

UNITED STATES DISTRICT COURT

for the Eastern District of Tennessee

FILED

MAY 13 2024

Clerk, U. S. District Court Eastern District of Tennessee At Knoxville

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

RESIDENTIAL PROPERTY LOCATED AT 821 W. KING STREET, JEFFERSON CITY, TENNESSEE 37760

Case No. 3:24-MJ-1128

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Tennessee

(identify the person or describe the property to be searched and give its location):

See Attachment A-1.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before May 22, 2024 (not to exceed 14 days)

[x] in the daytime 6:00 a.m. to 10:00 p.m. [] at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Debra C. Poplin

(United States Magistrate Judge)

[] Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

[] for ___ days (not to exceed 30) [] until, the facts justifying, the later specific date of

Date and time issued: 5/8/2024 01:30 PM

Debra C. Poplin (signature) Judge's signature

City and state: Knoxville, Tennessee

Debra C. Poplin, United States Magistrate Judge Printed name and title


Return		
Case No.: 3:24-MJ-1128	Date and time warrant executed: 05/09/2024, 7:33 am	Copy of warrant and inventory left with: [REDACTED]
Inventory made in the presence of: SA William Leckrone		
Inventory of the property taken and name of any person(s) seized: see attached FD-597.		

FILED

MAY 13 2024

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

PJS

Certification	
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.	
Date: 05/13/2024	 Executing officer's signature
	David J. Sekora, Special Agent Printed name and title

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

FILED

Case ID: [Redacted]

On (date) 5/9/2024

- item(s) listed below were:
- Collected/Seized
- Received From
- Returned To
- Released To

MAY 13 2024

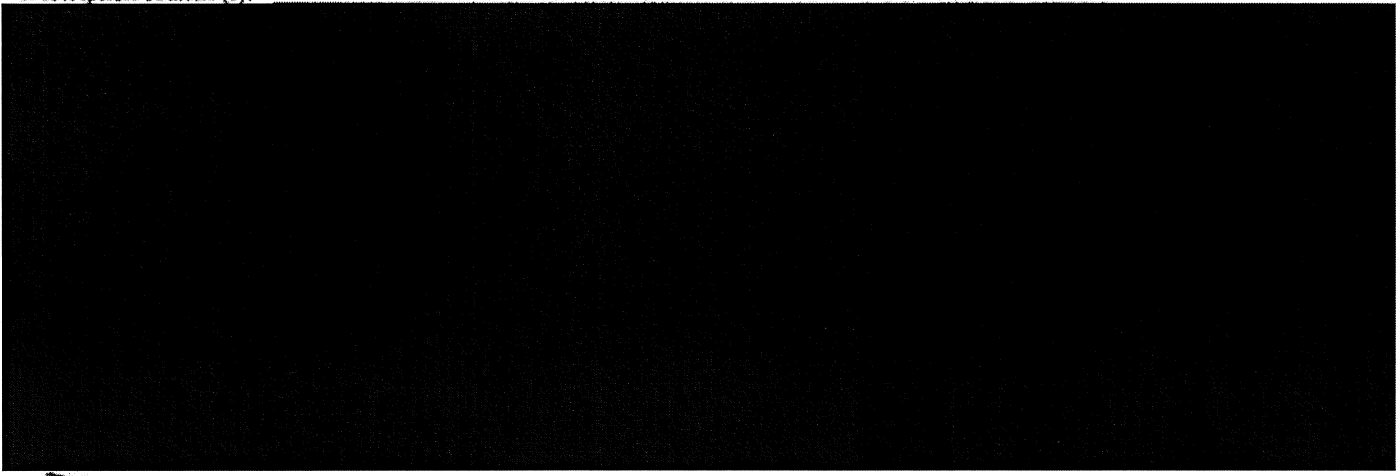
Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

(Name) [Redacted]

(Street Address) 821 W King Street, Jefferson City, TN 37760

(City) _____

Description of Item (s):



Received By: [Signature] (Signature)

Received From: [Redacted] (Signature)

Printed Name/Title: James Smith

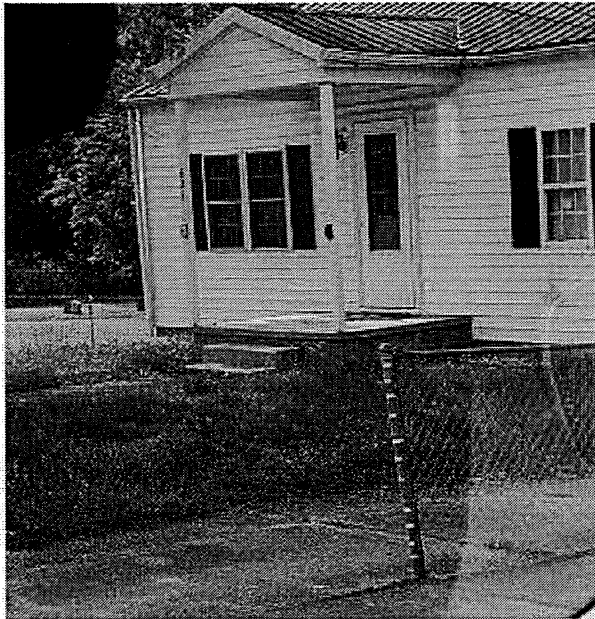
Printed Name/Title: [Redacted]

ATTACHMENT A-1

Property to Be Searched

The property to be searched is 821 W. King Street, Jefferson City, Tennessee 37760, further described as a detached single-story house with a detached garage. The exterior is painted white. The house number (821) is displayed vertically on the left side front porch column.

Photographs of the house are depicted below:



ATTACHMENT B

Property to Be Seized

1. All records relating to violations 18 U.S.C. § 371 (Conspiracy to defraud the United States and its agencies), 18 U.S.C. § 1343 and 1349 (Wire fraud and conspiracy to commit wire fraud), 18 U.S.C. § 1028A (Aggravated identity theft), 18 U.S.C. § Section 1028(a)(7), (b)(1)(D), (c)(3)-(A), and (f) (Fraud and related activity in connection with identification documents, authentication features, and information), 8 U.S.C. § 1324a (Unlawful employment of aliens), 18 U.S.C. § 1956(a)(1)(B)(i) and (a)(2)(A), and (h) (Laundering of monetary instruments and conspiracy to commit laundering of monetary instruments), and 18 U.S.C. § 1960 (Unlicensed money transmitting business) occurring in or after July 2018, including:

- a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;
- b. records and information relating to a conspiracy to launder funds;
- c. employment records;
- d. financial records;
- e. personal identification documents for [REDACTED]
[REDACTED]
- f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;
- g. records and information related to individuals gaining employment as a remote worker;
- h. records and information related to U.S.-based entities who employed remote workers;

- i. records and information relating to the identity or location of the suspects;
2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;
3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;
4. Packaging and shipping materials;
5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;
6. United States currency, foreign currency, financial instruments, negotiable instruments, jewelry, precious metals, stocks, bonds, money wrappers, and receipts or documents regarding purchases of real or personal property;
7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;
8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, and records of real estate transactions;
9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;
10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as "electronic storage media") owned, operated, maintained, or controlled by [REDACTED]

██████████ or ██████████ ██████████

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

- a. all information related to the offenses as described in paragraph 1;
- b. all bank records, checks, credit card bills, account information, or other financial records;
- c. any information recording schedule or travel;
- d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;
- e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;
- f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;
- i. evidence of the times the electronic storage media were used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

- k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;
- l. records of or information about Internet Protocol addresses used by the electronic storage media;
- m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or 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 FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their review.

FILED

MAY 13 2024

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

UNITED STATES DISTRICT COURT

for the

Eastern District of Tennessee

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

RESIDENTIAL PROPERTY LOCATED AT 1607 RUSSELL
AVENUE, UNIT 224F, JEFFERSON CITY, TN 37760.

Case No. 3:24-MJ-1129

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Tennessee
(Identify the person or describe the property to be searched and give its location):

See Attachment A-I.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(Identify the person or describe the property to be seized):*

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before May 10, 2024 *(not to exceed 14 days)*
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

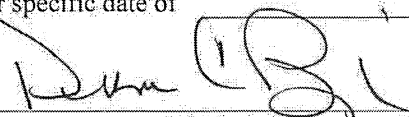
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Debra C. Poplin
(United States Magistrate Judge)

Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

for days *(not to exceed 30)* until, the facts justifying, the later specific date of

Date and time issued:

5/7/2024 @ 1:33pm



Judge's signature

City and state:

Knoxville, Tennessee


Debra C. Poplin, United States Magistrate Judge

Printed name and title

Return		
Case No.: 3:24-MJ- 1129	Date and time warrant executed: 05/09/2024 7:36a	Copy of warrant and inventory left with: [REDACTED]
Inventory made in the presence of: SA Nicholas Hanggi		
Inventory of the property taken and name of any person(s) seized: See attached FD-597		

FILED
MAY 13 2024
Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

DJS

Certification	
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.	
Date: 05/13/2024	 Executing officer's signature
	David J. Sekera, Special Agent Printed name and title

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property

FILED

MAY 13 2024

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

Case ID: [Redacted]

On (date) May 9, 2024

item (s) listed below were:

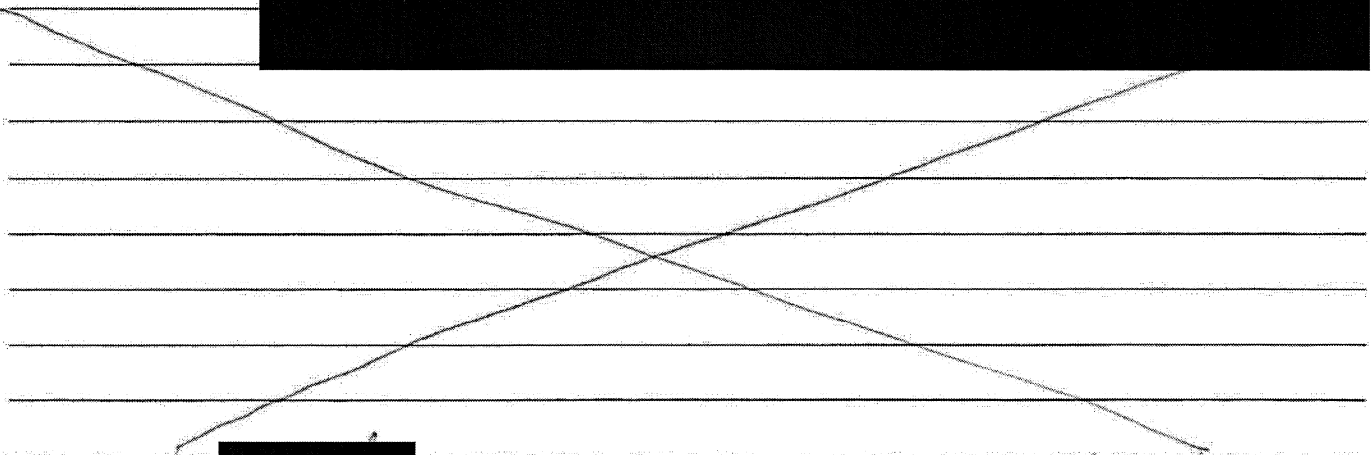
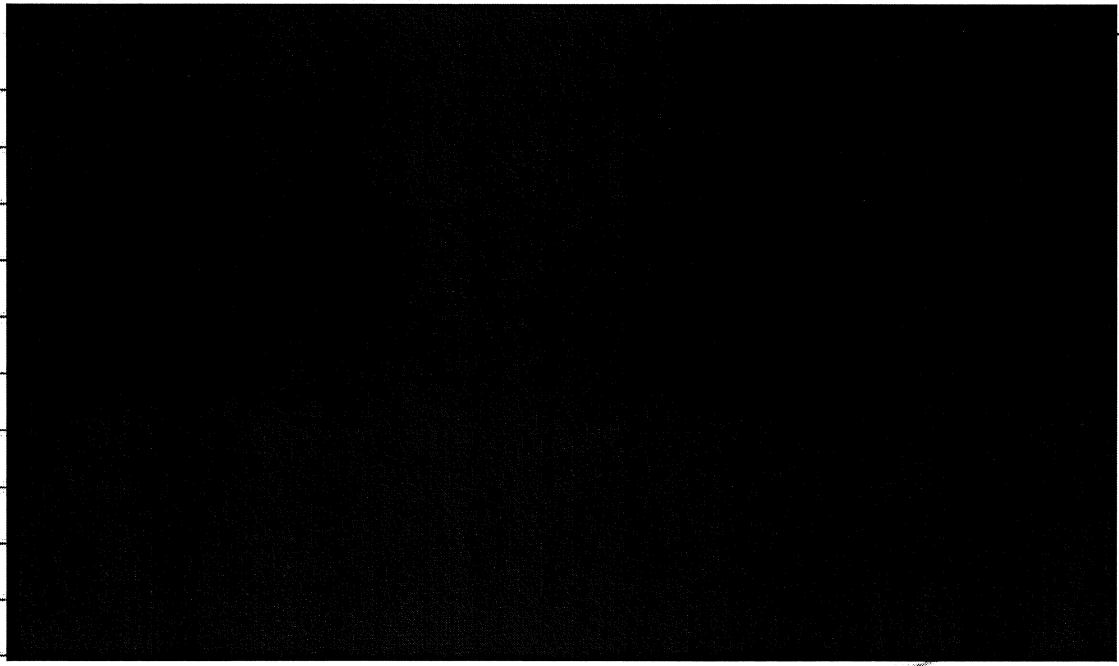
- Collected/Seized
- Received From
- Returned To
- Released To

(Name) [Redacted]

(Street Address) 1607 Russell Ave, Suite 224 F, Jefferson City, TN 37760

(City) Jefferson City

Description of Item (s):



Received By: [Redacted]

Printed Name/Title: [Redacted]

Received From: Nicholas Hangan
(Signature)

Printed Name/Title: NICHOLAS HANGAN
SPECIAL AGENT

ATTACHMENT A-2

Property to Be Searched

The property to be searched is 1607 Russell Ave, Unit 224F, Jefferson City, TN 37760, further described as a dorm room within the Carson-Newman University Burnett Residence Hall. The residence hall is three stories. Room 224F is accessible from an interior hallway. The room number is painted in black above the door frame. Photograph are depicted below:



ATTACHMENT B

Property to Be Seized

1. All records relating to violations 18 U.S.C. § 371 (Conspiracy to defraud the United States and its agencies), 18 U.S.C. § 1343 and 1349 (Wire fraud and conspiracy to commit wire fraud), 18 U.S.C. § 1028A (Aggravated identity theft), 18 U.S.C. § Section 1028(a)(7), (b)(1)(D), (c)(3)-(A), and (f) (Fraud and related activity in connection with identification documents, authentication features, and information), 8 U.S.C. § 1324a (Unlawful employment of aliens), 18 U.S.C. § 1956(a)(1)(B)(i) and (a)(2)(A), and (h) (Laundering of monetary instruments and conspiracy to commit laundering of monetary instruments), and 18 U.S.C. § 1960 (Unlicensed money transmitting business) occurring in or after July 2018, including:

- a. records and information relating to a conspiracy to defraud entities seeking to employ remote workers;
- b. records and information relating to a conspiracy to launder funds;
- c. employment records;
- d. financial records;
- e. personal identification documents for [REDACTED] [REDACTED] or [REDACTED]
[REDACTED]
- f. records and information relating to the location of participants in a scheme to defraud U.S.-based entities seeking to employ remote workers;
- g. records and information related to individuals gaining employment as a remote worker;
- h. records and information related to U.S.-based entities who employed remote workers;

- i. records and information relating to the identity or location of the suspects;
2. Books, records, receipts, notes, ledgers, invoices, and any other documentation related to the scheme;
3. Notes containing the individual names of such persons, telephone numbers or addresses of associates in the schemes, and any records of accounts receivable, money paid or received, cash or checks received, or intended to be paid;
4. Packaging and shipping materials;
5. Records relating to the receipt, transportation, deposit, transfer, or distribution of money, including but not limited to, direct deposit confirmations, wire transfers, money orders, cashier's checks, check stubs, PayPal, Payoneer, or other electronic money transfer services, check or money order purchase receipts, account statements, and any other records reflecting the receipt, deposit, or transfer of money;
6. United States currency, foreign currency, financial instruments, negotiable instruments, jewelry, precious metals, stocks, bonds, money wrappers, and receipts or documents regarding purchases of real or personal property;
7. Safe deposit box keys, storage locker keys, safes, and related secure storage devices, and documents relating to the rental or ownership of such units;
8. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises found thereon during the execution of the warrant, including, utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, and records of real estate transactions;
9. Photographs, including still photos, negatives, slides, videotapes, and films, in particular those showing co-conspirators, criminal associates, U.S. currency, real and personal property;
10. Computers, cellular phones, tablets, and other media storage devices, such as thumb drives, CD-ROMs, DVDs, Blu Ray disks, memory cards, and SIM cards (hereafter referred to collectively as "electronic storage media") owned, operated, maintained, or controlled by [REDACTED] L

██████████ or ██████████ ██████████

11. Records evidencing ownership or use of electronic storage media, including sales receipts, registration records, and records of payment;

12. Any records and information found within the digital contents of any electronic storage media seized from the Subject Premises, including:

- a. all information related to the offenses as described in paragraph 1;
- b. all bank records, checks, credit card bills, account information, or other financial records;
- c. any information recording schedule or travel;
- d. evidence of who used, owned, or controlled the electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, and phonebooks;
- e. evidence indicating how and when the electronic storage media were accessed or used to determine the chronological context of electronic storage media access, use, and events relating to crime under investigation and to the electronic storage media user;
- f. evidence indicating the electronic storage media user's state of mind as it relates to the crime under investigation;
- g. evidence of the attachment to an electronic storage medium of another storage device or similar container for electronic evidence;
- h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage media;
- i. evidence of the times the electronic storage media were used;
- j. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage media;

- k. documentation and manuals that may be necessary to access the electronic storage media or to conduct a forensic examination of the electronic storage media;
- l. records of or information about Internet Protocol addresses used by the electronic storage media;
- m. records of or information about the electronic storage media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as prints, slides, negatives, videotapes, motion pictures, or photocopies). This shall include records of telephone calls; names, telephone numbers, usernames, or other identifiers saved in address books, contacts lists and other directories; text messages and other stored communications; subscriber and device information; voicemails or other audio recordings; videos; photographs; e-mails; internet browsing history; calendars; to-do lists; contact information; mapping and GPS information; data from "apps," including stored communications; reminders, alerts and notes; and any other information in the stored memory or accessed by the electronic features of the computer, electronic device, or other storage medium.

This warrant authorizes a review of records and information seized, copied or 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 FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their review.