. FILED LODGED _

07-MJ-00383-APPL

_TES DISTRICT COUR**⁴**©

WESTERN DISTRICT OF WASHING TON US

In the Matter of the Search of

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

Crown College, located at 8739 S. Hosmer Street,
Tacoma, Washington. There are two connected buildings,
one two-story, the other single-story. Both are
light colored buildings with tan roofs.

APPLICATION AND AFFIDAVITY FOR SEARCH WARRANT

CASE NUMBER: MJ07-383

I, ADAM M. SHANEDLING , being duly sworn depose and say:
I am a(n) <u>Special Agent with the United States Department of Education</u> and have reason to believe that on the person of or <u>X</u> on the property or premises known as (name, description and/or location)
See Attachment A, which is attached hereto and incorporated herein by reference,
in the <u>Western</u> District of <u>Washington</u> there is now concealed a certain person or property, namely (describe the person or property to be seized)
See Attachment B, which is attached hereto and incorporated herein by reference,
which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
Evidence fruits and instrumentalitites of the crimes of Conspiracy to Defraud, Bank Fraud and Financial Aid Fraud
concerning a violation of Title 18 United States Code, Section(s) 371 and 1344 and Title 20, United States Code, Section 1097. The facts to support a finding of Probable Cause are as follows:
See Attached Affidavit of Special Agent ADAM M. SHANEDLING, attached hereto and incorporated herein.
Continued on the attached sheet and made a part hereof: X Yes No
ADAM M. SHANEDLING, Affiant
Sworn to before me and subscribed in my presence,
August 10, 2007 Date at Seattle, Washington City and State
MARY ALICE THEILER United States Magistrate Judge Signature of Judicial Officer

ATTACHMENT A

LOCATION TO BE SEARCHED:

Crown College is located at 8739 South Hosmer Street, Tacoma, Washington 98444. The college is made up of two connected buildings. The front building is two-stories and the back building is a single-story. Both buildings are lightly colored, sit on several rows of grey cinder blocks, and have tan roofs. The numbers "8739 is displayed on the west side of the front building, which is approximately 15 feet from Hosmer Street. There is also a Crown College sign in blue letters on a white background on the north side of the front building.

ATTACHMENT B

The following records, documents, and other items that constitute evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Section 371 (Conspiracy to Defraud), Title 18, Unites States Code, Section 1344 (Bank Fraud), and Title 20, United States Code, Section 1097 (Financial Aid Fraud), are to be seized:

Any and all Crown College records, books, papers and documents relating to the period of 2004 to present as described below:

- 1. Student records, including attendance records, ledgers of student charges and payments, tests and grade records, financial aid records, Pell Grant records, loan records, enrollment verification reports, eligibility records, and graduation records for the following individuals:
 - a. Mullineaux, Sheila
 - b. Byers-Martinez, Jennifer
 - c. Martinez, Jennifer
 - d. Lee, Misty
 - e. McMullin, Scott
 - f. McMullin, Jesica
 - g. Hinton, Brandon
 - h. Dogeagle, Jeremy
- 2. Student records, including attendance records, ledgers of student charges and payments, tests and grade records, financial aid records, Pell Grant records, loan records, enrollment verification reports, eligibility records, and graduation records of any other students who were employed by Crown College.
- 3. Any and all documents sent to or received from the Department of Education, including eligibility records, student payment summary reports, audit reports, program review reports, all correspondence with ED, and supporting documentation.
- 4. Documents reflecting or relating to communications with the Northwest Education Loan Association concerning the aforementioned students.
- 5. Documents reflecting or relating to communications with Sallie Mae concerning the aforementioned students.
- 6. Documents reflecting or relating to communications with the aforementioned students.
- 7. Internal correspondence, including correspondence directives, policy statements, and reference manuals relating to the operation and management of all Title IV federal student aid programs.

- 8. Records, rosters, or ledgers identifying the names of all employees and students at Crown College.
- 9. Financial records, including all payroll and financial statements, invoices, ledger books, disbursement journals, and all bank account information including checks, statements, cancelled checks, money orders, passbooks, certificates of deposit, and credit card receipts/statements.
- 10. Telephone and or address books, rolodexes, calendars, and any other documents listing telephone numbers and identifying information for Crown College employees.
- 11. Personnel records, including employment contracts, performance evaluations, attendance records, training records, resumes, salary and bonus information, termination, or severance agreements, and any additional information relating to employees.
- 12. Evidence of occupancy and/or ownership of the premises described in the search warrant, including bills, cancelled checks, and rental agreements.
- 13. All computer hardware consisting of all equipment that can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical, or similar computer data. Hardware includes, but is not limited to, any data processing devices, such as central processing units, memory typewriters, and self-contained laptop or notebook computers; internal and peripheral storage devices, such as fixed disks, external hard disks, floppy disk drives, tape drives, and tapes, compact discs, optical storage devices, and any other storage devices; peripheral input/output devices, such as keyboards, printers, scanners, plotters, video display monitors, and optical readers; and related communication devices, such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers; as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware, such as physical keys and locks.
- 14. All computer software consisting of digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software that is stored in electronic, magnetic, optical, or other digital form and programs to run operating systems, and applications, such as word processing, graphics, and spreadsheet programs.
- 15. All computer generated documents consisting of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.
- 16. All computer passwords and other data security devices that are designed to restrict access or hide computer software, documentation, or data.
- 17. All computer information related to the administration of Federal Student Financial Aid

programs, student attendance, or other records specified previously in this warrant affidavit as evidence to be seized.

THE SEIZURE OF COMPUTER SYSTEMS AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH COMPUTER SYSTEMS CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.

I, ADAM M. SHANEDLING, being duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

- 1. I am a Special Agent with the United States Department of Education (hereinafter ED), Office of Inspector General (hereinafter OIG). I have been a Special Agent of the ED-OIG since October 2, 2006, and am assigned to the Long Beach, California Field Office. Prior to working for ED-OIG, I was a Transportation Security Specialist for the United States Transportation Security Administration (TSA), based in Brussels, Belgium, for almost three years and Los Angeles, California, for one year. In this capacity I performed regulatory inspections and investigations throughout Europe, Africa, Middle East, and the Pacific. Prior to the TSA, I was a Special Agent for the Federal Aviation Administration (FAA) Security Division in Honolulu, Hawaii, for almost five years. In this capacity I performed regulatory inspections and investigations of regulated transportation entities, specializing in hazardous materials and cargo enforcement.
- 2. As part of my official duties, I am authorized to conduct investigations in connection with the enforcement and administration of all laws, regulations, orders, contracts, and programs to which ED is or may be a party of interest, and perform other duties on behalf of the Secretary of Education. Along with investigations referenced in this affidavit, I have been involved in the investigation of other cases involving student financial aid fraud and other illegal activities involving private, for-profit postsecondary schools. During my employment as a Federal Law Enforcement Agent, I have conducted multiple investigations. Throughout the course of these investigations, I have conducted interviews and secured other relevant information using a variety of investigative techniques.

3. I am familiar with information contained in this Affidavit, through personal investigation and communication with witnesses and other law enforcement and government personnel who have themselves obtained the information. I have also reviewed available documents relevant to this investigation and am personally familiar with their contents.

SPECIFICS FOR SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

- 4. I have consulted with forensic computer experts within our office regarding the search of computer systems. Based on my consultation with these experts and other agents who have been involved in the search of computers and retrieval of data from computer systems and related media, I know that searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:
- a. <u>Volume of Evidence</u>. Computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-ROMs, DVDs, and Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
- b. <u>Technical Requirements</u>. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity

8

9

6

10 11

12 13

14

15 16

17

18 19

20

21

22 23

24

25 26

27

28

of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

- Hidden Obfuscated Evidence. Computer users can conceal data C. within computers and electronic storage media through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Similarly, computer users can encode communications to avoid using key words that would be consistent with the criminal activity. Computer users can also attempt to conceal electronic evidence by using encryption technologies. For example, some encryption systems require that a password or device, such as a "dongle" or "keycard," be used to obtain a readable form of the data. In addition, computer users can conceal electronic evidence within another seemingly unrelated and innocuous file using a process known as "steganography." For example, by using steganography, a computer user can conceal text in an image file in such a way that it cannot be read when the image file is opened using ordinary means. As a result, law enforcement personnel may have to search all the stored data to determine which particular files contain items that may be seized pursuant to the warrant. This sorting process can take a substantial amount of time, depending on the volume of data stored and other factors.
- d. Deleted or Downloaded Files. Computers and other electronic storage media allow suspects to delete files to attempt to evade detection or to take other steps designed to frustrate law enforcement searches for information. However, searching authorities can recover computer files or remnants of such files months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. When a person "deletes" a file on a home computer, the data contained in the

- file do not actually disappear; rather, the data remain on the hard drive until they are overwritten by new data. As a result, deleted files, or remnants of deleted files, may reside in free or "slack" space (i.e., in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space) for long periods of time before they are overwritten. A computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve the residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
- e. <u>Search Techniques</u>. Because of the above-described technical requirements, volume of evidence, and the ability of suspects to delete, download, hide and/or obfuscate evidence, the analysis of electronically stored data may necessitate any or all of several different computer forensics techniques. Such techniques may include, but are not limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the pertinent files in order to locate the evidence and instrumentalities authorized for seizure by the warrant); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.
- 5. Based upon my consultation with experts in computer searches, data retrieval from computers and related media, and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I

3 4

5

6 7

8

9 10

11

12

13

14 15

16

17

18

19 20

21

22

23 24

25

26

27 28

know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

- a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them within a reasonable time.
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval. I have been advised by an examiner who has conducted computer searches and data retrieval from computers in a laboratory setting, that such searches can be complex and time consuming. Additionally, I have learned the following information:
- a. Over the last several years, the size of electronic storage media has doubled approximately every 12 months. Inexpensive software capable of "cloning" a computer drive onto a larger hard drive is readily available. As a result, the need for

users to routinely delete items from their hard drives due to a lack of space has all but disappeared. As a consequence, fewer deleted files are being identified relative to the total number of files stored on the computer.

b. Between the increasing complexity of operating systems today and the rich content available on the Internet, the interplay between software applications and the computer operating systems often results in material being stored multiple times and even in different locations in a given piece of computer media without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and sometimes in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it.

THE TARGET PREMISES & SUSPECTED OFFENSES

- 6. The information contained in the Affidavit is made for the purpose of establishing probable cause in support of a search warrant to search and seize the fruits, instrumentalities and evidence of violations of Title 18, United States Code, Section 371 (Conspiracy to Defraud), Title 18, United States Code, Section 1344 (Bank Fraud), and Title 20, United States Code, Section 1097 (Financial Aid Fraud) located on the premises of Crown College, 8739 South Hosmer, Tacoma, Washington 98444, as further described in Attachment B hereto, incorporated herein by reference. The location is more fully described in Attachment A. Based on the information included in this affidavit, there is probable cause to believe that the items described in Attachment B will be found at the location described in Attachment A. Because this Affidavit is submitted for the limited purpose of securing a search warrant, each and every fact known to me concerning this investigation has not been included.
- 7. Crown College is a proprietary school that offers Associate of Science degrees in Criminal Justice, Paralegal Studies, and Business Administration and

2

3

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

- 8. Crown College was accredited on July 1, 1979 by the Accrediting Commission of Career Schools and Colleges of Technology (hereinafter ACCSCT), an independent accrediting agency, as required by ED for participation in its Federal funding programs. Crown College lost its ACCSCT accreditation on July 27, 2007.
- 9. Crown classes are operated almost completely on-line via computer. Crown student's participate in their on-line classes by logging on to "classrooms" they've previously registered for through the school's website. While there are physical classrooms located within the buildings Crown operates, the vast majority of the teaching occurs on-line.
- 10. I know based on my interviews with former employees and students of Crown College and from the investigative efforts of other agents involved, that Crown maintains student records, financial aid data, and school administrative information in computers located in the administrative buildings located at 8739 South Hosmer Street, Tacoma, Washington 98444. I have probable cause to believe that the information sought in Attachment B is located at the location described in Attachment A.

FEDERAL STUDENT ASSISTANCE PROGRAM BACKGROUND

- 11. The Department of Education is a department of the United States Government established to ensure equal access to education and to promote educational excellence throughout the United States. One of the primary responsibilities of ED is oversight of the administration of Title IV Federal Student Assistance (FSA) Programs authorized by the Higher Education Act of 1965. Under the authority of Title 34 of the Code of Federal Regulations (CFR) Parts 600 and 668, ED is responsible for determining the eligibility of institutions to participate in FSA Programs, as well as ensuring that those eligible institutions properly execute their fiduciary responsibilities in administering the programs.
 - 12. Pursuant to 34 CFR 600, to participate in FSA programs, a school must,

21

22 23

24

25 26

- among other requirements, be accredited by a federally recognized accrediting organization also recognized by the Secretary of Education, and must enter into a Program Participation Agreement (PPA) with ED. The school is also required to have been in existence for at least two years. 34 CFR Part 600 further requires that once a school is deemed eligible to participate in FSA programs, it must continually comply with eligibility requirements. If a participating school fails to meet the requirements, it must notify ED within 30 days.
- 13. ED offers a number of financial aid programs to qualified students. To receive Federal Student Aid, a student must be a U.S. citizen or national, or permanent resident of the United States, or a citizen of certain Pacific Islands. Certain other non-citizens are eligible, such as refugees, persons granted asylum, and Cuban-Haitian entrants. Such individuals must provide the school with INS documentation indicating that their intention is to become a U.S. Citizen or permanent resident.
- A student must meet the following criteria to be eligible to receive federal 14. financial aid:
 - Have financial need, except for some loan programs. a.
- Have a high school diploma or a General Education Development b. (GED).
- Be enrolled or accepted for enrollment as a regular student working c. toward a degree or certificate in an eligible program.
 - d. Be a U.S. citizen or an eligible non-citizen.
 - Have a valid Social Security Number. e.
 - f. Make satisfactory academic progress.
- Sign a statement on the Free Application for Federal Student Aid g. (hereinafter FAFSA) certifying that federal student aid will only be used for educational purposes.
- h. Sign a statement on the FAFSA certifying that no federal student loans are in default status and that no money was owed back on a federal student grant.

8

11

17

18

16

19 20

22

23

24

21

25 26

- i. Register with the Selective Service, if required.
- 15. The Federal Pell Grant Program provides gift aid to eligible students in order to assist them with their education. This gift aid is in the form of a grant and is not required to be repaid. Pell Grants are awarded to students who have not yet earned a bachelor or professional degree. Pell Grants are awarded to students who have financial need. The ED program regulations specify eligibility requirements and application procedures for students. The institution and its officers, acting as fiduciary agents, disburse grant payments received for ED to the eligible student beneficiaries.
- 16. Subsidized Stafford Loans are awarded to students who demonstrate financial need. Because the U.S. Department of Education subsidizes the interest, borrowers are not charged interest while they are enrolled in school at least halftime and during grace and deferment periods.
- Unsubsidized Stafford Loans are awarded to students regardless of 17. financial need. Borrowers are responsible for paying the interest that accrues during any period.
- 18. A Parental Loan for Undergraduate Studies (PLUS) allows parents to borrow on behalf of their dependent undergraduate children who are enrolled at least halftime. As with unsubsidized Stafford loans, borrowers are responsible for the interest that accrues on PLUS Loans throughout the life of the loan. Independent students and students whose parents cannot get a PLUS have higher unsubsidized loan limits.
- Consolidation Loans allow any borrower to combine one or more federal education loans into a new Direct Loan or Federal Family Educational Loan (FFEL) to facilitate repayment. The process of consolidating loans usually does not directly involve the school - the consolidating lender purchases qualifying student loans from other lenders and combines them into a single loan.
- 20. The Northwest Education Loan Association (NELA) is a non-profit guaranty agency that works in partnerships with schools, banks, and other lending

institutions to help students continue their education. NELA administers the FFEL Program and guarantees the loans against default.

- 21. Per 34 CFR 685, should a school that was previously approved by ED to participate in Title IV Federal Student Loan programs cease operations, all students currently attending the school who have received Title IV Federal Student Loans will have their loans discharged the loans will be forgiven based on the following conditions:
 - a. The student was enrolled at least 90 days prior to the closure;
- b. The student had not transferred to another school with transferable credits;
- c. The student did not participate in teach-out, a program that allows students attending a school that is in the process of closing to find another educational institution to finish their degrees.

INVESTIGATIVE FINDINGS

- 22. This investigation was initiated based on information provided by Dr. Randi Jones, the former Dean of Academic Affairs at Crown College. Dr. Jones contacted the Washington State Higher Education Coordinating Board (HECB) to pass along her concerns regarding Crown College on March 1, 2007. The HECB referred this matter to The Department of Education Federal Student Assistance Program, who in turn referred it to my office. Dr. Jones began her employment at Crown College in August 2001. In January 2005, she became the Dean of Academic Affairs at Crown College. Dr. Jones terminated her employment at Crown College on February 28, 2007. On April 23, 2007, I interviewed Dr. Jones.
- 23. In late January 2007, Dr. Jones discovered that Crown College staff members, their friends, and significant others were receiving Title IV federal student aid, but were not enrolled at Crown College. Dr. Jones alleged that these individuals took out Stafford loans (Subsidized and Unsubsidized) and Pell Grants without enrolling in school, because the staff members learned that Crown College was on the brink of

- financial insolvency and as such, closure was imminent. Should Crown College go out of business, these individuals believed that their loans would be discharged and they would not have to pay the loans back to the lender. Thus, each of the individuals who had taken out federal loans, but had never enrolled in the school, would get to keep significant amounts of money without any further financial obligations to the government. Ultimately, however, this scheme began to unravel, because the individuals learned that Crown College was not going go out of business, and the individual's loans would not be discharged. These individuals would now have an obligation to pay back their loans, plus any interest accrued.
- 24. In late January 2007, John Wabel (WABEL), the owner of Crown College, and Dr. Jones were staffing the telephones at Crown College. Dr. Jones asked WABEL to show her how to work the computers in the financial aid office and how to handle questions based on the information in the computer. WABEL showed her the Crown College checking account. Dr. Jones stated that, consistent with the scheme described above, the checking account indicated that several Crown College employees and their friends and family received checks from Crown College, but were not enrolled as students. Dr. Jones stated that she immediately knew there was a problem based on the names in the computer. She alleged that when Crown College did not cease operations, these individuals created school documents and files to support their financial aid applications, to make it appear that they had enrolled in classes, to ensure their financial aid disbursements were commensurate with their enrollment and attendance records.
- 25. On or about January 30, 2007, Dr. Jones had a conversation with the Crown College Financial Aid Director, Misty Lee (LEE). According to Dr. Jones, LEE admitted to the existence of the scheme. Dr. Jones instructed LEE to correct the problem and go to the authorities.
- 26. Dr. Jones alleged the following Crown College employees, friends, significant others, and family members were involved in the fraudulent application,

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

\$5,000, and a FFEL Stafford Subsidized loan in the amount of \$5,500, both dated
December 15, 2006, cancelled prior to disbursement. She had a FFEL Stafford
Unsubsidized loan in the amount of \$5,000, and a FFEL Stafford Subsidized loan in the
amount of \$5,500, both dated December 26, 2006, and both fully disbursed on January
4, 2007.

- d. LEE had a FFEL Stafford Unsubsidized loan in the amount of \$5,000, and a FFEL Stafford Subsidized loan in the amount of \$5,500, both dated December 13, 2006, and both fully disbursed on December 26, 2006. She had a Pell Grant in the amount of \$3,200, with only \$1,600 disbursed as of August 24, 2006.
- DOGEAGLE had a FFEL Stafford Unsubsidized loan in the e. amount of \$4,000, and a FFEL Stafford Subsidized loan in the amount of \$2,625, both dated December 13, 2006, and cancelled as of March 5, 2007.
- f S. MCMULLIN had a FFEL Stafford Unsubsidized loan in the amount of \$6,625, dated December 13, 2006, cancelled as of March 3, 2007.
- J. MCMULLIN had a FFEL Stafford Unsubsidized loan in the g. amount of \$10,500, dated December 13, 2006, and fully disbursed on December 26, 2006.
- 28. Dr. Jones indicated that S. MCMULLEN and DOGEAGLE were given the opportunity by WABEL and MULLINEAUX to return the federal student aid that was fraudulently obtained by them. On June 4, 2007, I requested Barbara Wilhelm, Senior Director Claim Review at Sallie Mae to provide a written summary of loan and enrollment information maintained by Sallie Mae for DOGEAGLE. This summary indicated that he had his loans cancelled as of March 5, 2007. On June 26, 2007, Barbara Wilhelm provided a written summary of loan and enrollment information maintained by Sallie Mae for S. MCMULLIN. This summary indicates that S. MCMULLIN had his loans cancelled as of March 5, 2007, and that, according to her records, the loan was either disbursed and the money was later returned or the loan was never disbursed.

- 29. Dr. Jones further stated that LEE'S boyfriend "Jeremy" was never a student at or an employee of Crown College. Likewise, Dr. Jones stated that S. MCMULLIN, J. MCMULLIN's husband, was never a student at or an employee of Crown College.
- 30. On May 7, 2007, I interviewed Angela Rivera-Denny, who was employed at Crown College from 2002 until she was laid off around Christmas 2006. She held various positions at Crown College, to include admissions and academic services as well as the Registrar. Angela Rivera-Denny stated that S. MCMULLIN was not enrolled at Crown College, nor did he work at Crown College. Angela Rivera-Denny further stated that DOGEAGLE, LEE's boyfriend, worked at Crown College for one to two months sometime in early 2003 or 2004. She stated DOGEAGLE was not enrolled at Crown College as a student.
- 31. On June 14, 2007, I interviewed Arthur Rocco, a former Crown College employee who had the responsibility of ordering books and maintaining student files. Arthur Rocco stated that MULLINEAUX's boyfriend, HINTON, was the computer person at Crown College. Arthur Rocco was unsure if HINTON was a student at the school. Arthur Rocco further added that S. MCMULLIN was never a student at Crown College and may currently be a plumber.
- 32. On April 25, 2007, Martina Fernandez-Rosario, a compliance and oversight team leader with the Department of Education Federal Student Assistance Program, provided me with copies of ED FSA's internal program review documents of an ongoing Crown College Title IV program review. A review of these documents in conjunction with a telephone conversation with Martina Fernandez-Rosario indicated that in early December 2006, Crown College, through its owner WABEL, had notified the ACCSCT that Crown College would be preparing for closure because it could not meet its financial obligations. The ACCSCT sent Crown College a letter on December 19, 2006 indicating the impending closure based on conversations with WABEL. On December 20, 2006, ED FSA received a letter from ACCSCT placing Crown College

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

indicates that on October 19, 2006, HINTON electronically signed a request for foreberance on one of his loans, based on his financial hardship. HINTON requested a foreberance of amounts due for 12 months. A review of HINTON's loan history (exclusive of loans and grants taken out in December 2006) in NSLDS indicates that he has two FFEL Consoldiation loans with balances due of \$6,603 and \$8,938. In this same file provided by Sallie Mae, Crown College sent a letter, dated June 17, 2004, to US Bank that indicates Brandon Hinton was a graduate of Crown College and his last day of attendance was June 10, 2004.

A review of HINTON'S financial aid file provided by Sallie Mae

- 34. A review of J. MCMULLIN's financial aid file provided by Sallie Mae identified a letter from Crown College, dated June 29, 2005, to Sallie Mae indicating she was no longer a student at Crown College as of May 19, 2005.
- 35. A review of DOGEAGLE's financial aid file provided by Sallie Mae indicates that DOGEAGLE used HINTON as a personal reference on a Stafford Loan Master Promissory Note.
- 36. A review of LEE's financial aid file provided by Sallie Mae indicates that LEE used DOGEAGLE as a cosignor on a Sallie Mae Signature Student Loan (private non-Title IV loan).
- 37. A review of BYER'S financial aid file provided by Sallie Mae indicates that BYER's used LEE as a personal reference on a Stafford Loan Master Promissory Note.
- 38. A review of MULLINEAUX's financial aid file provided by Sallie Mae indicates that MULLINEAUX used HINTON as a personal reference on a Stafford Loan Master Promissory Note and a Sallie Mae Signature Student Loan (private non-Title IV loan).
- 39. Based on the above facts, I believe there is probable cause for the issuance of a search warrant to seize and view the fruits, instrumentalities and evidence

1	of violations of Title 18, United States Code, Section 371 (Conspiracy to Defraud),
2	Title 18, United States Code, Section 1344 (Bank Fraud), and Title 20, United States
3	Code, Section 1097 (Financial Aid Fraud) located in the target premises of Crown
4	College, 8739 South Hosmer, Tacoma, WA 98444.
5	A Company of the Comp
6	ADAM M. SHANEDLING, Affiant
7	Special Agent United States Dept. of Education
8	17
9	SUBSCRIBED AND SWORN to before me this day of July, 2007.
10	\mathcal{M}_{α} \mathcal{M}_{α} \mathcal{M}_{α} \mathcal{M}_{α}
11	MARY ALICE THEILER
12	United States Magistrate Judge
13	
14	
15	
16	·
17	
18	
19	
20	
21	• · · · · · · · · · · · · · · · · · · ·
22	
23	
24	
25	
26	
27	
28	