AO 93 (Rev. 12/03) Search Warrant

UNITED STATES DISTRICT COURT

EASTERN District of CALIFORNIA

In the Matter of the Search of

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

[redacted]
STOCKTON CALIFORNIA 95206

SEARCH WARRANT

Case Number: 2:11-SW-0239 GGH

TO: **U.S. Department of Education, Office of Inspector General Special Agent Howard Nance**, and any Authorized Officer of the United States

Affidavit(s) having been made before me by **Howard Nance** who has reason to believe
Affiant

that ☐ on the person of, or ☒ on the premises known as (name, description and/or location)

SEE ATTACHMENT A-1

in the Eastern District of California there is now concealed a certain person or property, namely (describe the person or property)

SEE ATTACHMENTS A & B

I am satisfied that the affidavit(s), which is attached hereto and incorporated herein by this reference, and any record 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 June 17, 2011
Date

(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 anytime 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 a 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

GREGORY G. HOLLOWS as required by law.
U.S. Magistrate Judge (Rule 41(f)(f4))

June 03, 2011 10:20a.m. at **Sacramento, California**
Date and Time Issued City and State

GREGORY G. HOLLOWS
US Magistrate Judge
Name and Title of Judge

GREGORY G. HOLLOWS
Signature of Judge

AO 93 (Rev. 12/03) Search Warrant

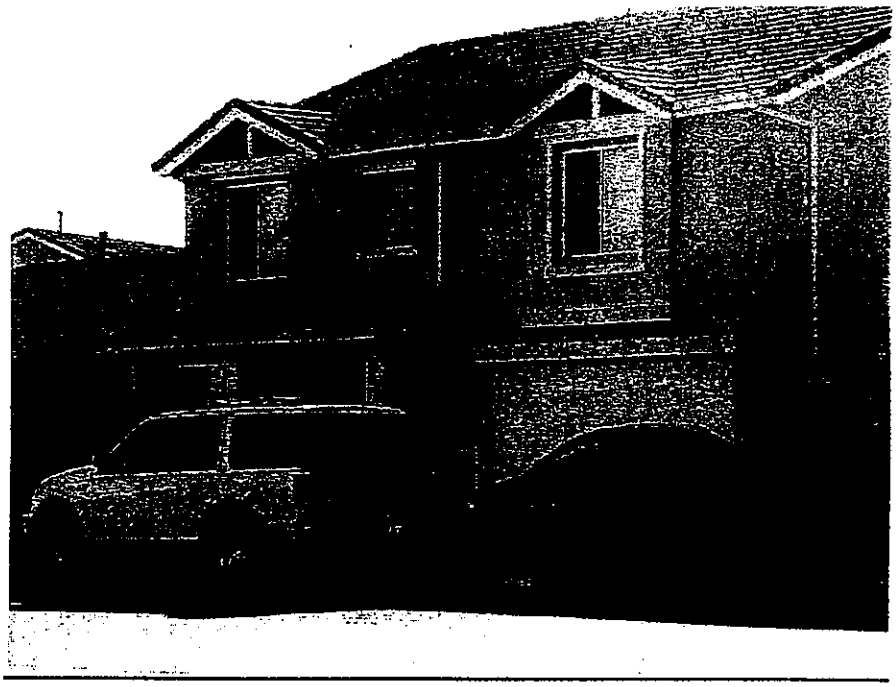
RETURN	Case Number:	
DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
INVENTORY MADE IN THE PRESENCE OF		
INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT		

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

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

ATTACHMENT A-1 – LOCATION TO BE SEARCHED – PAGE 1

[redacted] Stockton, CA 95206 (SUBJECT PREMISES #1). The residence is a tan stucco two-story four bedroom structure with a charcoal tiled roof and burgundy wood shutters. The residence is approximately 2,399 Sq feet. The numbers [redacted] appear in black letters affixed to the left of a two stall cream garage door. The residence is located on the north side of [redacted] The front door is burgundy and faces West onto [redacted] The residence is located in the City of Stockton, County of San Joaquin, and State of California.



The area to be searched includes SUBJECT PREMISES #1, including all rooms, annexes, attics, basements, porches, garages, carports, outside yard, curtilage, mailboxes, trash containers, debris boxes, storage lockers, locked containers and safes, cabinets, rooms, outbuildings, sheds and outbuildings associated with this subject premise and shall extend into desks, cabinets, safes, briefcases, backpacks, wallets, purses, trash receptacles, electronic storage devices, any vehicles or boats parked on the property or in the driveway specifically associated with, or assigned to SUBJECT PREMISES #1, and any other storage locations within the SUBJECT PREMISES #1.

The search of this SUBJECT PREMISES #1 shall also authorize officers conducting the search to require the production of identification of any person reasonably believed by the officers to have possession and control of the SUBJECT PREMISES #1. The search shall also authorize officers to search the persons and items attached to them (such as purses, backpacks, wallets, etc.) encountered at SUBJECT PREMISES #1, whether they are located indoors, outdoors or in an automobile found at SUBJECT PREMISES #1 and/or the curtilage of the SUBJECT PREMISES

ATTACHMENT B - <u>ITEMS TO BE SEIZED</u> – PAGE 1

1. The following records, documents, and items including information and/or data stored in a computer readable format to be seized at the premises of SUBJECT PREMISES #1 and SUBJECT PREMISES #2 and inside any such areas within the curtilage of the aforementioned locations that would reasonably serve to store or hide such items, such as storage sheds, outbuildings, storage containers, trailers, or vehicles that constitute evidence, contraband, fruits, and/or instrumentalities of violations of 20 U.S.C. § 1097 (Financial Aid Fraud), 18 U.S.C. § 371 (Conspiracy), 18 U.S.C. § 641 (Theft of Government Funds), 18 U.S.C. § 1001 (False Statement to Government Agency), and 18 U.S.C. § 1343 (Wire Fraud) for the time period of 2009 to present:

a. Financial aid applications, financial aid worksheets, financial aid records, tax records, wage and earning statements, W-2 documents, and any other documentation containing the names or personal identifying information for the names listed on Page 4 of this Attachment, and any other names not belonging to occupants of the residences set forth in Attachments A-1 and A-2 – Location to be Searched, relating to a fraudulent student financial aid scheme;

b. Applications for admission to post-secondary institutions and supporting documents, including, but not limited to, proof of eligibility (i.e. high school diploma, or GED transcripts), correspondence, e-mails, notes, and evidence of payment of fees;

c. Evidence of enrollment and/or attendance in a post-secondary institutions, including, but not limited to acceptance letters, academic transcripts, student handbooks, course schedules, campus informational pamphlets, student identification cards, e-mails, notes, and correspondence from schools to the students;

d. Correspondence relating to the award of federal and non-federal student financial aid and serving student loans, including, but not limited to, financial aid award letters, promissory notes, loan deferment requests, e-mails, notes, and outstanding loan balance letters;

e. Correspondence between any of the persons listed on Page 4 of this Attachment;

f. Records reflecting the expenditures and/or distribution of federal and non-federal student financial aid including, but not limited to debit cards, prepaid credit cards, checks, bank records, ledgers, and deposit slips;

g. Records relating to current and past residences and any mail receipts;

h. Any and all envelopes, letters, and or other correspondence, memoranda, mail, notes, ledgers, other documents and records of communications, whether handwritten, electronic or otherwise, bearing the identification of any school, university, post-secondary institution;

i. Any and all fax machines, scanners, and printers used to manufacture, produce, or facilitate the submission of fraudulent federal and non-federal student financial aid applications, fraudulent identification documents, wire fraud, and mail fraud;

j. Any and all records pertaining to U.S. Post Office mail boxes, or any other mail receipt facilities;

k. Indicia of occupancy, residency, rental and/or ownership of premises described herein, including but not limited to utility and telephone bills, canceled envelopes, rental purchases or lease agreements, and keys;

l. All safes or other locked compartments that cannot be opened on the premises during the search;

~~m. Contraband or any other item that is immediately apparent to be evidence of a crime;~~

n. Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices;

o. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes;

p. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes;

q. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

r. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

s. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

t. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

u. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) or owners of the computers or digital devices during the time the device was utilized to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software (or alternatively, the lack of software that would allow others to control the digital device).