

82. On February 28, 2008, ICE agents received additional social security "no match" information from the SSA for an additional 22 Agriprocessors employees suspected of using invalid social security numbers or social security numbers belonging to other real people. These 22 employees were all reported as having earned wages while working at Agriprocessors during the fourth quarter of 2007. All 22 employees were reported by SSA to either have used invalid social security numbers or social security numbers assigned to names of other people.
83. Based on the "no match" information received from the SSA for social security numbers used by Agriprocessors employees during the third and fourth quarters of 2007, about 737 current Agriprocessors employees are believed to be using a social security number not lawfully issued to that person. Due to the turnover in the Agriprocessors work force, the exact number of employees varies somewhat from quarter to quarter. The 737 fourth-quarter employees include about 147 using social security numbers confirmed by the SSA as being invalid social security numbers (never issued to a person) and about 590 using valid social security numbers, however the numbers did not match the name of the employee reported by Agriprocessors as having used that number during employment.

#### OTHER EVIDENCE

84. ICE agents used the Accurint database to further research the validity of the social security numbers used by Agriprocessors employees. Accurint is a web-based application tool available to law enforcement personnel for the purpose of searching for identity information, address location, financial records, property information, business listings, employment records, phone information, and other identifying information. Accurint uses a proprietary data-linking technology to gather the search results via more than 100,000 different public records and non-public information sources to aid in fraud detection and identity solutions. This includes such sources as Department of Motor Vehicles, County Assessor's Office, and private credit reporting entities. For example, if a social security number is

placed in the appropriate block of the search information that is queried for a person, then a name, or a list of names, for the person or persons who have previously used that social security number, and their address and telephone number (if available), will be shown. If there is no name associated with that social security card, or if that person is known to be deceased, then that will be reflected as well.

85. A request from ICE Special Agents to the IWD for an Employer's Contribution and Payroll Report Form 65-5300 (hereinafter "Payroll Report") for the 2<sup>nd</sup> Quarter of 2007 (April, May, and June of 2007) for Agriprocessors revealed there were 1,116 employees reflected as receiving wages for that time period. A search was conducted by ICE agents in the Accurant database for the individual social security numbers listed in the 2<sup>nd</sup> Quarter 2007 Payroll Report. This search revealed that approximately 878 out of 1,116 (78.6%) of the social security numbers input into Accurant either did not appear to be associated with the person assigned to that social security number or the number did not reveal any person associated with that number. This analysis would not account for the possibility that a person may have falsely used the identity of an actual person's name and Social Security Number. In my training and expertise, I know it is not uncommon for aliens to purchase identity documents which include Social Security Numbers that match the name assigned to the number.
86. ICE Special Agents conducted a search by social security number of the Federal Trade Commission's (hereinafter "FTC") Consumer Sentinel Network database that is used for reporting incidents of identity theft. The search revealed that a person who was assigned one of the social security numbers being used by an employee of Agriprocessors has reported his/her identity being stolen.
87. A request from ICE Special Agents to the IWD for a Payroll Report for the 3rd Quarter of 2007 (July, August, and September of 2007) for Agriprocessors revealed there were 1,063 employees reflected as

receiving wages for that time period. A search was conducted by ICE agents in the Accurint database for the 109 new employees whose additional social security numbers were listed in the 3rd Quarter 2007 Payroll Report. This search revealed that approximately 83 out of 109 (76%) of the social security numbers input into Accurint either did not appear to be associated with the person assigned to that social security number or the number did not reveal any person associated with that number. The previous 2<sup>nd</sup> quarter IWD Payroll Report of persons who had left employment showed that, based on the previous Accurint queries, 126 out of 162 (77%) had what appeared to be discrepancies. This left a total of 835 of the current 1063 employees (78.5%) as having discrepancies based on Accurint checks. A search by social security number of the 109 new employees was conducted in the FTC's Consumer Sentinel Network database did not reveal any person reporting his/her identity as being fraudulently used by an unknown party.

88. On February 20, 2008, ICE Special Agents in Cedar Rapids received a copy of the 2007 fourth quarter Payroll Report for Agriprocessors from IWD. The fourth quarter payroll report reflects the names and social security numbers reported by the company for employees who earned wages during the months of October, November, and December of 2007. A review of this report revealed that the company reported paying wages to a total of 968 employees during the fourth quarter of 2007. An analysis of the report by ICE agents showed that 52 new employees at Agriprocessors were paid during the fourth quarter that were not recorded as having been paid on the Payroll Report for the third quarter of 2007. Accurint law enforcement record checks revealed that approximately 22 of the 52 (42%) newly reported social security numbers used by employees of Agriprocessors either related to a real person's name that did not match the name listed on the payroll report, or the Accurint checks did not reveal any information relating to that social security number. Based on a comparison of the third and fourth quarter payroll reports for

Agriprocessors, and the Accurint law enforcement record checks, it appears that approximately 99 of the 148 (67%) employees who were reported on the 2007 third quarter report, but not reflected on the 2007 fourth quarter report, had social security number discrepancies. Thus, according to the reviews of the third and fourth quarter payroll reports combined, approximately 737 of the fourth quarter employees reported by Agriprocessors appear to have social security number discrepancies.

89. A comparison was made of the May 5, 2006, EDCOR letter sent from SSA to Agriprocessors to the combined "no match" information from February 20, 2008, and February 28, 2008, that was received from SSA and derived from both the third and fourth quarter Agriprocessors Payroll Reports. This analysis revealed that approximately 141 of the social security numbers were shown as still being actively used by employees at Agriprocessors.

#### **SUMMARY OF UNLAWFUL EMPLOYMENT INFORMATION**

90. It appears that based on:
- a. The apprehensions in the years of 2004 through 2007 by ICE Special Agents of known criminal offenders, the majority of whom were later prosecuted in federal district court for their use of fraudulent documents, and who have stated that their employer was Agriprocessors;
  - b. The EDCOR correspondence that shows that Agriprocessors has repeatedly been made aware that large numbers of its employees were using social security numbers that have discrepancies for each tax year from 2000 to 2005;
  - c. The indices checks conducted by ICE employees in commercial and government databases, and the IWD Payroll Reports for 2007, reflect discrepancies between the name attributed to each social security number in those databases and the working name and the social security number used for employment at Agriprocessors; and,

- d. Based on information thus far developed in this investigation, it appears, based on 2007 fourth quarter payroll reports, that approximately 76% of the 968 employees of Agriprocessors were using false or fraudulent social security numbers in connection with their employment,

That there is probable cause to believe that (a large percentage approximately 76% as of the 4<sup>th</sup> Quarter 2007) of the total workforce reported to IWD, nearly all of which appear to be Agriprocessors floor workers, used fraudulent documents or documents with social security or other identification numbers that were lawfully issued to others, or not issued at all, and are currently employed unlawfully by Agriprocessors. In addition, there is probable cause to believe there may be some Agriprocessors employees paid in cash who are not reported to IWD, and who are currently employed illegally without valid documents.

#### **HARBORING RELATED TO VEHICLE TITLE AND REGISTRATION FRAUD**

91. The United States Postal Inspection Service ("USPIS"), the Federal Bureau of Investigation ("FBI"), and the Iowa Department of Transportation ("DOT") have investigated possible document fraud involving the titles and registration of vehicles used by employees of Agriprocessors. The following is based on information provided to your affiant by these agencies.
92. In September 2005, the DOT began investigating reports of questionable title transactions between Des Moines and Allamakee Counties. Burlington is the County Seat for Des Moines County and Postville is located in Allamakee County. The suspect applicants showed addresses in Burlington, Iowa, but registration renewals were repeatedly made in Allamakee County.
93. A DOT Investigator who spent time in the Postville area noted a high number of license plates from Des Moines County. From time to time, the Investigator had involvement with vehicles in the Postville area during traffic stops made while working formerly as a Postville Reserve Police

Officer. The DOT Investigator also reviewed vehicle title transactions as a DOT Investigator. The majority of the vehicles showed Des Moines County addresses on the registration and title information despite the vehicles consistently remaining in Postville, even after ownership changed. The Agriprocessors facility contains a parking lot for employees. By driving into Postville and going through the parking lot at Agriprocessors, the DOT Investigator was able to determine that a large number of the vehicles in question appeared to be driven by employees of Agriprocessors and parked in the company parking lot during the employees' shifts.

94. The DOT Investigator was aware that a supervisor at Agriprocessors was connected with the sales of vehicles. On at least one occasion, the supervisor had retrieved or attempted to retrieve vehicles from impoundment at the Postville Police Department on behalf of another Agriprocessors employee. A number of the vehicles appeared to have a link to a car dealership located in Cedar Rapids, Iowa ("Dealership").
95. In October 2005, DOT Investigators audited the Dealership. The managers of the Dealership stated that the Agriprocessors' supervisor ("C") was a personal friend of theirs. They stated they had been selling a large volume of cars through the Agriprocessors' supervisor to people in the Postville area. The Dealership managers had supplied vehicles directly to the Agriprocessors supervisor for resale in Postville, in violation of Iowa law, which requires all vehicle dealers be licensed. In the year 2005, more than 50 vehicles were sold to people in the Postville area. According to the DOT Investigator, sales to Postville residents appeared to represent approximately 90% of the business for the Dealership. In many cases, the dealership's files contained copies of the ultimate purchaser's resident alien or social security card and other identification information.
96. According to the Dealership managers, pursuant to the arrangement "C" had with the Dealership, "C" supervisor would contact the Dealership and

indicate the need for a specific type of vehicle. The Dealership would then purchase the vehicle at auction. The Agriprocessors supervisor would pick up the vehicle in Cedar Rapids and pay for the vehicle at that time. The Dealership managers did not know the price the Agriprocessors supervisor charged the customers in Postville.

97. Though the vehicles were sold to people in Postville, they were being titled in Des Moines County, Chickasaw County, and a few other counties. The information provided to the county treasurers was often different from the information contained in the Dealership records. A Special Agent with the Office of Inspector General, Social Security Administration, confirmed that the majority of the social security numbers used on applications for registration of vehicles did not belong to the person using the number.
98. The DOT Investigator was told, by unconfirmed sources, that the Agriprocessors supervisor forced Agriprocessors employees to purchase vehicles from him or they would be fired or given poor work shifts. According to an unconfirmed source, a former Clayton County Deputy Sheriff said the Agriprocessors' supervisor told the former deputy that the Agriprocessors' supervisor had \$80,000 of his personal money loaned out to Agriprocessors employees in connection with selling them vehicles.
99. In the fall of 2005, the DOT investigator attempted to speak with several of the purchasers of the vehicles. When he attempted to do so at the Agriprocessors plant, he discovered that the Agriprocessors supervisor ("C") had personally escorted the employee to the office for the interview with the DOT Investigator and waited outside the room during the interviews. When the DOT Investigator decided to terminate the attempt to interview employees at the plant, the Agriprocessors supervisor confronted the Investigator and appeared visibly angry about the investigation.
100. A short time later, the Investigator contacted an Agriprocessors' employee, Source #13, off site of the plant, and interviewed him/her about

the purchase of a vehicle from the Agriprocessors' supervisor. A few days after this interview, Source #13 filed a complaint with the Postville Police Department, asserting that the Agriprocessors' supervisor had threatened Source #13 about being interviewed by the DOT Investigator. Source #13 reported that the Agriprocessors supervisor threatened to harm Source #13 and also fired him/her.

101. The DOT Investigator learned from talking with Des Moines County Treasurer's Office personnel that a person hereafter referred to as Source #14 was involved in making applications to title and register cars in Des Moines County on behalf of people living in Postville. In the fall of 2005, the DOT Investigator interviewed Source #14 at the Des Moines County Treasurer's Office. Having been advised of and waiving his Constitutional rights, Source #14 stated that s/he would receive the application information or vehicle title information from two people in Postville, one hereafter referred to as Subject 1 (an Agriprocessors' employee) or another Subject Z. Source #14 received the documents (application information or title information for the transfer) via the mail, along with money. Source #14 then applied at the Des Moines County Treasurer's Office for the registration and title on behalf of the owner, using one of several addresses in the Burlington or West Burlington area. Source #14 advised her/his friends living at those addresses to expect to receive the registrations and titles in the mail. Source #14 arranged to pick the documents up from her/his friends and then sent them to Postville in bulk to be provided to the vehicle owner. Source #14 reported doing this more than 200 times, and s/he received a small fee each time.

102. On October 3, 2006, FBI and ICE Special Agents interviewed Source #15, a citizen of Guatemala. Source #15 stated s/he began work at Agriprocessors in October 2004, gaining employment by providing fraudulent social security and resident alien cards to the company. Source #15 began work in the turkey kill part of the Agriprocessors facility. Source #15 described the work as very difficult and that it hurt Source

#15's hands, so Source #15 requested a transfer to another area of the plant. Source #15's request was turned down by the Agriprocessors supervisor. Other Agriprocessors employees told Source #15 that, in order to get a favorable position in the plant, Source #15 would have to purchase a car from the supervisor. In January 2006, the supervisor approached Source #15 and offered to sell him/her a car, but Source #15 declined. When Source #15 asked for a transfer, the supervisor refused.

103. Your affiant knows, based on his training and experience, that undocumented aliens sometimes title vehicles in false identities using fraudulent documents and using false or fraudulent addresses to avoid detection by law enforcement and immigration authorities.

#### **EXPLOITATION OF ILLEGAL ALIENS AS INDICIA OF HARBORING**

104. Your Affiant is aware, from his training and experience, that those who employ illegal aliens often exploit the aliens in various ways. Those who knowingly employ or supervise illegal aliens, knowing their unlawful status, are able to exploit illegal aliens because illegal aliens are unlikely to contact authorities for fear they will be arrested and/or deported. Exploitation can take on many forms, such as requiring employees to provide money or other things of value to maintain employment or secure better working hours or tasks, providing sub-par working conditions, failing to pay overtime, and physically harassing or mistreating employees.
105. In this case, as outlined in paragraphs 86 through 98 above, there is probable cause to believe an Agriprocessors supervisor has assisted, for a cut of the proceeds, illegal aliens in obtaining false documentation in relation to purchasing vehicles, and thereby has aided in harboring the illegal aliens. The supervisor has also required illegal aliens to purchase vehicles through the supervisor in an attempt to secure better working conditions, as indicated by Source #15.
106. As further evidence of harboring illegal aliens through exploiting their reluctance to contact the authorities, your Affiant is aware that the Iowa Department of Labor has uncovered workplace safety problems at

Agriprocessors. On March 21, 2008 the Cedar Rapids Gazette reported that the Division of Labor Services for the State of Iowa issued to Agriprocessors 39 citations with proposed penalties of \$182,000 for allegedly violating state workplace safety and health standards. According to the article, a health inspection done on February 11, 2008, identified 13 serious health violations. On October 31, 2007, an inspection by the Division of Labor Services resulted in 26 citations, including two repeat violations.

107. On April 1, 2008, during testimony before the U.S. Senate Committee on Health, Education, Labor and Pensions, Agriprocessors was among three packing plants cited for having a history of safety violations. According to the testimony, during the period of April 2001 to February 2006, OSHA records show no less than twenty violations at AgriProcessors' Postville plant. Of these, twelve were identified by OSHA as serious. An examination of Agriprocessor's Postville plant's "OSHA 300" logs revealed five amputations along with dozens of other serious injuries such as broken bones, eye injuries and hearing loss. The witness also testified that there is concern that injuries are often unreported or under-reported. The witness also cited numerous reports in the media regarding workers' mistreatment at Agriprocessors, including a 2006 article "In Iowa Meat Plant, Kosher 'Jungle' Breeds Fear, Injury, Short Pay," published in a newspaper The Forward.
108. Following an article in The Forward, the Washington Post reported on July 7, 2007, that some conservative rabbis who toured the plant were shocked. " We found people arriving from the mountainsides of Guatemala on a Tuesday and being on the front of the production line on Wednesday . . . . We saw people who could barely read Spanish getting training in English and having no idea what was said to them."
109. On March 27, 2007, over twenty current and former employees filed a civil suit in the U.S. Court for the Northern District of Iowa against Agriprocessors, alleging violations of the Fair Labor Standards Act. The

lawsuit alleged that Agriprocessors failed to pay workers for time spend preparing for and cleaning up after work. Seven of those plaintiffs are included among the employees listed on the third and fourth quarter of 2007 IWD reports as working for Agriprocessors using social security numbers which did not match the names to which they were assigned, or that were unassigned to any person. The lawsuit was settled out of court.

**REQUEST TO SEARCH FOR AND IDENTIFY ALL SUBJECTS OF CRIMINAL COMPLAINTS**

110. On April 16, 2008, the United States filed criminal complaints against 697 current Agriprocessors employees under their alias names, charging them with unlawfully using social security numbers in relation to their employment in violation of Title 42, United States Code, Sections 408(a)(7)(B); aggravated identity theft in violation of Title 18, United States Code, Section 1028A(a)(1); and/or possession or use of false identity documents for purposes of employment in violation of Title 18, United States Code, Section 1546. Three of those subjects have subsequently been encountered and arrested by local authorities on unrelated criminal charges. Because the true identities of the 697 subjects was unknown at the time, (and with the exception of three people remain unknown today) the court issued "John Doe" arrest warrants which describe the subject by the name under which the subject is employed at Agriprocessors. Each of these subjects was listed on the fourth-quarter payroll records obtained from IWD. (Though ICE has requested payroll records from IWD for the first quarter of 2008, IWD has advised that Agriprocessors has not yet reported that information to IWD.) There is probable cause to believe one or more of those subjects are present at Agriprocessors during regular working hours. This Search Warrant Application seeks authorization to search the Agriprocessors plant and curtilage for and identify any of those 697 employees for whom the United States obtained a criminal complaint.

**REQUEST TO SEARCH FOR AND SEIZE IDENTIFICATION DOCUMENTS  
FROM PERSONS**

111. As explained in the prior section, the government filed criminal complaints against 697 employees of Agriprocessors who were reportedly working there under aliases. With the exception of approximately 15 of those people for whom the government has photographs, (and the three who have recently been encountered by local authorities) the government cannot positively identify the other people who are subject to the arrest warrants due to their suspected use of assumed names and/or Social Security numbers or other means of identification. Moreover, determining the identities of all employees at the Agriprocessors's facility, including a determination of their lawful status (whether a United States citizen, lawful permanent resident alien, an alien eligible for employment, or an illegal alien) and what percentage of the workforce is illegally in the United States and employed at Agriprocessors, constitutes potential evidence of violations of law, including possible harboring of aliens by Agriprocessors and/or its management and supervisors. In other words, in harboring cases, the percentage of the workforce that is working legally, versus the percentage of the workforce that is working illegally, constitutes evidence of harboring admissible at a criminal trial against those accused of harboring the illegal aliens. Based on the facts set forth in this Affidavit, there is probable cause to believe that Agriprocessors' employees possess, either on their persons or in lockers or similar storage areas at the facility, company-issued identification cards, drivers' licenses and other forms of identification. (As part of this investigation, ICE Special Agents have confirmed from an Iowa DOT database that Iowa drivers licenses have been issued to many of the employees for whom ICE has "no-match" social security information.) Furthermore, false or fictitious immigration documents, social security cards, and similar fraudulent identification documents constitute contraband, the possession of which is itself illegal. Your affiant also knows from his training and experience that

illegal aliens often attempt to dispose of or discard identification documents during an immigration raid either at the instruction of their employer or based on their own volition. Management or supervisory personnel may sometimes pick up or collect these discarded identification documents in an effort to conceal the harboring of the illegal aliens. The agents intend to engage in consensual conversations with employees concerning their identification, and to request voluntary production of identification documents. This Search Warrant Application seeks authorization to, if necessary, search for and seize from each person believed to be an employee of Agriprocessors any and all Agriprocessors-issued identification cards, Agriprocessors-issued entry or proximity cards, drivers' licenses, or other means of identification from any person or any location within the Agriprocessors facility.

#### **REQUEST TO SEARCH AND SEIZE BIOMETRIC INFORMATION**

112. As stated in the previous paragraph, determination of the identities of all employees at the Agriprocessors's facility, including a determination of their lawful status (whether a United States citizen, lawful permanent resident alien, an alien eligible for employment, or an illegal alien) and what percentage of the workforce is illegally in the United States and employed at Agriprocessors, may constitute evidence of violations of law, including possible harboring of aliens by Agriprocessors and/or its management and supervisors. Moreover, Agriprocessors uses swipe cards and/or biometric devices to identify employees and as a form of time clock, registering the hours of employment. There is probable cause to believe that having employees place their hand on the biometric device used in the plant on the day of the search will reveal evidence of the identity of the employee and provide further evidence as to hours of work. Having the employees "clock out" using the biometric devices on the day of the search will, incidentally, aid in ensuring the employees are paid for any time they worked on the day of the search. This Search Warrant Application seeks authorization to search for and seize biometric

information using Agriprocessors' biometric identification system. This will be accomplished by having employees "clock out" by either placing their hand on the biometric device and/or using the swipe cards issued to employees as necessary to disclose the identity evidence contained in the system. This Search Warrant Application also seeks authorization to search for and seize from Agriprocessors any electronic or computer hardware, software, or storage devices utilized by the company in connection with the biometric identification system, as set forth below in more detail.

**REQUEST TO SEARCH FOR AND SEIZE ALL DES MOINES COUNTY VEHICLE TITLE AND REGISTRATION INFORMATION**

113. One or more Agriprocessors supervisory employees are involved in harboring, or aiding and abetting the harboring, of illegal aliens by assisting them to obtain titles and registrations for vehicles in their false names, and by arranging to have the vehicles titled and registered with false addresses in Des Moines County. This false information on the titles and registration documents aids illegal aliens in avoiding detection at their actual place of residence and in their use of false means of identification. There is probable cause to believe that vehicles bearing Des Moines County license plates located at the Agriprocessors' facility would contain title and registration information that would constitute evidence of this harboring activity and vehicle registration fraud. This Search Warrant Application seeks authorization to search all vehicles on the Agriprocessors property bearing license plates from Des Moines County for titles and registration documentation and any other evidence of the owner or use of the vehicle.

**REQUEST TO SEARCH AND SEIZE COMPUTER SYSTEM**

114. The foregoing establishes probable cause to believe that evidence of criminal activity is stored on the premises in the form of computer data. Computer hardware, software, and electronic files on the premises

therefore may be important to this criminal investigation because they may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, the warrant application requests permission to search and seize all records described in Attachment #2, including records that happen to be stored in electronic form. These records constitute evidence of crime. This application also requests permission to seize the computer hardware that may contain those electronic records if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site.

115. Based upon my training, experience, and consultations with ICE Computer Forensic Agent(s), I know that information stored in an electronic format may be found not only on the hard disk drive of a computer, but on other computer hardware and storage media, including back-up tapes, diskettes, CD-ROMs, handheld organizers, and other devices capable of storing information in an electronic format. I also know that during the search of the premises it is not always possible to search computer hardware and storage media for data for a number of reasons, including the following:

(A) The volume of evidence: The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. Computer storage devices like hard disks, tapes, CD-ROM's, and Digital Video Disks (DVD's), can store the equivalent of thousands of pages of information. A single megabyte of storage space is equivalent to 500 double-spaced pages of text. A single

gigabyte of storage space, or 1,000 megabytes, is equivalent to 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high.

(B) Technical requirements: Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

(C) Files may be hidden or encrypted: Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".txt." often are text files; however, a user can easily change the extension to ".jpg." to conceal the text file and make it appear that the file contains an image. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime. The forensic procedures used to recover hidden, compressed, password-protected or encrypted files can be extremely time consuming, even for a qualified expert. In fact, if robust

encryption software is utilized to encrypt a file and the password is unknown, it may be impossible to decrypt the file in order to view the information contained within it. Files encrypted with less secure encryption algorithms may still require considerable time or outside agency assistance to decrypt, absent a password.

(D) Danger of the Destruction of Evidence: Computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction, both from external sources and from destructive code embedded in the system as a "booby trap." In order to maintain the integrity of the original evidence, a qualified expert may need to conduct a forensic examination of the storage media in a controlled environment, such as a law enforcement laboratory, where scientific procedures and specialized software designed to protect the integrity of the original media will be used.

116. ICE Computer Forensic Agent(s) have also advised me that in order to retrieve electronically stored evidence from a seized computer, agents may be required to seize most or all of a computer system's equipment, including hardware, peripherals, software, documentation, security devices, and passwords. This is true because of the following:

(A) Some operating systems, software or hardware configurations require the original equipment and/or installed software to be present in order to access the information contained on the system.

(B) Peripheral devices that allow users to enter or retrieve data from the storage devices vary in their compatibility with other hardware and software.

(C) The Computer Forensic Agent may have to install software used by the suspect on a government computer in order to retrieve information the suspect may have stored using that software. The CFA may need to refer to software and hardware documentation maintained by

the suspect to complete his/her analysis in a timely manner. The suspect's computer documentation may also contain hand-written notes specific to the seized computer system.

(D) Physical keys, encryption devices, dongles, and similar physical items may be necessary to gain access to the computer equipment. Passwords, pass-phrases, password files, and similar decryption codes may be required to access specific information stored on the seized computer system.

117. Therefore, it is requested that agents executing this search warrant be authorized to employ the following procedure upon execution of this search warrant:

(A) After the premises have been secured, an ICE Computer Forensic Agent and/or other law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer hardware and storage media to determine if it is possible to search these items on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data. If for some unforeseen circumstances, the computer personnel are not present during the execution of the search warrant, then all hardware, storage media, peripherals, software, documentation, security devices, and passwords, as defined below, will be seized and transported to an appropriate law enforcement facility for review. The hardware and storage media will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized, as set forth in Attachment B.

(B) If the computer hardware and storage media cannot be searched on-site, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the

data. The computer personnel will also determine if these backups will be useable for an off-site examination conducted at a later date without the original equipment. As stated above, some operating systems, software or hardware configurations require the original equipment and/or installed software to be present in order to access the information contained on the system.

(C) If the computer personnel determine it is not practical to perform an on-site search or make an on-site copy of the data, then all hardware, storage media, peripherals, software, documentation, security devices, and passwords, as defined below, will be seized and transported to an appropriate law enforcement facility for review. The hardware and storage media will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized, as set forth in Attachment B.

(D) If law enforcement personnel determine, either on-site or during a subsequent off-site search, that any hardware, storage media, peripheral, software, security device, or data (1) is an instrumentality of the offense stated above, meaning that it was designed or intended for the use of, or is being or has been used, as the means of committing the offense; (2) contains any contraband, such as counterfeit or stolen software, child pornography, national security information, or unauthorized access devices such as stolen credit card numbers; (3) is the fruits of criminal activity; or (4) is otherwise criminally possessed, the property shall be seized and not returned pursuant to Federal Rule of Criminal Procedure 41(b).

(E) Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the

offense specified above.

(F) In searching the data, the computer personnel may examine and copy all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized, as set forth in Attachment B. In addition, the computer personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

(G) All hardware, storage media, peripherals, software, documentation, security devices, and passwords that were seized for off-site examination, and are not otherwise subject to seizure, shall be returned by the government to the subject premises within a reasonable period of time.

118. For purposes of this affidavit, the foregoing terms are defined as follows:

(A) Hardware: Hardware includes the following equipment: (1) data-processing devices containing central processing units, such as "desktop", "tower", "laptop" and "notebook" computers, hand-held electronic organizers, and "personal digital assistants"; (2) internal and external storage devices, including magnetic storage devices such as hard disk drives, diskette drives, and tape drives, optical storage devices such as CD-ROM drives, CD-R/CD-RW recorders, and DVD drives/recorders, and other memory storage devices such as smart-card readers.

(B) Storage Media: Storage media includes any material capable of storing information in a manner that can be used by computer hardware to save and/or retrieve information. Examples of storage media include diskettes, CD-ROM's, CD-R's, CD-RW's, DVD's, DVD-R's, DVD-RW's, magnetic tapes, ZIP disks, JAZ disks, Peerless disks, SparQ disks, ORB disks, optical disks, smart-cards, EPROMS, and digital memory media

such as CompactFlash, SmartMedia, Sony Memory Sticks, and USB "thumb" or "key" drives.

(C) Peripherals: Peripherals are equipment that send data to, or receive data from, computer hardware, but do not normally store user data. Keyboards, mice, printers, scanners, plotters, video display monitors, modems, cables, and certain types of facsimile machines are examples of peripherals.

(D) Software: Software is digital information that can be interpreted by computer hardware to direct the way hardware works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems (like Microsoft "Windows"), applications (like word-processing, graphics, or spreadsheet programs), utilities, and communications programs.

(E) Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

(F) Security Devices: Security devices include physical keys, encryption devices, "dongles", and similar physical items needed to gain access to associated computer hardware.

(G) Passwords: Passwords include alphanumeric strings, pass-phrases, password files, and similar decryption codes necessary to access data that is encrypted or otherwise inaccessible.

119. No wire communications or electronic communications shall be intercepted during the execution of this search warrant. I have no information to indicate that the computer(s) to be searched operate in any way as an Internet Web Site Host/Server, Internet File Transfer Protocol (FTP) server, Internet Chat Server, or Internet Email forwarder or server. As such, it would appear that the provisions of the Wire and Electronic

Communications Interception Act, 18 U.S.C. § 2510 et seq. do not apply. Should information of this type be discovered, the government will preserve it and set it aside.


120. I have no information to indicate that any "work product" or "documentary" materials are stored on the computer(s) to be searched, for the purpose of disseminating it to a public newspaper, broadcast, or other similar form of public communication. Should agents become aware of any such materials as described in 42 U.S.C. § 2000aa, they shall be returned as quickly as circumstances permit.

### **CONCLUSION**

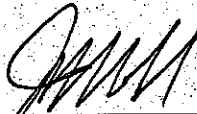
121. Based on the above information, there is probable cause to believe that evidence of the crimes of harboring illegal aliens in violation of Title 8, United States Code, Sections 1324(a)(1)(A)(iii), 1324(a)(1)(A)(iv), 1324(a)(1)(A)(v)(II), and 1324(a)(1)(B)(I); engaging in a pattern or practice of hiring and continuing to employ undocumented aliens in violation of Title 8, United States Code, Sections 1324a(a)(1)(A), 1324a(a)(2) and 1324a(f)(1); document fraud in violation of Title 18, United States Code, Section 1546(b); misuse of a social security number in violation of Title 42, United States Code, Section 408(a)(7)(B); and aggravated identity theft in violation of Title 18 United States Code, Section 1028A(a)(1); will be found on the property described in Attachment 1.

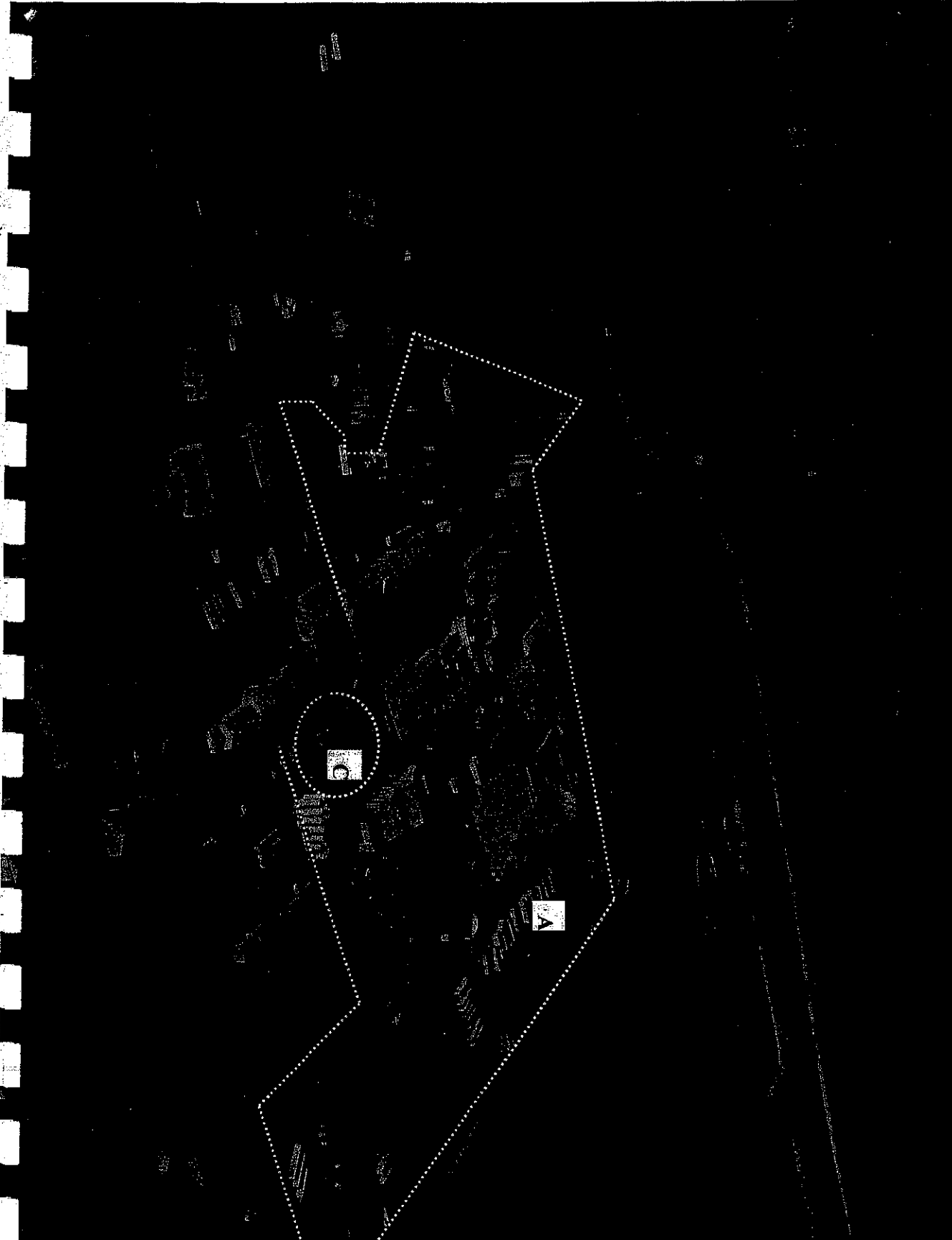
122. The items and/or persons to be searched for, identified, and/or seized are set out in Attachment 2. The United States requests an order sealing this application and search warrant until entry is made on the premises to execute the search warrant, except with respect that portion of Attachment 2 which lists the names of the 695 people for whom there are criminal complaints. The United States requests those names remain sealed until further order of this Court because the criminal complaints have been already been ordered sealed until further order of this Court, and the names may also be victims of identity theft.

Further your affiant sayeth not.

  
\_\_\_\_\_  
David M. Hoagland, Senior Special Agent  
U.S. Immigration and Customs Enforcement

Subscribed and sworn to before me this 9<sup>th</sup> day of May, 2008.

  
\_\_\_\_\_  
JON STUART SCOLES  
Magistrate Judge



**EXHIBIT 1**