account. The statute provides categories of expenses that can be disbursed from the Jail Commissary fund at the Sheriff's discretion. All categories of expenditures listed within the statute are at the discretion of the Sheriff without the need for further appropriation by the county fiscal body. Specifically, Indiana Code 36-8-10-21 states the following:

> ***IC 36-8-10-21 Application to certain counties; jail commissary fund; disposition of money from commissary sales; record of receipts and disbursement:s***
>
> *Sec. 21. (a) This section applies to any county that has a jail commissary that sells merchandise to inmates.*
>
> *(b) A jail commissary fund is established, referred to in this section as "the fund". The fund is separate from the general fund, and money in the fund does not revert to the general fund.*

(c) The sheriff, or the sheriff's designee, shall deposit all money from commissary sales into the fund, which the sheriff or the sheriff's designee shall keep in a depository designated under IC 5-13-8.

(d) The sheriff, or the sheriff's designee, at the sheriff's or the sheriff's designee's discretion and without appropriation by the county fiscal body, may disburse money from the fund for:

(1) merchandise for resale to inmates through the commissary;

(2) expenses of operating the commissary, including, but not limited to, facilities and personnel;

(3) special training in law enforcement for employees of the sheriff's department;

(4) equipment installed in the county jail;

(5) equipment, including vehicles and computers, computer software, communication devices, office machinery and furnishings, cameras and photographic equipment, animals, animal training, holding and feeding equipment and supplies, or attire used by an employee of the sheriff's department in the course of the employee's official duties;

(6) an activity provided to maintain order and discipline among the inmates of the county jail;

(7) an activity or program of the sheriff's department intended to reduce or prevent occurrences of criminal activity, including the following:

(A) Substance abuse.

(B) Child abuse.

(C) Domestic violence.

(D) Drinking and driving.

(E) Juvenile delinquency.

(8) expenses related to the establishment, operation, or maintenance of the sex and violent offender registry web site under IC 36-2-13-5.5; or

(9) any other purpose that benefits the sheriff's department that is mutually agreed upon by the county fiscal body and the county sheriff.

Money disbursed from the fund under this subsection must be supplemental or in addition to, rather than a replacement for, regular appropriations made to carry out the purposes listed in subdivisions (1) through (8).

(e) The sheriff shall maintain a record of the fund's receipts and disbursements. The state board of accounts shall prescribe the form for this record. The sheriff shall

semiannually provide a copy of this record of receipts and disbursements to the county fiscal body. The semiannual reports are due on July 1 and December 31 of each year. Funds misappropriated, diverted or unaccounted for through malfeasance, misfeasance, or nonfeasance in office of any official or employee may be the personal obligation of the responsible official or employee. (Accounting and Uniform Compliance Guidelines Manual for Counties of Indiana, Chapter 1)

As stated above, under Indiana Code 36-8-10-21(d)(9), other expenditures not specifically listed that benefit the Sheriff's Department must be mutually agreed upon by both the Sheriff and the County fiscal body prior to being disbursed.

During their audit, State Board of Accounts investigators located approximately $78,000.00 of questionable expenses. Of those expenses, Kleinhelter was able to provide State Board of Accounts with unverified justifications, for all but $16,774.71 of expenses, of which $8,852.95 of these expenses were attributed to airfare and training conference costs for Kleinhelter's wife, Angela "Angie" Kleinhelter (See itemized table below).

Travel and Conference Expenses Paid With Jail Commissary Funds

Travel Expenses for Angie Kleinhelter	Payee	Payment Method	Purchase Date	Purchase Amount
Registration for the National Sheriff's Association Conference in Phoenix, AZ	Vendor	Check 3702	02-26-21	$ 244.40
Airfare to Panama City, FL for a law enforcement training event	Vendor	Commissary Card [redacted]	05-02-23	887.40
Reimbursement for airfare to Dubai for the World Police Summit	Sheriff	Check 4083	05-16-23	7,373.65
Reimbursement for airfare to Sandestin, FL for a law enforcement training conference	Vendor	Commissary Card [redacted]	10-04-23	347.50
Total				$ 8,852.95

Angie Kleinhelter was not an employee of the County during the time of these expenses. Thus, the expenditures from the Jail Commissary fund for her travel reimbursements and the conference registration fall outside the Sheriff's discretionary spending authority under Indiana Code. Therefore, any expenditure of commissary funds on travel or training conferences for Angie Kleinhelter must have been for the benefit of the Sheriff's Department and approved by the County fiscal body pursuant to Indiana Code 36-8-10-21(d)(9). Sheriff Kleinhelter did not request or obtain approval from the County fiscal body for these expenses regarding his wife.

The remainder of the unjustified expenses were found to have occurred on November 1, 2023, when Kleinhelter purchased four Visa $100.00 prepaid gift cards and fifty Blackstone, 22-inch, flat-top grills for a total of $7,921.76. Kleinhelter took possession of one of the grills, leaving the gift cards and forty-nine grills to be given to employees of the Sheriff's Department as gifts. Purchasing grills and kitchen equipment may be otherwise permissible if the equipment is installed in the jail and used to serve inmates. However, since the expenditures were gifts for

employees and Kleinhelter himself, the purchases did not satisfy the acceptable expenses outlined in Indiana Code. Additionally, these expenses were not approved by the County Council in accordance with Indiana Code 36-8-10-21(d)(9). Following State Board of Accounts inquiries to Kleinhelter and an evaluation of County policies, it was determined there is no gift policy approved by the Board of County Commissioners which would have allowed this expenditure.

The State Board of Accounts determined Kleinhelter was personally responsible for the unjustified expenses and charged with repaying the Jail Commissary fund $16,774.71.

During the week of June 17, 2024, Kleinhelter was notified he was solely responsible for the charges and needed to pay the balance from his own personal funds. Below is an itemization.

1. Airfare for World Police Summit May 5-7, 2024, $8,852.95
2. Four Visa $100.00 prepaid gift cards and fifty Blackstone, 22-inch, flat-top grills for a total of $7,921.76
3. Total reimbursement of $16,774.71

On June 18, 2024, after having been notified he was individually responsible for repaying $16,774.71 to the Jail Commissary fund, Kleinhelter contacted the Dubois County Auditor, Sandy Morton, via email, and requested, “Can you get me a check for $16,774.71 from the Sheriff donation [redacted]?” Kleinhelter instructed Morton, “Just put it into my commissary account.” Morton, responded, “I don’t understand. That money was a donation and can be used for your purposes. Why would we put it in the commissary and not just spend it from the donation fund?” Kleinhelter remained adamant the amount be placed into the commissary fund, stating “Because that is how I want to do it.” After receiving Kleinhelter’s response, Morton contacted the State Board of Accounts field examiners for guidance.

Again, State Board of Accounts informed Kleinhelter he was personally responsible for paying the balance, as airfare and law enforcement conference fees for his wife were not permissible expenses, nor were the purchases of gift cards and flat-top grills for himself and his employees. Again, Kleinhelter expressed understanding and explained he would need to speak with his accountant to arrange for the repayment of funds to the commissary account. Kleinhelter prepared a check, which was photographed and shared with State Board of Accounts. The check was to be deposited the following week, when Kleinhelter returned from a Sheriff’s Conference in Oklahoma.

Later, after Kleinhelter made the appropriate payment, it was discovered Kleinhelter submitted a voucher to receive a reimbursement of $16,774.71 from the Sheriff’s donation fund. This reimbursement was dated July 15, 2024, and included Scott Stockton’s (State Board of Accounts) name, as if the reimbursement had been endorsed by Scott Stockton of the State Board of Accounts (Image of voucher below).

Prescribed by State Board of Accounts

7-15-2024

County Form No. 17 (Rev. 1996)

ACCOUNTS PAYABLE VOUCHER

DUBOIS COUNTY • JASPER, INDIANA

An invoice or bill to be properly itemized must show: kind of service, where performed, dates service rendered, by whom, rates per day, number of hours, rate per hour, number of units, price per unit, etc.

Payee: Tom Kleinhelter

Purchase Order No. 048-01-01-05

Terms

Date Due

Invoice Date	Invoice Number	Description (or note attached invoice(s) or bill(s))	Amount
		reimbursement State Auditor Scott Stockton	$16,774.71
		Total	$16,774.71

I hereby certify that the attached invoice(s), or bill(s), is (are) true and correct and that the materials or services itemized thereon for which charge is made were ordered and received except

Date 7-15- 20 24

Tom J. Kleinhelter
Signature

Sheriff
Title

I hereby certify that the attached invoice(s), or bill(s), is (are) true and correct and I have audited same in accordance with IC 5-11-10-2.

Date _____ 20 ____

County Auditor

Form Prescribed by State Board of Accounts

County Form No. 133 (2001)

Sheriff's Fees Due County

Commissary Sold	$	
Phone Commission	$	
DOC Inmate Refund	$	
Miscellaneous	$ 16,774	71
Total	$ 16,774	71

COMMISSARY CASH RECEIPT

Jasper, Indiana

No. 2408

June 26, 20 24

Cause No.

Acct. No. Tax Warrant No.

Received of Tom Kleinhelter the sum

of Sixteen thousand seven hundred seventy-four and 71/100 Dollars

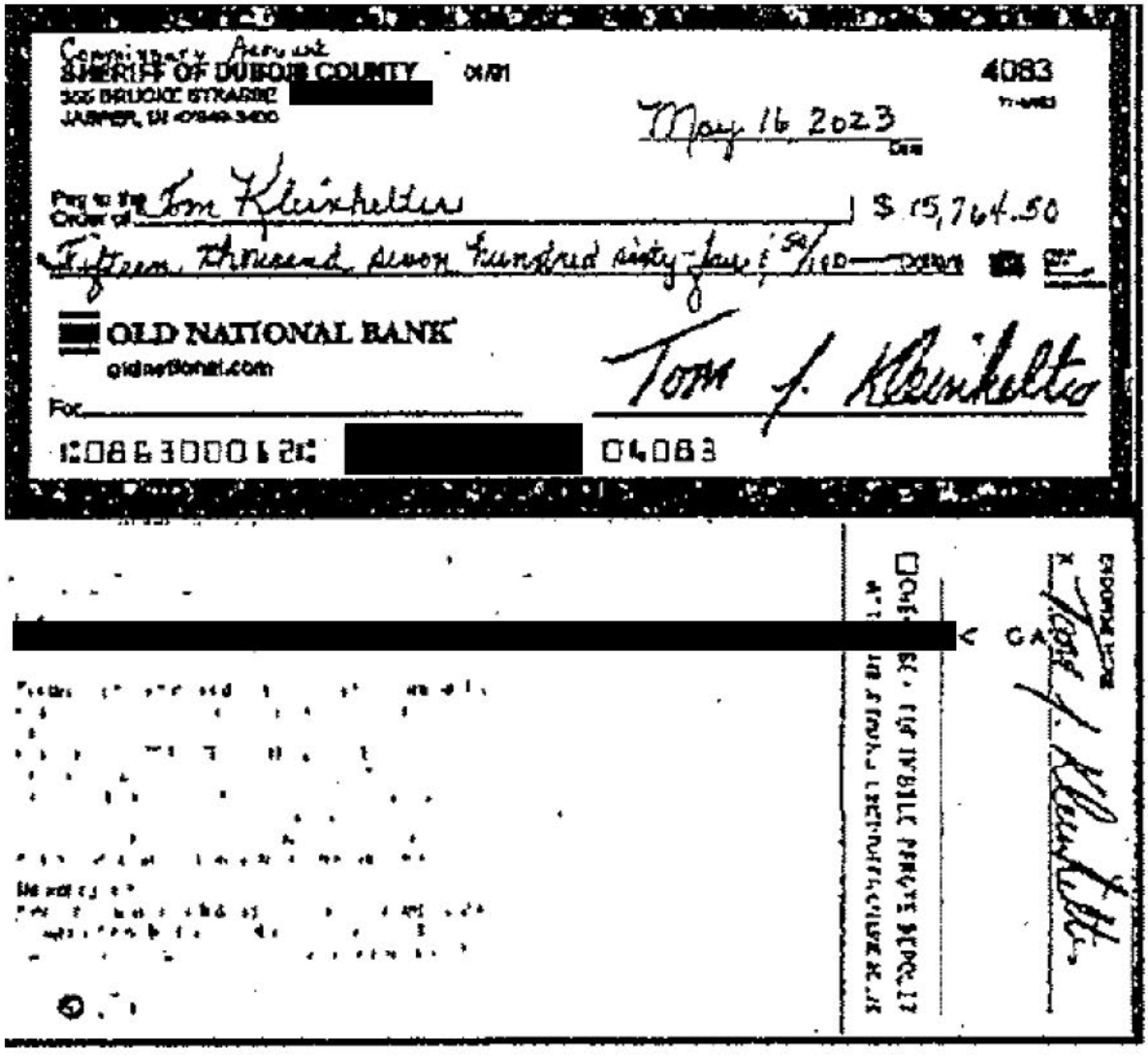
Payment Type ✓ Check / Cash / Money Order

$ 16,774.71

Joann M Schnarr
Sheriff Dubois County

Kleinhelter eventually withdrew this voucher request, which he claimed to have done through a phone call with Ed Wheele (SBOA). However, it was found during the exit conference the voucher request was still standing. Kleinhelter did not formally withdraw the voucher request until it was pointed out during the State Board of Accounts Exit Conference, which was a meeting discussing their findings with the County fiscal body.

Reviewing ledgers for the Commissary fund, check no. 4083 was observed, dated May 16, 2023. This check was endorsed to Tom Kleinhelter for $15,764.50. This check was written the same day Kleinhelter booked the trip for him and his wife for the World Police Summit, scheduled to take place in Dubai during March 2024 (Image of check below).



Review of the records regarding the Dubai trip show Kleinhelter officially booked the flight on May 16, 2023. The Kleinhelters were scheduled to leave Indiana and begin their journey to the United Arab Emirates on February 29, 2024. The Audit conducted by State Board of Accounts did not begin until May 2024. During the audit process, which included discussions and inquiries with State Board of Accounts Investigators Ed Wheele, Scott Stockton, and James Donoho, Kleinhelter failed to tell or correct the impression he had canceled the United Arab Emirates World Police Summit Trip. Kleinhelter did not make any mention of the trip being canceled until he was interviewed by the Indiana State Police on August 29, 2024. The SBOA Audit was completed and published on July 26, 2024. Because Kleinhelter withheld information about the cancelation of the trip, State Board of Accounts only found Kleinhelter liable for repaying costs related to his wife. Had State Board of Accounts known the trip was canceled, Kleinhelter would have been responsible for returning all the county funds used to pay for the trip.

Additionally, if he did cancel the trip, Kleinhelter would have needed to make the cancelation prior to February 2024. This means, at minimum, the trip would have been canceled for at least 4 months, without any repayment of county funds. Kleinhelter did not make any payment until he was directed to do so by State Board of Accounts, which Kleinhelter repeatedly attempted to circumvent.

When Indiana State Police asked Kleinhelter to explain the finances regarding the Dubai trip, he stated the following:

“Um, the Dubai trip did not, did not happen. So, that was on my personal credit card.

*Okay. The commissary paid me part of that, from that. When I canceled the trip**, Delta provided me airline credit instead of cash.***

So, I did not pay it back immediately.

But when I had, when this came through, I immediately moved some money around to, from my financial advisor to get that paid off. And then I also paid my ticket off, that paid for it and the darn hotel room, which I didn't know at the time, but it was a non, um.”

Interviewing officer: It's non-refundable?

*Kleinhelter: **“**Cancelation policy, so I paid that. Um, and that's, that's all been paid back.”*

The Commissary ledgers provided from SBOA to the Indiana State Police fail to show any deposits from Kleinhelter or Delta Airlines for 2023 or 2024. At this point, there is no documentation corroborating Kleinhelter’s claims of the Dubai trip being fully paid back to the Commissary fund, and his explanation of what occurred with the airline credit is left unresolved. Additionally, receipts document Tom and Angela Kleinhelter as having “SkyMiles” accounts registered with Delta Airlines. The “SkyMiles” program is a frequent flyer program with rewards including free upgrades, free travel, free drinks, and other preferred customer benefits. As they

are documented using their “SkyMiles” accounts for their purchases, the Kleinhelters would have reaped additional, personal profits through Delta Airlines (Image of receipt below).

The Delta Airlines receipt also documents Kleinhelter paying for the trip with an American Express credit card ending in [redacted]. The State Board of Accounts audit determined that number belonged to Kleinhelter’s personal credit card. (Image of receipt below).

Date of Purchase: May 16, 2023

Evansville, IN ▸ Dubai, United Arab Emirates

Passenger Information

THOMAS JOSEPH KLEINHELTER
SkyMiles#: [redacted]
ANGELA MARIE KLEINHELTER
SkyMiles#: [redacted]

Confirmation Number: JO7JU2
Ticket Number: 0062109765270
0062109765272

FLIGHT

Date and Flight	Status	Class	Seat/Cabin
EVV ▸ ATL | Thu 29Feb2024 | 9E 4925 |	OPEN	I	
ATL ▸ CDG | Thu 29Feb2024 | AF 8672 |	ARPT	I	
CDG ▸ DXB | Fri 01Mar2024 | AF 8626 |	ARPT	I	
DXB ▸ CDG | Fri 08Mar2024 | AF 8627 |	ARPT	D	
CDG ▸ ATL | Fri 08Mar2024 | DL 83 |	OPEN	D	
ATL ▸ EVV | Fri 08Mar2024 | 9E 5174 |	OPEN	D	

DETAILED CHARGES

Air Transportation Charges	
Base Fare:	$6,000.00 USD
Carrier-imposed International Surcharge (YR):	$1,200.00 USD
Taxes, Fees and Charges	
United Arab Emirates - Passenger Service Charge (AE)	$20.40 USD
United States - September 11th Security Fee(Passenger Civil Aviation Security Service Fee) (AY)	$11.20 USD
F6	$9.50 USD
France - Civil Aviation and Airport Tax (FR)	$11.00 USD
France - Passenger Service Charge (QX)	$44.30 USD
United Arab Emirates - Passenger Security and Safety Fee (TP)	$1.40 USD
United States - Transportation Tax (US)	$42.20 USD
United States - Animal and Plant Health Inspection Service Fee (APHIS User Fee - Passengers (XA)	$3.83 USD
United States - Passenger Facility Charge (XF)	$13.50 USD
United States - Immigration and Naturalization Fee(Immigration User Fee) (XY)	$7.00 USD
United States - Custom User Fee (YC)	$6.52 USD
United Arab Emirates - Advanced Passenger Information Fee (ZR)	$2.80 USD
Total Per Passenger:	**$7,373.65 USD**
Total (2 Passengers)	$14,747.30 USD

Paid with American Express ending [redacted]

A search warrant, granted under cause no. 19D01-2410-MC-001127, gave law enforcement authority to obain records from Delta Airlines regarding Kleinhelter's travel. According to the records, the itenerary for the flights regarding the World Police Summit in Dubai were documented under identifier "JO7JU2." This was the same as the confirmation number provided on the aforementioned receipt (Image above). According to the records, the phone number [redacted], was provided as a contact number. This phone number was known to belong to Tom Kleinhelter, as it is included in the signature line of his emails (Image below).

Tom J. Kleinhelter
Sheriff
Dubois County Sheriff's Office
Phone: [redacted]
Cell: [redacted]
Fax: [redacted]

The phone number [redacted] was also provided as a phone number. Open source information showed this phone number was associated with Angie Kleinhelter. Additionally, the email addresses [redacted] and [redacted] were provided as additional contacts. As changes were made to the itenerary, **such as updates to arrival and departure times, notifications were sent to the Kleinhelter's phone numbers through SMS (text) and both listed email addresses (Image from record below).**

PAX ADVZD AT [redacted]
PAX ADVZD SMS [redacted] - CNS 1026A 23MAR24
PAX ADVZD AT [redacted] - CNS 1026A 23MAR24
DL1836 23MAR24 PUJATL 522P 858P HK*41MIN LATER DEPT
CNS - UNRBK 308P 23MAR24
PAX ADVZD AT [redacted]
PAX ADVZD SMS [redacted] - CNS 308P 23MAR24
PAX ADVZD AT [redacted] - CNS 308P 23MAR24
PAX ADVZD SMS [redacted] - CNS 308P 23MAR24

A review of Delta records revealed Kleinhelter was, in fact, issued refunds from Delta Airlines regarding his purchases related to the World Police Summit in Dubai. The refunds were issued on 01/18/2024. Kleinhelter was issued a total refund of $14,747.30 for his expenses and the expenses of his wife, Angie Kleinhelter. These costs are documented as being refunded to his American Express ending in [redacted] (Images below).

MISCELLANEOUS DOCUMENT - FULL DISPLAY

0060795879235 **JO7JU2/DL** ATLREFR 0066

KLEINHELTER/ANGELA MARIE REFUND DATE

CPN TYPE STATUS **US 18JAN24**

1 EMD EREF

ISSUED FOR REF - REFUND RECEIPT

ENDORSEMENT RESTRICTIONS AGENT ID DL/KS

REFUND TRANSACTION ID: DLM0060795879235

756461/ATLREFR/18JAN24 -

BASE USD

TOTAL TAX USD 1373.65

FEE USD 0.00

TOTAL REFUND AMOUNT USD 7373.65

TAX BREAKDOWN

XF 13.50 AY 11.20 US 42.20 FR 11.00

XA 3.83 YC 6.52 QX 44.30 XY 7.00

YR 1200.00 F6 9.50 ZR 2.80 AE 20.40

TP 1.40

7373.65 USD REFUNDED TO AXXXXXXXXXXXX[redacted]

MISCELLANEOUS DOCUMENT - FULL DISPLAY

0060795593670 **JO7JU2/DL** ATLREFR 0066

KLEINHELTER/THOMAS JOSEPH REFUND DATE

CPN TYPE STATUS US **18JAN24**

1 EMD EREF

ISSUED FOR REF - REFUND RECEIPT

ENDORSEMENT RESTRICTIONS AGENT ID DL/KS

REFUND TRANSACTION ID: DLM0060795593670

756461/ATLREFR/18JAN24 -

BASE USD

TOTAL TAX USD 1373.65

FEE USD 0.00

TOTAL REFUND AMOUNT USD 7373.65

TAX BREAKDOWN

XF 13.50 AY 11.20 US 42.20 FR 11.00

XA 3.83 YC 6.52 QX 44.30 XY 7.00

YR 1200.00 F6 9.50 ZR 2.80 AE 20.40

TP 1.40

7373.65 USD REFUNDED TO AXXXXXXXXXXX[redacted]

The State Board of Accounts audit has shown Kleinhelter to engage in deceitful behavior, such as making false statements, misrepresenting the statements of others, attempting to manipulate others to avoid consequences, and attempting to manipulate others for future benefit. Additionally, the records from Delta Airlines show Kleinhelter lied to Indiana State Police about receiving a refund from Delta Airlines. This information was also withheld from State Board of Accounts. This resulted in Kleinhelter only reimbursing funds for his wife's expenses, rather than his expenses as well. Currently, it appears, Kleinhelter made an inappropriate personal profit of $7,373.65 from the Commissary Fund.

Further review of the records indicate that Delta Airlines recorded the Internet Protocol (IP) address for the device used to book the Dubia trip on May 16, 2023 at 1345 hours Zulu Time. An IP Address is a unique identifing number assigned to every device connected to the internet. The IP number for the Dubia trip was [redacted].

I consulted with the American Registry for Internet Numbers and determined that the IP number listed above is utilized by Perry-Spencer Communication, Inc, 11877 East State Road 62, PO Box 126, St. Meinrad, IN 47577.

DL RLOC JO7JU2
CREATION DATA: 13:45 Z DATE 16 MAY 2023 DUTY CODE GS SIGNATURE WW CITY LAX
AGENT SET: 24D532 SECURITY ID: D006217
THIS PNR: WAS ORIGINATED BY AGENT-SET
PASSENGER NAMES: 01KLEINHELTER/THOMASJOSEP
01KLEINHELTER/ANGELA
PHONE: EVV[redacted]
NO ACTIVE SEGMENTS

TICKETING: TK/TE/0932A/07NOV

	NMNBR NMRMK	NAME W/BLANKS
NAME REMARK	1.01	KLEINHELTER/THOMAS JOSEPH
NAME REMARK	2.01	KLEINHELTER/ANGELA MARIE

REMARKS
-IPAP-[redacted]PDWDC** / 1345Z16MAY23
SCHEDULE CHANGE
DL4925 29FEB24 EVVATL 500P 734P WK*FLIGHT CHANGE
DL5174 8MAR24 ATLEVV 425P 450P WK*FLIGHT CHANGE
MINOR SCHEDULE CHANGE

A search warrant, granted under cause no. 19D01-2410-MC-001184, provided law enforcement the authority to review records from the service provider Perry-Spencer Communications, Incorporated. Regarding the IP Address captured by Delta Airlines when Kleinhelter booked the flight to Dubai.

A review of these records showed the subscriber was "Dubois County Courthouse" with the address of 1 Courthouse Sq, Jasper, IN 47546.

When speaking with a representative of Perry-Spencer Communications, Incorporated, it was explained the county government properties are integrated under the subscriber's name "Dubois County Courthouse." The courts and the jail were specifically provided as examples of separate government properties that operated under this subscriber name. It was further explained that the local business, **Matrix Integration** was responsible for providing IT (Information Technology) services to the government body, known as the "Dubois County Courthouse" subscriber. According to Perry-Spencer Communications, Incorporated, Indiana State Police would need to seek records from Matrix Integration to determine which of the government properties and/or devices under the subscriber's name "Dubois County Courthouse" was associated with the specific records requested.

Detectives traveled to Matrix Intergration 417 Main Street Jasper, Indiana and spoke to Senior Support Engineer Brandon Beadles. Beadles advised IP address [redacted] was consistant with being utilized by the sheriff office. I then spoke to Matrix Senior Systems Engineer Riley Rumfelt and he advised the IP address was consistant with being used by Tom Kleinhelter. He also advised Kleinhelter was issued a county laptop and desktop computer.

To further this investigation, I am requesting the court grant law enforcement authority to seize and search the cellphone, laptop, and desktop computers mentioned above and known to belong/issued to Tom Kleinhelter. A review of these devices would confirm Kleinhelter received correspondence from Delta Airlines regarding booking, changes to the itinerary, cancelation, and refunds.

REGARDING MOBILE DEVICE CAPABILITIES AND COMPONENTS:

The Indiana State Police Computer and Digital Forensics Unit, or other law enforcement agencies with the capability to conduct a forensic examination of a cell phone or other digital device, such as, Indiana National Guard, ATF, HSI, and/or FBI ("Forensic Unit"), who will be doing the forensic examination of any mobile devices in this case, knows the following information:

The following are characteristics of mobile devices:

1. Mobile devices perform an array of functions ranging from a simple telephone device to those of a personal computer. Designed for mobility, they are compact in size, battery-powered, and lightweight. Most mobile devices have a basic set of comparable features and capabilities. They house a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD).

2. Different mobile devices have different technical and physical characteristics (e.g., size, weight, processor speed, memory capacity). Mobile devices may also use different types of expansion capabilities to provide additional functionality. Furthermore, mobile device capabilities sometimes include those of other devices such as handheld Global Positioning Systems (GPS), cameras (photo and video) or personal computers. Overall, mobile devices can be classified as feature phones that are primarily simple voice and messaging communication devices or smartphones that offer more advanced capabilities and services for multimedia, similar to those of a personal computer.

3. Both feature phones and smartphones support voice, text messaging, and a set of basic Personal Information Management (PIM) type applications including phonebook and calendar facilities. Smartphones add PC-like capability for running a wide variety of general and special-purpose applications. Smartphones generally support a wide array of applications, available through an application storefront.

4. A tablet device, commonly referred to as a tablet computer, or more simply, tablet, is a mobile device with a touch screen display that provides many of the same services as mobile smartphones.

5. A GPS navigation device is a mobile device that calculates the device's geographical location by receiving information from GPS satellites.

Identity modules (commonly known as SIM cards) are synonymous with mobile devices that interoperate with GSM cellular networks. A Universal Integrated Circuit Card (UICC), commonly referred to as an identity module (e.g., Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM]), is a removable component that contains essential information about the subscriber. The UICC's main purpose entails authenticating the user of the mobile device to the network providing access to subscribed services. The UICC also offers storage for personal information, such as phonebook entries, text messages, last numbers dialed (LND), and service-related information.

Smartphones may provide an interface that supports removable media (e.g., microSD or MMC), which may contain significant amounts of data. Memory cards are typically flash memory, used as auxiliary user file storage, or as a means to convey files to and from the device.

THE INDIANA STATE POLICE COMPUTER AND DIGITAL FORENSICS UNIT INFORMS THIS COURT THAT:

1. Mobile devices and computer forensics is the science of recovering digital evidence from a mobile/computer device under forensically sound conditions using accepted methods. Mobile/computer device forensics involves validation, preservation, acquisition, examination, analysis, and reporting of digital information.

2. The analysis of evidence from mobile/computer devices requires the digital device to be processed by a qualified expert in a laboratory or other controlled environment. The high volume of the contents and potential concealment of the data through the use of a password, or other challenges in extracting and examining data as described below, combined with the caseload of the examiner, could cause this process to take weeks or months.

3. Recognizing that specialized and highly technical equipment and software will be needed to conduct the analysis of the previously seized device(s) and/or external storage device, the device(s) will be transferred to a Forensic Unit other qualified laboratory with a request that an examination be conducted in this matter. Additionally, under limited circumstances, assistance may be required by the receiving laboratory from other qualified laboratories.

To conduct a forensic analysis on device(s), the Forensic Unit may encounter certain challenges and therefore are requesting specific permission for the following challenges:

1. Acquisition is the process of imaging or otherwise obtaining information from a mobile device/computer and its associated media. Mobile/computer device operating systems consist of open source operating systems as well as closed source operating systems. Closed operating systems make interpreting their associated file system and structure more difficult. Many mobile/computer devices with the same operating system may also vary widely in their implementation, resulting in a myriad of file system and structure permutations. These permutations create significant challenges for mobile/computer forensic tool manufacturers and examiners.

2. For many mobile/computer devices, a forensic examiner is able to use commercial and/or open source forensic tools to acquire data from the device. Depending on the type of device and its operating system, an examiner may use one or more methods of extraction using these forensic tools. These methods vary in the type of data they extract from the device, ranging from recovering only the logical data, to a physical data acquisition, which is a bit-for-bit extraction of all data stored on the device's internal and/or external storage devices.

3. Depending on the device, an examiner may be required to make some changes to the configuration settings of the device to facilitate the acquisition. In some instances, it also may be necessary for software to be loaded onto the device to facilitate the acquisition of the data.

4. Some mobile/computer device manufacturers design devices in a way that prevents the mobile/computer device from communicating with the examiner's forensic workstation, preventing extraction from these devices using the previously described methods. With other devices, a physical acquisition of the phone's entire memory may not be possible using the previously described methods. To extract data from such devices, as well as from devices on which the examiner is unable to bypass a user's lock using the below described methods, or when the device is damaged beyond repair, more advanced methods of extraction may be necessary, including chip-off forensics.

5. Chip-off forensics is a technique used after all other acquisition methods have been exhausted. Chip-Off forensics is a technique in which the device is disassembled and the Ball Grid Array (BGA) or memory chip is removed from the device's printed circuit board, the memory chip is cleaned and repaired and raw data is extracted from the chip using specialized tools. This process renders the mobile device unusable but preserves the data content.

6. Depending on the model of the device, it may not be possible to extract data from the device for analysis. In some instances, an examiner may document data on the mobile device by viewing the data on the screen and documenting the data by capturing a photograph of the device's screen.

7. In some instances, a mobile/computer device may be damaged to an extent that extraction of data from the device or other analysis of the device in its current state would not be possible. This affiant is requesting authorization for the examiner, or a qualified third-party, to make any necessary repairs to such devices as necessary to allow for examination of the device.

8. When a mobile/computer device is locked by a user's lock code, password, pattern lock, or other form of lock, commercial and/or open source forensic tools may be able to bypass the lock to extract the data. In instances in which the forensic tools are unable to bypass the lock, an examiner may be able to bypass the lock by making modifications to the device or by using non forensic hardware or software to decipher the passcode or otherwise bypass the passcode. In some instances, making these modifications to the device may void the device manufacturer's warranty.

The examination process uncovers digital evidence, including that which may be hidden or obscured. The results are gained through applying established scientifically based methods. Mobile/computer device manufacturers typically offer a similar set of information handling features and capabilities. The set of features and capabilities vary based on the era in which the device was manufactured, the version of the firmware running, modifications made for a particular service provider, and any modifications or applications installed by the user. The potential evidence on these devices may include, but is not limited to, the following types of data:

1. Contacts – A listing of the device's contacts, such as name, address, phone number, email address, and other contact information. This contact information can be user generated in a contacts application, or can be documentation of a user's contacts through other applications such as social media applications.

2. Calendar – Items persons document in their calendar application, such as meetings, events, and birthdays.

3. Notes – Most smart phones have an application in which users can enter notes or memos.

4. Call Logs – Records of phone calls made, received, or missed. These records can come from the phone's native phone application, or through third party applications through

which users can make and receive phone calls using a number other than the number assigned through the phone's carrier. These phone numbers are obtained through the provider of the third-party application.

5. User Dictionaries – Most smart phones contain a dictionary to which words are added that don't exist in the phone's native dictionary. This feature works in conjunction with the messaging applications on the device to autocomplete words typed in messages or to make suggestions for auto-completion. These dictionaries will often contain slang words or words a user commonly misspells, which could assist an examiner for use during keyword searching.

6. User Accounts – Information about the user of the phone, as well as email addresses or other usernames and their associated service. This user account information is useful for identifying other web-based services or cloud storage services for which another search warrant could be sought to search for evidence of criminal activity.

7. Web Browser Data – This includes bookmarks and web browser history. Bookmarks are websites that are sometimes saved by default or entered by a user to provide easier access to their bookmarked websites. Web browser history is documentation of websites visited.

8. Messages – This includes Short Message Service (SMS) messages, commonly referred to as "text messages", Multimedia Messages (MMS), instant messages, and chat messages. Through a mobile device's native messaging applications, as well as third-party applications, a user has the ability to send and receive messages containing text, audio, video, and photos. Most smart phones also have the ability to capture screenshots of what is displayed on the screen and save it as an image. It is common to find screenshot images of messages stored on mobile devices.

9. Email – Modern smart phones have the ability to sync a user's email accounts to the mobile device through email applications or through a web browser. The mobile device may contain these emails.

10. Audio Files – Mobile devices can store audio files, including but not limited to: Voicemail, audio recorded using recording functionality of the device, and music files.

11. Documents – Documents such as PDF files, documents, and spreadsheets which can be saved to a device or external storage.

12. Applications – Examination of the applications present on the mobile device, such as social media applications, could lead the examiner to data stored within files created by that application.

13. Location Information – This includes Global Positioning System (GPS) data associated with metadata in photo and video files, and databases from applications that use GPS data in their operation. This location information can also come from cellular towers and Wi-Fi networks with which the device has interacted.

14. Photos – Images stored on the mobile device or external storage. This includes images captured by the device, in sent and received messages, downloaded, transferred from other devices, screenshots captured of the device's display, and other images created on the device through the user's device usage. In addition to photos related to criminal activity, it is common to find photos commonly referred to as "selfies" in which the user takes an image of him/her. These images can assist in identifying the user of the device.

15. Videos – Video movie files captured by the device or received from other sources. Like photos, these can often assist in identifying the user of the device.

16. Wireless Network Information – These records or wireless network connections could give clues to a device's historical locations.

17. Phone Number – The phone number associated to the mobile device.

18. Subscriber Identity Module (SIM) Card information – The SIM card can contain the phone number associated to the device, as well as limited information such as phone call logs, contacts, and text message records. SIM cards also contain an Integrated Circuit Card Identifier (ICCID) which is a unique identifier of the SIM card.

19. Subscriber and equipment identifiers – Such as Serial Number, Mobile Equipment Identifier (MEID), Electronic Serial Number (ESN), or International Mobile Station Equipment Identity (IMEI). Varying models of phones differ in the unique identifier they contain.

20. Unallocated space – This is available space on the storage media to which the operating system can write date. This space could contain data which has previously been deleted but has not yet been overwritten.

21. Information about cloud-based services – Mobile cloud computing is the combination of mobile networks and cloud computing allowing user applications and data to be stored on the cloud (i.e., internet servers) rather than the mobile device memory. (National Institute of Standards and Technology, 2014) Identification of these cloud-based services could be useful to this investigation to identify additional sources of digital evidence that may need to be searched through future legal process.

22. Information about synched devices – The data contained on a mobile device is often present on a personal computer due to the capability of mobile devices to synchronize or otherwise share information among one or more host computers. Because of synchronization, a significant amount of data may be present on the owner's laptop or personal computer. Identification of synced devices could yield information about these devices which could potentially contain evidence related to this matter.

23. Portable GPS Device data which may be of importance may include maps, tracks/archived tracks, waypoints, routes/journey, saved locations, favorites, owner information, "Home" location, recent destinations, city and state history, contacts/addresses, points of interest, last GPS fix, and pictures.

Some artifacts recovered may be only partial information or missing associated timestamp information but could still be of evidentiary value. Additionally, many mobile devices allow the user to change the time and date settings on their mobile device. A knowledgeable individual could alter the date/time of the mobile device to falsify timestamps associated with logged activities. For these reasons, this affiant requests for this search warrant to not be restricted to analysis or examination of activity during a specific timeframe.

Conclusion:

I am investigating official misconduct and theft involving Dubois County Sheriff, Thomas "Tom" J. Kleinhelter.

The facts set forth in this affidavit are based upon my own personal observations, my training and experience, and information obtained during this investigation, along with my mapping and analysis of the data.

Based upon the facts and circumstances set forth above, I hereby request that the Court issue a search warrant, authorizing the seizure and forensic examination of the mobile/computer device(s) to be seized under case number 24ISPC011536.

The property or data to be seized or documented, which constitutes unlawfully obtained property, contraband, property used or possessed with the intent to use in the commission or concealment of an offense of official misconduct is described as follows:

1. **Cellphone utilizing the phone number** [redacted]
2. **Desktop and laptop computer utilized by Tom Kleinhelter.**

The cellphone number [redacted] is known to be associated with:

1. **Thomas "Tom" J. Kleinhelter**
   575 N Weisheit Dr. Jasper, IN 47546
   [redacted]
   Gender: Male
   [redacted]

which is to be submitted to the Indiana State Police Digital Forensics Unit with an evidence hold, and any identity modules and/or removable media contained therein, using the above-described mobile device forensic methods, for the following:

1. Records of dialed and/or received phone calls, text messages, voicemails, emails, media messages, media searches, video recordings, audio recordings, photographs, contact logs/address book, and other digital evidence located within the device(s);

2. Indicia of ownership consisting of telephone number, images, nicknames, and other information which will assist law enforcement in establishing the identity of the person or persons who own, rent, lease, or purchased the device(s).

For the reasons described above, this Affiant also respectfully requests for this search warrant to include:

1. Authority to bypass or remove user locks using software or hardware tools, including methods or modifications which may void the device manufacturer's warranty;

2. Authority to, if necessary, perform a chip-off examination of the device;

3. Authority to repair a damaged device if necessary for the examination, including seeking assistance from non-law enforcement officers with experience in device repair; and

4. Authority to seek assistance from another qualified laboratory, including laboratories with forensic experts who are not sworn law enforcement officers.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

All of the above events occurred in Dubois County, Indiana.

I swear (affirm), under penalty of perjury as specified by IC 35-44-2-1, that the foregoing representations are true.

DATED: October 25, 2024 /s/ Lieutenant Jeffrey C. Hearon PE 5201
AFFIANT

REDACTED COPY

LIST OF PROPERTY, OBJECTS, THINGS, INFORMATION OR PERSONS SEIZED OR PRODUCED

SEARCH WARRANT 5

STATE OF INDIANA	)	IN THE DUBOIS COURT
	) SS:	_____
COUNTY OF DUBOIS	)	
		CAUSE NO:
		19D01-2410-MC-001192
IN THE MATTER OF	)	
A REQUEST FOR THE	)	
ISSUANCE OF A	)	
SEARCH WARRANT	)	

Law enforcement officer(s) are hereby authorized and ordered, in the name of the State of Indiana, with the necessary and proper assistance, to execute the search warrant and search the below more particularly described property as follows:

Dubois County Security Center
255 Brucke Strasse, Jasper, IN 47546

The property or data to be seized or documented, which constitutes unlawfully obtained property, contraband, property used or possessed with the intent to use in the commission or concealment of an offense of official misconduct and theft is described as follows:

1. **Cellphone utilizing the phone number** [redacted]
2. **Desktop and laptop computer utilized by Tom Kleinhelter.**

The cellphone number [redacted] is known to be associated with:

1. **Thomas "Tom" J. Kleinhelter**
   575 N Weisheit Dr, Jasper, IN 47546
   [redacted]
   Gender: Male
   [redacted]

This search warrant authorizes law enforcement officers to seize and conduct a forensic examination analysis on the above-described device(s), including any identity modules and/or removable media contained therein, using forensic methods described in the attached Affidavit, to search for and seize the following:

1. Records of dialed and/or received phone calls, text messages, voicemails, emails, media messages, media searches, video recordings, audio recordings, photographs, contact logs/address book, and other digital evidence located within the devices;

2. Indicia of ownership consisting of telephone number, images, nicknames, and other information which will assist law enforcement in establishing the identity of the person or persons who own, rent, lease, or purchased the devices.

The Court is specifically grants permission, in order to locate and retrieve the above-described information and data, the forensic examiners and/or law enforcement officers have:

3. Authority to bypass or remove user locks using software or hardware tools, including methods or modifications which may void the device manufacturer's warranty;

4. Authority to, if necessary, perform a chip-off examination of the device;

5. Authority to repair a damaged device if necessary for the examination, including seeking assistance from non-law enforcement officers with experience in device repair; and

6. Authority to seek assistance from another qualified laboratory, including laboratories with forensic experts who are not sworn law enforcement officers.

This **Search Warrant and Affidavit**, and attached and incorporated **Statement of Probable Cause** and associated attachments were sworn to as true and subscribed before me on this _____ day of _____, _____, at _____A.M. / P.M.

Wherefore, I find probable cause for the issuance of this Search Warrant and do issue it.

ORDER APPROVED: _____ YES _____ NO

_____
(Signature)
Judge