

## RETURN

DATE WARRANT  
RECEIVED

3/11/09

DATE AND TIME WARRANT  
EXECUTED

3/17/09 6:00am

COPY OF WARRANT AND RECEIPT  
FOR ITEMS LEFT WITH

BRADLEY HENNER

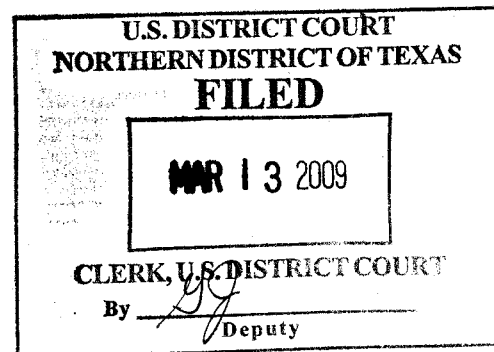
INVENTORY MADE IN THE PRESENCE OF

BRADLEY HENNER

3-09-MJ-75

INVENTORY OF PROPERTY SEIZED PURSUANT TO THE WARRANT

532 ATTORNS



## CERTIFICATION

I Swear that this inventory is a true and detailed account of the property seized by me on the warrant.

Subscribed, sworn to, and returned before me this date.

U.S. Judge or Magistrate

3-13-09

Date

United States District Court

NORTHERN

DISTRICT OF

TEXAS

In the Matter of the Search of

(Name, address or Brief description of person, property or premises to be searched)

SEARCH WARRANT

2323 Bryan St., Cabinet 24.02.900  
Dallas, TX

CASE NUMBER: 3:09-mj-75

To: Special Agent Allyn Lynd, Federal Bureau of Investigation (FBI) and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Allyn Lynd who has reason to believe that XX on the property or premises known as (name, description and/or location)

(SEE ATTACHMENT A)

in the NORTHERN District of TEXAS there is now concealed a certain person or property, namely (describe the person or property to be seized)

(SEE ATTACHMENT B)

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before

March 21, 2009

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.) (~~at any time in the day or night as I find reasonable cause has been established~~) and if the person or property be found there to seize same, leaving copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to PAUL D. STICKNEY, United States Magistrate Judge as required by law.

March 11, 2009 @ 1:30  
Date and Time Issued

at Dallas, Texas  
City and State

PAUL D. STICKNEY  
United States Magistrate Judge  
Name and Title of Judicial Officer

[Signature]  
Signature of Judicial Officer

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # 288A-DL-108410

On (date) March 12, 2009

item(s) listed below were:

- ☐ Received From  
☐ Returned To  
☐ Released To  
☒ Seized

(Name) TelX, Bradley J. Heller, Technical Support Manager  
(Street Address) 2323 Bryan Street Suite 2410  
(City) Dallas, TX 75201

Description of Item(s):

1. Fiber panel - data code 0747-032
2. T1/DS1 panel S/N 223946719
3. DS-3 Bulkhead
4. Fiber panel data code 0746-315
5. T1/DS1 panel S/N 22409779
6. DS3 bulkhead S/N 199265600017

*nothing follows*

Received By:

Alberto L. Michael  
(Signature)

Received From:

Bryon Heller  
(Signature)

ATTACHMENT A

DESCRIPTION OF 2323 BRYAN ST, CABINET 24.02.900, DALLAS, Texas, 75201

The cabinet is located on the 24<sup>th</sup> floor of 2323 Bryan and is marked 24.02.900. It is colored blue and is locked. It contains connections to two DS-3s and a T-1. The building is an office skyscraper located at the corner of Bryan and Crockett. It has a large corporate logo for Ultravision which is a four colored U at the top of the building.

ATTACHMENT B

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

1. Proceeds, records of proceeds, documents pertaining to, and/or payments related to the conspiracy, computer hardware, and bank records.
2. Electronic storage devices which consist of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar transmission, reception, collection and storage of data. Electronic storage device includes (but is not limited to) any wireless/cellular telephone, cordless telephone, pager, fax machine, digital camera, audio recorder, video recorder and any data-processing device e.g. central processing units, memory typewriters, self-contained "laptop", "notebook", "mini-notebook", or "personal data assistant" computers.
3. Any telephonic device which consists of all equipment which can transmit information over any telephone network, assist in said transmission, alter said transmission, disguise such transmission, pay for such transmission, conceal such transmission, and otherwise enhance or degrade such transmission, to include but not limited to telephones, headsets, calling cards, voice alteration devices and software, microphones, speakers, Voice over IP equipment (both hardware and software), ANI altering devices and software, war dialing equipment, etc.
4. Internal and external storage devices e.g. fixed disks (hard drives), memory cards, floppy disk, LS-120, zip drive, jaz drive, Orb drive, CD drive, DVD drive, diskettes, tape drives, optical storage devices, transistor-like binary devices, and other memory storage devices including the storage media used in the devices. Peripheral input/output device such as keyboards, printers, scanners, plotters, video display monitors, and optical readers.

5. Related communication devices e.g. modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices. Any device, mechanism, or parts that can be used to restrict access to electronic storage devices e.g. physical keys and locks bio metric readers, retinal scanners, facial recognition, signature verification, smart card or voice authentication.

6. Computer/Equipment software (digital information) which can be interpreted by electronic storage device equipment, computers and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communication programs.

7. Electronic storage device documentation consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use electronic storage device hardware, software, or other related items.

8. Electronic storage device passwords and other data security devices are designed to restrict access to or hide software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

9. A password (a string of alphanumeric characters). A password usually operates as a sort of digital key to “unlock” particular data security devices.

10. Data security hardware, including but not limited to, encryption devices, chips, dongles, biometric readers, retina scanners, facial recognition systems, voice authentication systems, hand writing authentication systems and circuit boards.

11. Data security software or digital code, including but not limited to,

programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt; compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

12. Records, notes, address books, calendars, and any other documents that may relate to the violations; magnetic and/or electronic storage media which may contain information relating to the violations; financial records, bank records, correspondence, currency, or other forms of payment that may represent payments related to the violations; property, including manuals, records, media, and work papers, that may relate to trafficking Fraud and Related Activity in Connection with Computers.

13. It is further requested that a forensic technician, sworn or non-sworn, be granted authorization to examine; make duplicate images/copies of the above-mentioned electronic media and to determine if evidence of the offenses enumerated above are contained therein. Therefore authorization is requested to make images/copies of the requested data. Evidence copies of the items relating to these offenses will be created and retained for further proceedings and made available to the authorities.

14. Only those items recovered under the Search Warrant and relating to the offenses will be retained. The master copy will be retained in evidence storage for later discovery and trial purposes.

15. Articles of personal property which would tend to establish the identity of persons in control of said premises, which items of property would consist in part of and include, but not limited to papers, documents and effects which tend to show possession, dominion and control over said premises, including but not limited to keys, canceled mail envelopes, rental agreements and receipts, utility and telephone bills, prescription bottles,

vehicle registration, vehicle repairs and gas receipts, whether such items are written, typed or stored electronically.

16. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).