APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

STATE OF NEVADA)

SS:

COUNTY OF CLARK)

Now comes Colin Haynes, Criminal Investigator III with the Nevada Secretary of State being first sworn, deposes and states, under penalty of perjury, that I am the affiant herein and that the following assertions are true and accurate to the best of my knowledge.

This affidavit is made of my own personal knowledge except where stated on information and belief, and as to those matters, I believe them to be true and if called as a witness, I could competently testify thereto.

I am a Criminal Investigator III with the State of Nevada, Office of the Secretary of State ("SOS"). I have been assigned to the SOS for approximately one (1) year. Prior to my employment with the SOS, I was employed as an investigator with the Office of the Attorney General for three (3) years and six (6) months, assigned to the Bureau of Consumer Protection and Medicaid Fraud Control Unit.

Prior to my employment with the Attorney General's Office, I worked as an investigator with Las Vegas Metropolitan Police Department assigned to investigate Elder Financial Exploitation for a period of five (5) years and six (6) months. I also have eleven (11) years experience working as a police officer in London, England, assigned to patrol, field training and intelligence divisions.

In addition to my experience investigating complex financial crimes, I have attended NASAA investigator training courses and the Financial Investigations Practical Skills Training hosted by the National White Collar Crime Center and Research Institute where I learned investigative skills pertaining to Securities Fraud and other financial crimes. In 2004 I successfully completed the requirements for Peace Officer Category II Basic Certification, which included 276 hours of instruction. I also have the Intermediate and Advanced Peace Officer certificates from the State of Nevada and I am a Certified Fraud Examiner through the National Association of Certified Fraud Examiners. During my career as a law enforcement officer and

criminal investigator I have assisted in the planning, preparation and execution of numerous search and seizure warrants.

The Secretary of State has jurisdiction over enforcement of the Nevada Election laws contained in NRS 293.

In support of the assertions to constitute the existence of probable cause for the requested warrant, the following facts are offered:

I. DESCRIPTION OF LOCATION TO BE SEARCHED

Probable cause exists to believe that certain property hereinafter described will be found at the following premise, to-wit:

The office of Association for Community Reform Now (ACORN), located at 953 E. Sahara Ave, building D suite 201, Las Vegas, NV 89109. The building is a two storey, building located on the south west corner of the parking lot of Commercial Center, a development of commercial buildings and offices. The front of building D is clearly marked with the words "Commercial Arts Building" and the number "953" across the front fascia of the building above the main door. The main door is on the east side of the building facing into the parking lot, with the rear of the building on State Street. The roof of the building is a distinctive split level two-tone tile. The building contains a number of different offices and companies, many of which have their name on banners across the front of the building. The building has a small access road running to the north of it connecting the parking lot to State Street.

Based on surveillance of the building and prior investigative activities, ACORN are known to have been using an office located on the second floor at the northwest corner of the building. The entrance to this individual office is identified from the corridor only by the number "201" on a plate on the door. To the east of the office door is a stairway that leads out to the small access road on the east side of the building connecting the parking lot and State Street. This office was used for all activities of ACORN, including recruitment and training of staff, storage of documents and all computers used in connection with the activities described in the attached affidavit.

New information was obtained on October 6 2008 indicting that ACORN has now acquired an office located in the same building on the first floor, identified as office D18. This office has it's front entrance on the east side of the building, facing east. ACORN have placed

banners above the door way to office D18 announcing their occupancy. Office D18 is two doors to the south of the main entrance. The windows to this office have a blue tint on them.

Until this date all indication was that ACORN operated exclusively from suite 201. No credible information has been obtained to support that ACORN have moved all of their documentation from suite 201 to D18. No new tenant has been seen in suite 201 and it is believed that ACORN still has possession and control of suite 201.

II. DESCRIPTION OF PROPERTY TO BE SEIZED

The property referred to and sought to be seized consists of the following:

- 1. Any and all documents and records, whether hard copy or digital media, pertaining to the hiring, ongoing employment and termination of employment for all staff, including canvassers, supervisors, team leaders, political organizers and managers, involved in the gathering, handling, recording, reviewing and submission of Voter Registration Application forms in the county of Clark, State of Nevada. Documents to include applications for employment, employment agreements or contracts, employee transmittal forms, affirmations, W4's, INS form I9's, disciplinary files, complaints and investigations, termination records, letters relating to resignation, performance evaluations, time sheets, payroll records.
- 2. Any and all Voter Registration Applications gathered by or submitted to ACORN from any source, including electronic copies of said forms.
- Any and all databases populated with the information contained on any Voter Registration Application forms, or databases containing any data extracted from said forms.
- 4. Any and all internal quality control or verification documentation or files pertaining to the recording, storage or review and verification of any Voter Registration Forms, including Problematic Card Cover Sheets, Performance Investigation Sheets, Worker Batch Sheets.

- Any and all orientation, training or instructional materials used in the hiring and training of staff to work as voter registration canvassers, supervisors, team leaders and political organizers.
- 6. Any and all documents and records, to include information stored in computers, more specifically described in items one (1) through five (5) which may contain or reveal the identities of the persons responsible for the illegal activities described within the attached Affidavit; and
- Tape recordings, notes, correspondence, voter databases, computers and disks, facsimile messages, or any similar data compilation pertaining to the collection of Voter Registration Application forms; and
- 8. Limited items of personal and business property which would tend to establish a possessory interest in the items seized pursuant to this warrant and tend to establish occupancy and/or ownership of the premises described above, including but not limited to, lease agreements, utility and telephone bills, keys and personal items such as photographs or addressed envelopes; and
- 9. Computers and/or databases including, but not limited to: Computer equipment, including any electronic devices which are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (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 and diskettes, tape drives and tapes, optical storage devices, and other memory storage devices); and
- 10. Peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as 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); as well as any devices, mechanisms,

or parts that can be used to restrict access to such hardware (such as physical keys and locks); and

- 11. Information, instructions, programs, or program code, stored in the form of electronic, magnetic, optical, or other media which are capable of being interpreted by a computer or its related components, data, data fragments or control characters integral to the operation of computer software, operating system software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended for use to communicate with computer components; and
- 12. Any written, recorded, printed or electronically stored material which explains or illustrates the configuration or use of any seized hardware, software, or related item; and
- 13. Devices, programs, or data—whether themselves in the nature of hardware or software—that can be used or is designed for use to restrict access to or facilitate concealment of any computer hardware, computer software, computer-related documentation, electronic data, records, documents or materials within the scope of this application, any data security hardware (such as any encryption devices, chips and circuit boards), passwords, data security software or information (such as test keys and encryption codes), and similar information that is required to access computer programs or data or to otherwise render programs or data into a useable form; and
- 14. Any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment. This media includes but is not limited to any fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices; and
- 15. Any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs), or any information on an

electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks), as well as printouts or readouts from any magnetic storage device; and

- 16. Any and all communications previously received or transmitted, or prepared in contemplation of transmission, including electronic mail or data associated with electronic bulletin board systems, stored on any of the electronic media named above. All electronic communications, including those previously received or transmitted, or held in temporary, intermediate storage incident to transmission, documents, and materials, including those used to facilitate communications, as used above shall include any and all communications, previously received, transmitted, or stored, or prepared in contemplation of transmission, including electronic mail or data associated with electronic bulletin board systems, whether stored on any of the electronic media named above or held in temporary, intermediate storage incident to transmission to the individuals or premises within the scope of this application; and
- 17. Any and all electronic information or electronic data, stored in any form, which is used or has been prepared for use either for periodic or random back-up (whether deliberate or inadvertent, or automatically or manually initiated), of any computer or computer system, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes, and other media capable of storing magnetic or optical coding; and
- 18. Such electronic data in the form of electronic records, documents, and materials, including those used to facilitate communications; and
- 19. Computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer; and
- 20. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, Bernoulli drives, etc.), stored data; and
- 21. "Hidden," erased, compressed, password-protected, or encrypted files; and

- 22. "Mainframe" computers, or "micro" or "personal" computers, either standing alone or joined through a series of connected computers called a "network"; and
- 23. All magnetic storage devices as well as the central processing units (CPUs) and applicable keyboards and monitors which are an integral part of the processing unit; and various file "directories" and the individual files they contain, recently deleted data; scanning storage areas for deliberately hidden files; and
- 24. The above items to be seized, in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications, may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs), or any information on an electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks), as well as printouts or readouts from any magnetic storage device; and
- 25. The above items to be seized shall include any and all communications previously received or transmitted, or prepared in contemplation of transmission, including electronic mail or data associated with electronic bulletin board systems, stored on any of the electronic media named above. All electronic communications, including those previously received or transmitted, or held in temporary, intermediate storage incident to transmission. The terms "records, documents, and materials, including those used to facilitate communications" as used above shall include any and all communications, previously received, transmitted, or stored, or prepared in contemplation of transmission, including electronic mail or data associated with electronic bulletin board systems, whether stored on any of the electronic media named above or held in temporary, intermediate storage incident to transmission to the individuals or premises within the

scope of this application. Because such communications are believed to have been used to facilitate the commission of the offences of Voter Registration Fraud and Offering False Instrument for filing or recording by multiple parties as yet unknown, probable cause exists to search such communications as property that constitutes evidence of the commission of a criminal offense; and

- 26. The above items to be seized shall also be read to include any and all electronic information or electronic data, stored in any form, which is used or has been prepared for use either for periodic or random back-up (whether deliberate or inadvertent, or automatically or manually initiated), of any computer or computer system. The form such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes, and other media capable of storing magnetic or optical coding; and
- 27. Such electronic data in the form of electronic records, documents, and materials, including those used to facilitate communications constitutes evidence of the commission of a criminal offense. These materials are therefore subject to seizure pursuant to NRS 179.035 and/or NRS 179.1164/65, and the devices used to store or facilitate storage of such materials may be retained as evidence in the commission of a crime for a reasonable period of time and may be examined, analyzed, and tested for a reasonable period of time as evidence in the commission of a crime; and
- 28. Based upon affiant's knowledge, training and experience, and consultations with CHRIS DEFONSEKA, Computer Network Specialist I, who has been specially trained in the seizure of computers and how computer operating systems function and store data, affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, to insure accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that some computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate

such a computer be seized and subsequently processed by a qualified computer specialist in a laboratory setting. This is true because of the following:

- A) The volume of evidence. Computer storage devices (such as hard disks, diskettes, tapes, laser disks, Bernoulli drives, etc.) can store the equivalent of thousands of pages of information. Additionally, a user may seek to conceal criminal evidence by storing it in random order with deceptive file names. Searching authorities are thus required to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. 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 analysis "on-site."
- B) Technical requirements. Analyzing 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. Thus it is difficult to know prior to the search which expert possesses sufficient specialized skills to best analyze the system and its data. No matter which system is used, however, data analysis protocols are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Due to the volume of the data at issue and the technical requirements set forth above, it is usually necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. It may be the case, however, under appropriate circumstances that some

types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such---or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively analyzed off site, with due consideration given to preserving the integrity of the evidence. This, in turn, is often dependent upon the nature of the criminal offenses. These computers are likely to take the form either of "mainframe" computers, or "micro" or "personal" computers, either standing alone or joined through a series of connected computers called a "network".

Computers recognized in the computer trade as "mainframe" computers share the characteristic that they are physically large pieces of equipment designed to process and store large amounts of data. Such computers often are designed to facilitate usage by more than one individual at a time, often servicing a number of users at any of several remote locations. Because of these characteristics, physical removal of mainframe-types of computers is often impractical, thus necessitating that investigators analyze these computers on-site to seize pertinent data. Thus a presumption exists that such computers will be analyzed and pertinent data seized from them, by investigators working on the subject premises.

Computers recognized in the computer trade as "micro" or "personal" computers share the characteristic that they are often substantially smaller devices, often capable of being stored on or in a single desk or station. While the storage capabilities of such devices vary, micro or personal computers are more often designed to facilitate usage by a single individual. Because of these characteristics, physical removal of micro or personal computers is often the more practical alternative, and is often less intrusive than requiring investigators to remain at the premises for the amount of time reasonably required to review, analyze, and copy pertinent data. Thus a presumption exists that such computers will be seized and subsequently processed by a qualified computer specialist in a laboratory setting for reasons set forth above.

Based upon affiant's knowledge, training, and experience, and the experience of other law enforcement personnel, affiant knows that searches and seizures of evidence from computers taken from the subject premises commonly require agents to seize most or all of a computer system's input/output peripheral devices for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the subject premises, and in order to fully retrieve data from a computer system, investigators must seize all magnetic storage devices as well as the central processing units (CPUs) and applicable keyboards and monitors, which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, such materials and/or equipment will be returned within a reasonable time.

The analysis of electronically stored data, whether performed on site or in a laboratory or other controlled environment may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "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; or performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

III. PROBABLE CAUSE SUPPORTING SEARCH AND SEIZURE WARRANT

The property herein described constitutes evidence which tends to demonstrate that the criminal offenses of Offering False Instrument for Filing or Recording, in violation of NRS 239.330, Acts Concerning Registration of Voters, in violation of NRS 293.800 (1), Prohibited Acts of Field Registrars, Employees of Voter Registration Agencies or Persons Assisting Voters, in violation of NRS 293.505 (12) and Obtaining and using personal identifying information of

another person to harm or impersonate person, to obtain certain nonpublic records or for other unlawful purpose in violation of NRS 205.463 have been committed since March 2008 and continue to be committed and/or constitute instrumentalities of said criminal offenses.

Based upon my investigation, I assert that probable cause exists to believe that employees of Association for Community Reform Now (ACORN), while employed to solicit members of the public to complete Voter Registration Applications, have themselves completed forms using fictitious and false information and submitted those forms to ACORN, along with legitimately gathered forms, knowing that those fraudulent forms will be forwarded to the Clark County Registrar for filing as an official voting record.

This investigation started on July 2, 2008 when Larry Lomax (LOMAX), Clark County Registrar of Voters reported to the DIVISION that his office had received a significant number of suspicious Voter Registration Applications Forms from ACORN. LOMAX reported that organizations, such as ACORN, that wish to assist individuals to register to vote can obtain Voter Registration Application Forms from his office in bulk. In order to obtain bulk applications, organizations have to submit to the county a Plan of Distribution providing brief details of their intentions. When bulk applications are supplied to these organizations the serial number of each application is recorded by the county so that forms that are completed and returned to the county can be linked to specific distribution locations or organizations.

LOMAX reported that his staff had identified a significant number of applications being returned by ACORN over the last several months on which one or more of the following problems were identified:

• Multiple applications were being received that contained the same name, address and personal identifiers. These applications were being received within days of each other, suggesting that one Voter Registration Application form was being duplicated and submitted multiple times. The writing on each application frequently appeared to be different.

 Many applications contained addresses that, according to the US Postal Service and County Assessors records, did not exist, or if the street did exist, the house number range did not exist on that street.

• Many applications were being received containing personal identifying information that did not match the records of Nevada Department of Motor Vehicles or the Social Security Administration, indicating that the identifiers may be false. When this fact was combined with a false address being recorded on the form, this was strongly suggestive of fraudulent applications being made in the name of non-existent people.

Based upon this information the DIVISION opened an investigation on July 2, 2008. On or around July 18, 2008, a meeting took place between Brian Wade (WADE), legal counsel for ACORN, Chris Edwards (EDWARDS), Director of the ACORN Las Vegas office, two ACORN employees who gave their names as Ali Cochran (COCHRAN) and Jo (last name unknown), Larry Lomax (LOMAX), Clark County Registrar and a representative of the SOS, Chris Lee (LEE), Deputy Secretary of State for Southern Nevada. At this meeting Jo identified himself as the director of quality control for the Las Vegas office of ACORN and he explained that he had established a computer database into which all of the data from the Voter Registration Application forms was being input and stored. This enabled him to identify any forms that were turned in by ACORN canvassers that contained information that was duplicated on any other form. Jo claimed that ACORN was terminating approximately ten canvassers per week for turning in duplicate and suspicious forms.

WADE advised that ACORN had identified several egregious cases of canvassers turning in fraudulent forms, including one case in which a canvasser was caught completing forms using names and addresses copied from the telephone book. WADE stated that ACORN would be willing to provide such information and supporting documentation to the county for further investigation.

On or around August 7, 2008, at the request of LOMAX, ACORN provided copies of Problematic Card Cover Sheets, Performance Investigation Sheets, Worker Batch Sheets and copies of Voter Registration Applications for thirty three (33) ex-employees of ACORN who

had been terminated after suspicious Voter Registration Applications were identified through ACORN'S internal quality control process. These packages of documents were forwarded to the DIVISION for examination.

On September 12, 2008, I contacted Brian Mellor (MELLOR), another legal counsel for ACORN. I identified fifteen (15) of the ex-employees that ACORN had included in the documents they provided, and I requested additional information pertaining to these individuals. During the course of this discussion, MELLOR advised me that the procedure within ACORN was to scan the completed Voter Registration Application forms and save a digital copy of each form on a computer. The original forms were then delivered to Clark County Registrar of Voters. MELLOR also confirmed that the database and documentation being maintained by ACORN enabled the management to identify which forms had been collected by which canvasser.

I began my examination of the packages provided by ACORN by selecting all of the documents pertaining to one of the ex-employees, identified in the documentation as Darmela Jones (JONES). These documents consisted of copies of seventeen (17) Voter Registration Application forms identified by ACORN as being turned in to them by JONES. The internal process followed by ACORN required that they document the serial numbers of all forms provided to each canvasser when the canvasser booked forms out each day and when they returned the forms at the end of each day. By this method the management at ACORN was able to identify which forms were submitted by which canvasser.

I researched the addresses listed on each of the Voter Registration Application forms turned in by JONES to determine if the addresses existed in the Clark County area. I used the database of the Clark County Assessor along with commercially available mapping databases, including MapQuest and Google Earth. I also visited those addresses for which the street name existed but the number range appeared incorrect. I found that of the fifteen (15) readable addresses on these forms, only four (4) were real addresses. Eleven (11) of these addresses simply did not exist, or, if the street existed, there was no such number on that street. Two (2) of the addresses on the Voter Registration Applications were unreadable.

I then researched the registrant names, dates of birth and partial (last four digits) social security numbers on each form submitted by JONES. I checked this information through the records of the Nevada Department of Motor Vehicles, through the records of Las Vegas Metropolitan Police Department (SCOPE), and through county records such as Assessor's records and business license. I also checked these personal identifiers through the state criminal history repository and conducted driving license searches in other states. I also checked to see if the identifying information contained in each form had been input into the Clark County or State of Nevada voter registration databases. Through this process I determined that fourteen (14) of the individuals identified in these applications had no record of existing in the State of Nevada.

I performed the same research on all of the Voter Registration Applications provided by ACORN for two more ex-employees. I found similar results for each of these employees, with a total of thirty one (31) non-existent addresses out of fifty two (52) readable listed addresses and forty one (41) names showing no record of a person with those identifiers out of fifty six (56) names listed.

On September 30, 2008, I located and interviewed Darmela Jones (JONES). During this interview JONES confirmed that she had been employed by ACORN as a canvasser for about one month from June 2008. When confronted with the results of the analysis of the Voter Registration Applications submitted by JONES to ACORN, JONES admitted that she had submitted a significant number of applications that she knew to be false. JONES stated that she submitted approximately forty (40) Voter Registration Applications while employed at ACORN and of those only ten (10) were real applications collected from different members of the public. JONES stated that ACORN required her to obtain 20 completed Voter Registration Applications during each day that she worked, and she was finding it very difficult to meet this target. JONES also stated that it was very hot outside while she was trying to get people to complete a form. JONES stated that many people that she approached would not complete a form.

JONES stated that as a result, she began asking people who had agreed to complete a form if they would be willing to fill out additional forms for other people. JONES stated that some people agreed to do this and they filled out multiple forms in different names and handed the signed forms back to her. She then submitted these forms to ACORN, representing that they were legitimate Voter Registration Applications when she knew that they were fake. JONES stated that she was eventually confronted about some of her forms by one of the managers of ACORN who JONES knew only as Elisha. JONES quit ACORN when she was confronted about the fictitious forms.

On October 2, 2008, I attempted to locate a second canvasser who had been terminated from ACORN. The address for this canvasser, Richard Rivera (RIVERA) was the Casa Grande Transitional Housing Facility of the Nevada Department of Corrections located at 3955 W. Russell Road, Las Vegas. Upon contacting staff at this facility I learned that this facility housed convicted felons who were eligible for work release programs.

Nevada Department of Corrections contracts with a private company, Choices Group Inc. to handle the work services programs offered to the inmates at this facility. Dave Wonnacott (WONNACOTT), Re-Entry Services Administrator for Choices Group Inc. provided the following information:

On March 5, 2008, one of the inmates advised Choice Group Inc. staff that he had secured a job with ACORN working as a canvasser. In this capacity he was to approach members of the public and ask them to register to vote by completing a Voter Registration Application. This inmate advised Choices Group Inc. that ACORN was looking to hire a lot of temporary staff. A member of Choices Group Inc. staff contacted Chris Edwards (EDWARDS), the Director of ACORN Las Vegas office and discussed placing the inmates in employment with ACORN. During this process it was made clear to ACORN that the individuals they would be hiring were convicted felons serving sentences in a Nevada Department of Corrections facility. EDWARDS was required to agree to all of the conditions of employment that were set by Nevada Department of Corrections for inmates on work release, which included such things as constant supervision and no access to telephones or

internet. Based on the level of discussion and involvement with Choices Group Inc. it is clear that EDWARDS understood that ACORN would be hiring inmates for this position.

According to the records of Choice Group Inc. and Nevada Department of Corrections a total of fifty nine (59) inmates worked for ACORN between March 5, 2008 and July 31, 2008. On July 31, 2008 all inmates were withdrawn from this employment. Some of these inmates worked for only one or two days, while some remained employed by ACORN for several months.

On October 3 2008, I interviewed another ex-employee of ACORN, Jason Anderson (ANDERSON). ANDERSON worked for ACORN from May 7, 2008 to July 31, 2008, while he was an inmate at Casa Grande. By the time ANDERSON was withdrawn from this employment he was in a supervisory position as a team leader. ANDERSON confirmed that ACORN was receiving large numbers of fictitious applications submitted by some of the employees. ANDERSON stated that ACORN had established a verification system that included calling phone numbers listed on the applications and looking for duplicate applications. ANDERSON also confirmed that many canvassers were terminated by ACORN when it was discovered that they had submitted fictitious applications. ANDERSON described that some of the canvassers hired by ACORN were "lazy crack-heads" who were not interested in working and just wanted the money.

ANDERSON confirmed that canvassers were required to collect twenty (20) completed forms each shift, but it was more normal that they would bring in eight (8) to twelve (12). ANDERSON stated that if a canvasser's number dropped down less than this, they would be put on probation and terminated if they did not improve.

ANDERSON described that he even saw one of the canvassers submit Voter Registration Applications using the names of famous football players from a Texas team. ANDERSON stated that he was not sure that these forms were ever sent to Clark County Registrar as required by law.

In addition to the investigative activities described above, I obtained samples of suspicious Voter Registration Applications that Clark County Elections staff had identified

through their own review process. I was provided with one hundred and eighty-three (183) files, each identified by a different voter name. In most of these files there were multiple applications containing the same name and personal identifying information; all of which had been submitted by ACORN. In examining the individual application forms it was not possible to determine which employee of ACORN had gathered or submitted the applications.

Between August 8, 2008 and August 30, 2008 I attempted to locate a number of the people whose identifying information appeared on these forms. On August 14, 2008, I located and interviewed Diceona Green (GREEN). GREEN was shown two (2) Voter Registration Applications that contained her name, address and personal identifying information and had been submitted to Clark County by ACORN. Two of these forms were dated between April 3, 2008 and April 30, 2008. GREEN stated that she had completed only one of those two (2) forms after she was approached by a person at the Downtown Transportation Center. GREEN stated that she did not complete the other form.

On August 18, 2008, I located and interviewed Roberta Casteel (CASTEEL). CASTEEL was shown two (2) Voter Registration Application forms that had been submitted to Clark County by ACORN. These forms contained the name, address and personal identifying information of CASTEEL, including her driving license number on one and a partial social security number on the other. CASTEEL stated that she did not fill out these forms. She stated that in February 2007 she had her purse stolen. Her purse contained her driving license and all the information on that driving license was an exact match to the information on these Voter Registration Applications.

On August 18, 2008, I located and interviewed Areanna Carter (CARTER). CARTER was shown six (6) Voter Registration Application forms that had been submitted to Clark County by ACORN. These forms contained the name, address and personal identifying information of CARTER and were all dated between February 28, 2008 and June 28, 2008. CARTER stated that she completed two (2) of these forms. She was approached by a person outside a DMV office and she agreed to complete a Voter Registration Application form to register to vote. She then changed her address a few months later and was approached

again by a different person. She filled out a second form to notify the elections department of her change of address. CARTER stated that she did not complete the other four (4) forms.

On August 20, 2008, I obtained a statement from Darryl Bension (BENSION). BENSION was shown one (1) Voter Registration Applications that contained his name, address and had been submitted to Clark County by ACORN. The form was dated June 6, 2008. BENSION stated that he did not complete this form and that the personal identifying information on the form, such as date of birth and partial social security number, were not his.

Based upon the evidence gathered during the course of this investigation, I believe there is sufficient probable cause to support that the records and databases in the possession and control of ACORN, as described in more detail in section II of this affidavit, are located at the premises described in more detail in section I of this affidavit, and that these records and databases constitute evidence which tends to demonstrate that the criminal offenses of Offering False Instrument for Filing or Recording, in violation of NRS 239.330, Acts Concerning Registration of Voters, in violation of NRS 293.800 (1), Prohibited Acts of Field Registrars, Employees of Voter Registration Agencies or Persons Assisting Voters, in violation of NRS 293.505 (12) and Obtaining and using personal identifying information of another person to harm or impersonate person, to obtain certain nonpublic records or for other unlawful purpose in violation of NRS 205.463 have been committed since March 2008 and continue to be committed and/or constitute instrumentalities of said criminal offenses.

Wherefore, I request that a search and seizure warrant be issued directing a search for and seizure of the aforementioned items at the premises set forth herein.

Wherefore, based on the above stated good cause, I request that search and seizure warrants be executed between 7:00 am and 7:00 pm at the aforementioned premises set forth herein.

Colin Haynes, Criminal Investigator III Secretary of State Securities Division

SUBSCRIBED and SWORN to before me this _______

_ day of (

2008.