FILED

BY: DL

2010 APR -5 AM 9:28

VIRLYNN TINNELL
SUPERIOR COURT CLERK

AFFIDAVIT FOR SEARCH WARRANT

COUNTY OF MOHAVE

STATE OF ARIZONA

NO. SW 2010-00020

Your affiant, W.T. Flanagan, a Peace Officer in the State of Arizona, being first duly sworn, upon oath, deposes and says:

That between August 1st 2004 and January 14, 2010, in the County of Mohave, State of Arizona

(X) the crime(s) of :

A.R.S. § 13-2310 - Fraudulent schemes and artifices; Class 2 Felony

A.R.S. § 35-301(A)(1) and (A)(4). Duties and liabilities of custodian of public monies; Class 4 Felony

> 35-301. Duties and liabilities of custodian of public monies; violations; classification
>
> A public officer or other person, including justices of the peace and constables, charged with the receipt, safekeeping, transfer or disbursement of public money is guilty of a class 4 felony who:
>
> 1. Without authority of law, appropriates it, or any portion thereof, to his own use, or to the use of another...
>
> 4. Without authority of law knowingly deposits it, or any portion thereof, in a bank, or with a banker or other person, except on special deposit for safekeeping.

is being committed by :

Jacob "Jake" L. Barlow, WMA, DOB XXXXX, SSN XXXXXXXX

David William Darger, WMA DOB XXXXXX SSN XXXXXXX

in the following manner:

~~( ) an arrest warrant # _____ was issued for the arrest of _____.~~

That the affiant has probable cause to believe and he does believe that there is now:

(X) in the possession of: **Jacob "Jake" L. Barlow** and **David William Darger**

(X) in and on the premises and building(s) described as:

1: xxxxxxxxxxxxxx Colorado City, AZ.
2 story single family residence, grey stucco in color. Wood covered front porch with log pole as columns, Brown cement wall at front of house.

2: xxxxxxxxxxxxx Colorado City, AZ.
1 story ranch style house, red brick front. The closest cross street is Carling. The house is a one story residence with a basement; it has a wood fence on the east side.

3: 20 South Pioneer St., Colorado City, AZ.
A Colorado City Fire Station, Fire Station #1 is located at 20 S Pioneer St. on the south west corner of Pioneer St. and Township across the street from the Town hall and Marshal's Office. It has a brown brick on the out side, and 3 white bay doors on the east side and on the west side. It also has a pedestrian door on the south side of the bay doors.

4: 40 South Pioneer St., Colorado City, AZ.
A Colorado City Fire Station, 40 S Pioneer is a green metal building that sits on the north side of fire station 1.

5: 220 East Township, Colorado City, AZ.
A Colorado City Fire Station, Fire Station #2 is located at 220 East Township on the northeast side of Township and Carling. It is a gray, 2-story metal building. It has a chain-link fence around the back of the building. In the yard behind the building is a brown shipping container, a white enclosed trailer, a 20' to 24' silver semi trailer, and a full size semi van trailer white in color.

in the County of Mohave, State Of Arizona including all the curtilage of said premises, as well as out buildings and storage sheds.

(X) in the vehicle(s) described as:
Vehicles registered to the Colorado City Fire District/Department/Hilldale Fire department, to include, but not limited to, Fire trucks, ambulances, and emergency service vehicles. Vehicles registered to **Jacob "Jake" L. Barlow** and **David William Darger**

certain person, property or things:

~~( ) is the subject of an outstanding arrest warrant #_____~~

(X) which were stolen or embezzled from: **Colorado City Fire District/Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department.**

(X) were used as a means for committing: A Felony to wit:

A.R.S. § 13-2310. Fraudulent schemes and artifices; Class 2 Felony

A.R.S. § 35-301(A)(1) and (A)(4). Duties and liabilities of custodian of public monies; Class 4 Felony

(X) is being possessed with the intent to use a means of committing: A Felony to wit:

A.R.S. § 13-2310. Fraudulent schemes and artifices; Class 2 Felony

A.R.S. § 35-301(A)(1) and (A)(4). Duties and liabilities of custodian of public monies; Class 4 Felony

(X) are in the possession of **Jacob "Jake" L. Barlow** and **David William Darger** who it was delivered for the purpose of concealing it or preventing it from being discovered

(X) consists of any item or constitutes any evidence which tends to show that

A.R.S. § 13-2310. Fraudulent schemes and artifices; Class 2 Felony;

A.R.S. § 35-301(A)(1) and (A)(4). Duties and liabilities of custodian of public monies; Class 4 Felony

has been committed, or tends to show that **Jacob "Jake" L. Barlow** and **David William Darger** has committed A.R.S. § 13-2310. Fraudulent schemes and artifices; Class 2 Felony; A.R.S. § 35-301(A)(1) and (A)(4). Duties and liabilities of custodian of public monies; Class 4 Felony

That said person, property or things are described particularly as follows:

See Items to be seized List
ATTACHMENT A

Affiant's Expertise and Background

Your affiant is currently employed as an investigator by the Mohave County Attorney's Office in Mohave County Arizona. Your affiant has been employed as an investigator with Mohave County Attorney's Office from 1997 to this date. Your Affiant has been a law enforcement officer for over 30 Years. Your affiant was a patrol officer with the Plainfield Police Department in New Jersey from 1972 to 1977. Your affiant was employed by the Mohave County Sheriff's Office from 1977 to 1997 and served in the positions of Deputy Sheriff, Detective, Patrol Sgt., Fugitive Sgt. and Detective Sgt. While serving with both the Mohave County Sheriff's Office and the Mohave County Attorney's Office, your affiant has had several occasions to investigate crimes of a financial nature which included fraudulent schemes, theft and misuse of funds and money laundering. Your affiant has also attended at least 80 hours worth of training in the area of financial investigations that dealt with various types of fraud, theft, money laundering and conspiracy. Your affiant has prepared and or assisted with the preparation and execution of at least a dozen search warrants that have dealt with the crimes of fraud and theft and conspiracy as it may deal with both public and private monies.

Your affiant has received in excess of 80 hours of training in the area of computer investigations, dealing the in the area of the forensic examination of computers in order to search a computer and/or electronic media that may be evidence in the course of an investigation. This training has been received from a combination of workshops, seminars and meetings dealing with the manner in which electronic documents are stored, maintained, transferred and copied. This training has been from such agencies as The Arizona Department of Public Safety, Federal Drug Enforcement administration, Arizona Attorney Generals Office. Your affiant has also consulted with trained computer forensic investigators on various ways the digital media and/or electronic media can be stored, transferred, maintained and accessed.

Your affiant has also prepared search warrants; on at least six or more occasions; that have lead to the seizure of computers and/or electronic storage media. These items have then been turned over to a trained forensic investigators for the retrieval of the information.

Investigator Gary Engels' Expertise and Background

Gary Engels is currently employed as an investigator with the Mohave County Attorney's Office in Mohave County, Arizona. He has worked for the County Attorney's Office from 2004 until present. He was employed as a law enforcement officer for 20 years. He was a patrol officer for Adams County Sheriff's Department in Colorado from 1973 to 1979. He worked for the Golden Police Department in Colorado from 1979 to 1982. From 1983 to 1987, he worked for Silverthorn Police Department in Colorado as a patrolman and back-up detective. In 1987, he went to work for the Bullhead City Police Department and worked in Patrol and in Detective Bureau. He retired from Bullhead City in 1993. In his 20 years as a police officer, as well as the five years he worked for the County Attorney's Office, he has had several occasions to investigate crimes of a financial nature from bad checks to fraudulent schemes. He has also been involved in investigating thefts of money and misuse of funds

STATEMENT OF PROBABLE CAUSE

That the following facts establish probable cause for believing that grounds for the issuance of a search warrant for the aforementioned items exists:

In preparation of this affidavit and Search Warrant your affiant has meet with both Investigator Engels and Deputy County Attorney James Schoppmann. During these meetings your affiant has received information as noted and also reviewed various documents that are referred to in this affidavit..

Starting in 2008 the Mohave County Attorney's Office began an investigation dealing with the suspected misuse of public funds by the members of the **Colorado City Fire District ("CCFD")**. **CCFD** is governed by two public officials/members identified as **Jacob L. Barlow** (elected Fire Chief), also known as "Jake" Barlow; and **David William Darger** (elected Secretary/Treasurer).

Between January 2008 and the January 2010, the Mohave County Attorney's Office obtained various documents: monthly bank statements; credit card statements, invoices and records dealing with the expenses and purchases by Barlow and Darger with CCFD pubic monies beginning around September 2004 to June 2009 that involved the use of credit cards and accounts

of the **Colorado City Fire District/Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department.** Added information was obtained by a series of public records requests by Deputy County Attorney James Schoppmann, as well as interviews conducted by Schoppmann and Mohave County Attorney's Office Investigator Gary Engels.

On or about January 17, 2008, a Mohave County employee in the Office of Management and Budget, received a phone call from a restaurant owner in St. George, Utah, who had called to report that Colorado City Fire Chief Barlow had bought dinner for his family using a fire district credit card.

The County Attorney's Office ("**CAO**") decided to request public records from the CCFD. CCFD is governed by Chief Barlow and Secretary/Treasurer Darger, who are public officials, who were recently appointed to their current four-year term at a Board of Supervisor's meeting held 8/10/2008.

On February 12, 2008, James Schoppmann, a Deputy Mohave County Attorney, spoke to Chief Barlow via telephone regarding a public records request. Chief Barlow asked to meet with him in person after Schoppmann indicated that the CAO wanted public records such as bank statements and credit card statements.

Chief Barlow told Schoppmann that people might not understand the situation and agreements between Hildale, CCFD, and the Town of Colorado City because they work together and have intergovernmental agreements due to the small community. He stated that CCFD pays the Town of Colorado City because the employees work part time for the City and part time for the fire district and that an employee's salary would include portions of City work and portions of CCFD work. He stated that CCFD did this because there are hidden cost of worker's compensation and insurance, among other things. Chief Barlow also told Schoppmann that his volunteers do a great job and don't need to be subject to public scrutiny or slapped around. He also told Schoppmann that Hildale, Utah, has a lot of the financial records regarding billing and ambulance services.

Records received from CCFD at the beginning of this investigation indicated the following:

1. Copies of Minutes of the CCFD indicating that persons other than Chief Barlow and Secretary-Treasurer Darger made and seconded motions as well as voted on District

business.

2. Copy of CCFD Resolution 06-2006 regarding reimbursement and per diem for fire district officials and employees. The policy states that an employee shall be eligible for a meal per diem for a non-employee co-driver.
3. U.S. Bank statements for account ending -1940 which show numerous purchases to Cooperative Mercantile (a local general store in the Town), including several purchases in a single day.
4. U.S. Bank CCFD Medic 10 Credit Card Statements which showed multiple purchases several days of any given week, for which records were obtained and reviewed, to restaurants in St. George, Utah, including Ruby River and Steak and Seafood. One purchase on October 17, 2007 at Steak and Seafood was for $288.54.
5. An invoice for twenty (20) $15.00 gift certificates from Dezereta (a local gas station in Colorado City) dated December 18, 2007.
6. An invoice for fifteen (15) $15.00 gift certificates from Garden Gate Inc. (Owned by David Darger) dated December 15, 2007.
7. An invoice for one hundred (100) candy gift boxes for a total amount of $575.00 to Jill Johnson Special Manufacturing dated December 17, 2007.
8. Several invoices from Big Dan's Drive Thru LLC and Vermillion Candy Shoppe/ Fine Restaurant (both located in Colorado City) indicating various employees/volunteers charging food to the CCFD.

On June 4, 2008, Schoppmann emailed CCFD attorney about the status of a public records request and wrote that the CAO heard that Chief Barlow has repaid the District for personal expenses on district cards and funds including perhaps food charged to the District and asked for copies of any repayments to the fire district by any official or employee, including Chief Barlow.

On June 10, 2008, Schoppmann received an email from CCFD's attorney indicating that Chief Barlow informed him that he has not used the District's cards or funds for personal expenses (and, therefore, there are no records to be disclosed).

The 1st public records request was delivered to Jake Barlow on February 14, 2008. Several, but not all requested documents were finally received on April 18, 2008, two days after Schoppmann sent CCFD's attorney a draft Special Action and Application for Order to Show

Cause via email. Schoppmann later asked this attorney why CCFD did not send any of the bank statements requested and the attorney replied that CCFD had not made them aware of other accounts the District uses besides the credit card statements provided. Additionally, the MCAO obtained documents (that were part of the request), via subpoenas, from various financial institutions that were not provided by CCFD. A 2nd public records request was made on May 19, 2008, to include sale receipts for purchases at Costco and Sam's Club and records detailing the dates and ending locations of ambulance runs for a 3 month period so that the MCAO could assess whether the numerous purchases were legitimate fire district expenses. However, CCFD's attorney responded that they were not aware of any record that was not already provided that would contain such information asserting that we could not have medical records even though we told CCFD that we did not want/need any patient information just information to confirm expenses were related to fire district business.

As the investigation continued into April 2009, Schoppmann asked Darger via email if he and Jake Barlow would meet and talk with him and an investigator regarding the district. Darger responded by accusing Schoppmann of having a biases agenda against CCFD and the Town of Colorado City and stated that they had met with Supervisor Watson and Bill Ekstrom in an attempt to resolve any issues and directed Schoppmann to their new attorney in Anthem, Arizona.

Schoppmann then made a request for a meeting to CCFD's new attorney who responded by saying that "given the logistics involved" they would rather respond to written questions. A list of question was directed to Jake Barlow and sent to the attorney. The questions (similar to interrogatories) also requested documents that corresponded to any answers provided. The response was provided in June of 2009 with no back up documents. Instead the attorney stated that if we wanted public records we could make a public records request and they would comply if not unduly burdensome. Additionally, the answers were characterized by Schoppmann as "vague and incomplete".

Bank Statements *from US Bank National Association* were received for the period January 2, 2007 to September 30, 2007, and April 1, 2008 to August 31, 2008. The Legal Records Coordinator for US Bank indicated that Jacob Barlow and David Darger are signers on this account and that there is one check card, which is held by David Darger. The Bank Statements indicated numerous purchases at Cooperative Mercantile. Cooperative Mercantile is the main

general store in the Colorado City area. The records indicate that Darger's card was used approximately 30 times at Cooperative Mercantile during February 2008, including five times on 2/4/08 and seven times on 2/19/08, which appears inconsistent with general government spending of public monies that is based upon an adopted budget and usually requires scheduled and authorized purchase approval.

Credit Card Statements from *US Bank National Association ND* were received for the period December 16, 2006 to August 15, 2008. The Credit Card Statement for the Medic 10 card indicates six purchases at Dezereta (gas station in the Town) on Christmas Day, 12/25/2007. Additionally, the Medic 10 card was used for two large meal purchases in St. George, UT, on 07/02/08 (Steak and Seafood $102.46 and The Claim Jumper $156.68). The Medic 11 card was used for two (2) purchases at Dezereta on Christmas Day, 12/25/2007 as well.

Our investigation indicates CCFD has at least two bank accounts in addition to its lawful County Treasurer's Warrant Account (where public monies are received from taxes). The two bank accounts are: U.S. BANK NATIONAL ASSOCIATION (the "**HCCFD Training Fund**") and FAR WEST BANK, DIVISION OF AMERICA WEST BANK. Far West Bank has no branches in Arizona.

CCFD also has at least the following credit card accounts: AMERICAN EXPRESS COSTCO BUSINESS CARD; CHASE MASTERCARD; U.S. BANK NATIONAL ASSOCIATION ND, VISA BUSINESS CARD; and SAM'S CLUB (GE CAPITAL FINANCIAL, INC.).

The records indicated that Barlow and Darger periodically draw large warrants (checks) off the CCFD Warrant Account and deposit them into the two bank accounts. The bank accounts are then used to pay for various expenses, including CCFD credit cards, and public funds transferred from CCFD's County Warrant Account to these banks appear to have been used for personal use. Schoppmann advised Engels that, pursuant to Title 48, Arizona fire districts are to operate out of their county warrant account. In mid February 2010 Engels obtained copies of 2 warrants (checks) of CCFD which showed that CCFD wrote warrants checks on 12/31/2009 and 1/14/2010 in the amounts of $10,000 and $20,000, respectively, to themselves as "fund transfer[s]" which were both deposited in CCFD's Far West Account. Jake Barlow is a signer on both of these checks, which is consistent with previously reviewed warrants. CCFD continues to transfer large amounts

of public funds into traditional bank accounts instead of operating out of the CCFD County Warrant Account.

Turbo Tax Purchases

The statements for the American Express Card in the name of Jake Barlow, **CCFD** indicate the following purchases of Turbo Tax Software:

1.	$64.45 purchase for TurboTax software on	02/04/04
2.	$31.70 purchase of Intuit Software on	01/27/05
3.	$31.70 purchase of Intuit TurboTax Software on	01/26/06
4.	$59.99 purchase of Turbo Tax 06 Prmier w/ Sta	01/05/07
5.	$59.99 purchase of TTax 07 Prem on	01/04/08
6.	$37.69 purchase of Intuit TurboTax Software on	01/16/08
7.	$43.09 purchase of Intuit TurboTax Software on	01/30/09

The records show that Turbo Tax software was purchased with public monies by Jake Barlow on multiple occasions. Jake Barlow used a CCFD credit card, which was paid with public monies of CCFD in the Far West Account.

Your affiant is familiar with the fact that Turbo Tax is a computer program that can be used to prepare and generate tax reports for both state and federal income tax returns. Updated programs could be used to track investments. The program, in its various forms, can be used for both a private individual and also for a business.

Deputy County Attorney Schoppmann is familiar with the operation of Fire Districts in Arizona, having been legal adviser to several Fire Districts in Mohave County. Deputy County Attorney Schoppmann advised your affiant that his research showed that there appears to be no legal justification for the purchase of Tax Preparation software and/or Investment software by the CCFD Fire Chief Jake Barlow, on his department issued credit card.

Your affiant knows that this type of computer program can be used to generate reports and records in both digital and printed format. Your affiant knows that in a digital format such records can be stored on various types of storage media that would include CD's, DVD's; built in computer hard drives, portable hard drives, thumb drives, flash drives, as well as disks and compact cards.

Home Hotel – Lava Hot Springs, Idaho Purchases

The records indicate that Jake Barlow used CCFD credit cards to buy gas, food, and lodging for a trip to Lava Hot Springs, Idaho. Copies of Home Hotel & Motel receipts indicate that Jake Barlow charged three (3) rooms for two (2) nights with two (2) persons in each room. Jake Barlow and other fire district personnel received travel expenses of $270.00 and still used CCFD credit cards for food.

On or about 09/24/08, Schoppmann contacted the City of Lava Hot Springs, Idaho, and spoke to Gene Fagnat who could not recall any training on those dates and said that training would not usually be done during that time and the training would not include people from Arizona. Schoppmann also spoke with Division Chief Williamson of the Pocatello Fire Department (as it is in the same county as Lava Hot Springs, and Pocatello is the closest big city – approximately 30 miles away). Williamson could not think of any training during that time. Engels also later confirmed this by talking with Chief Williamson via phone. Schoppmann also contacted Allen Farnsworth of Chubock Fire Department, and he did not believe there was any training going on during that time. He said they had some local firefighter training but it was not open to others.

New Egg

A review of newegg.com invoices, which were obtained by requests via mail and phone (including a follow-up phone call and email communication with Anna Hernandez, a Fraud Prevention Analyst with newegg.com) indicate that 15 purchases were shipped to Glen Nielson (also known as Glen Jeffs) at 585 North Homestead St., P.O. Box 194, Colorado City, Arizona, which is a personal residence, and billed to the CCFD. The invoices going to Nielsen's home date from 3/9/2004 to 1/19/2009.

A review of other invoices received show that the items were sent to Jake Barlow at 40 South Pioneer Street, which is a CCFD location, approximately 120 times with a total of more than $25,000 from June 2004 to August of 2008. The fire district made other purchases of computer equipment, including purchases on the CCFD American Express card as shown on reviewed statements previously obtained.

COSTCO

Credit Card Statements were obtained by the CAO for the period May 2003 to September 2008 and show that the Fire District spent $22,907.50 at Costco from 09/03/04 to 08/21/08.

Statements from January 2008 indicate 58,000 points were redeemed for an iPod. The Statement for June 2008 indicates 50,000 points were redeemed for five (5) $100.00 gift cards to The Home Depot.

In going through the receipts that we received from Costco, I noticed several purchases on the CCFD American Express Costco Credit Card Account # 3715-356709-11003, including the following:

1. On 7/18/06, a Motion Sofa "Geneva" leather sofa for $889.99; Martin Newbury L-Shape Desk w/Return for $749.99; NB450 Newbury Lateralfile for $259.99; and a Martin "Newbury" 2-Door Bookcase for $274.99;

2. On 11/21/06, (on-line order) for a Geneva 3-PC Workstation and Geneva Armoire for $1,151.02;

3. On 12/18/06, several food items, including two spiral hams, one for $20.48 and the other for $20.41;

4. On 1/5/07 Turbo Tax 06 Prmier W/ Sta for $59.99;

5. On 1/10/07 a West Dig 160GB W/Case (an IPod like device) was bought for $129.99. Food items were also bought for a grand total of $340.02;

6. On 2/2/07, another West Dig 160GB W/Case was bought for $129.99 and two "Panama" Leather Sofas at $789.99 each, for a total of $1579.98;

7. On 6/5/07, another West Dig 160GB W/Case was bought for $109.99;

8. On 12/6/07, a West Dig 250GB Port HD W/Case was bought for $139.99;

9. On 12/14/07, two spiral hams were bought, one for $25.76 and the second for $24.98, food items, including over $100 dollars in chocolate candy and seven 24-ounce Wild Alaskan King Salmon items for a total of $121.73. The grand total for this receipt was $843.45;

10. On 1/4/08, T.Tax '07 Premier W/ State was purchased for $59.99, and the receipt also showed a West Dig 1TB My Book Home for $279.99;

11. On 12/19/08, 17 units of Dove Asst Mini 35 oz were purchased for a total of $169.83, 19 units of Chocolate Delicate Square for a total of $187.72, and 18 units of KS Chocolates of the World 32 oz. for a total of $206.82 were also purchased. The total receipt was $822.67;

12. On 12/22/08, three digital frames totaling $419.97 (less $120.00 in coupons) were purchased, as well as two hams, one for $19.30 and the other $20.52, four Fresh Hen Turkeys were bought at $11.70, $11.49, $11.47, and $11.28, and four units of Shrimp, Tiger Tail On, at $79.96.;

See Attachment B & C
Costco Receipts

Sam's Club

Statements received from GE Money Bank-Sam's Club were received for the period January 2007 to September 2008 and show that the Fire District spent $13,865.96 at Sam's Club Warehouses during that time.

In going through the purchase history documents that we received from Wal-Mart Legal Department for purchases made at Sam's Club, there were a number of items of interest as indicated below:

1: On 12/8/05, 40 Danish hams for a total price of $286.80.

2: On 12/22/06, two chocolate gift towers for $19.87 each.

3: On 3/16/07, two oversized throws at $14.64 each, and fresh salmon fillets for $21.70.

4: On 3/17/07, a queen mattress pad for $24.84 and size 4 diapers for $26.88.

5: On 4/12/07, a six-pack of briefs for $8.88.

6: On 7/26/07, a four pairs of men's dress socks for $9.47.

7: On 12/1/07, a jumpsuit for a three to 13-month-old at $6.88.

8: On 1/19/09, a fleeced-lined hoodie for $24.23 and an IPod Dock alarm clock/radio for $79.47.

9: On 3/26/09, a Sea Lord Orange Roughy Fillets for $13.46, two eight-packs of bath towels for $19.88 each, a 12-pack of hand towels at $13.87, and a 24-pack of washcloths at $10.83.

10: And on 4/30/09, a set of king sheets at $49.84, and linen bath towel at $11.76. A video surveillance that we have from Sam's Club shows this particular purchase.

Food Purchases

The records obtained indicate a large volume of food purchased at local eateries, in addition to purchases at Costco and/or Sam's Club. For example, records from December 2007 show that Jake Barlow purchased approximately $1500 in food from Sam's Club and Costco while approximately $837 was spent at local eateries. Records from January 2008 show that approximately $537 in food was purchased at the St. George, Utah, Costco by Jake Barlow, in addition to approximately $1460 of CCFD monies used at local eateries in Colorado City.

Joseph Barrett, who was a volunteer with CCFD for approximately 14 years – up to about 2007, told me that the fire district did not have sleeping quarters or a full kitchen and that he only recalled being furnished food on search and rescue operation and big fire calls.

An article in the Kingman Daily Miner, from 12/26/09, reported that according to Daniel Barlow, a member of the CCFD, none of the firefighters, EMTs or paramedics have to sleep at the fire stations. They are able to eat and sleep at their own homes and are on call if an emergency occurs.

Another article in the 1/3/10 edition of the Kingman Daily Miner reported that the CCFD and Hildale Fire Department both have a total of 5 full time employees and one part-time employee with about 100 volunteer firefighters, EMTs, and paramedics. The report indicates that none of the firefighters, EMTs, and paramedics have to sleep at the stations and are able to eat and sleep at their homes. Additionally, the report indicates CCFD and Hildale Fire Department average just three calls a week.

Association between CCFD, Hildale Fire District, Hildale, UT, and the Town of Colorado City

You affiant was advised both by Deputy County Attorney Schoppmann and Investigator Engels that the two fire districts/departments have intergovernmental agreements ("**IGA**") between themselves and the cities of Hildale, Washington County, Utah and Colorado City, Mohave

County, Arizona. In at least one conversation Chief Jacob L. Barlow advised that Hildale keeps a lot of the financial records regarding billing and ambulance services.

Your affiant reviewed two of the IGAs. The first IGA reviewed is an "interlocal" cooperation agreement dated March 2005. Page one of this document noted:

> *WHEREAS, "HILDALE and the "DISTRICT"* (CCFD) *have operated under this Agreement of Mutual Understanding for fire, EMS & rescue services for automatic aid , mutual aid and other cooperative/joint use if resources and manpower since the "DISTRICT" was organized on March 1975, and...*

Another part of this document noted that Hildale and CCFD have operated under an IGA since 1999.

This IGA was signed by subjects Jacob Barlow as Fire Chief of the CCFD and David Darger as secretary Treasurer for the CCFD. Subjects identified as city officials from Hildale also signed the document.

The second IGA reviewed is an "interlocal" cooperation agreement dated May 2007. This IGA is between the "Town" of Colorado City and the **CCFD**. This agreement stated that:

> *WHEREAS, the "TOWN" houses the main dispatch center and is responsible for national, state and local criminal information access and law enforcement services as well as providing payroll and insurance administration, and...*

This agreement also states that the Town has a duty to keep accurate records of all incidents dispatched and other information necessary for the Town and CCFD.

Additionally, and as mentioned above, documents reviewed by Engels show that CCFD has a bank account referred to as the "HCCFD Training Fund" (Hildale-Colorado City Fire District). This is the account for which Darger has a check card. In addition to being CCFD's elected secretary-treasurer, Darger is also the Colorado City Town Manager.

E-Mails

Your affiant knows via training and experience that it is common practice for parties to communicate information in an electronic and/or digital format known as E-Mail; or electronic mail as well as text messages. This E-mail may also include documents that are also in electronic or digital format. This information could be on the personal computers of the named parties as

well as the computers owned and operated by the **Colorado City Fire District/Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department.**

Authority to Copy and Examine of Digital and Electronic Records

As noted prior and contained on Attachment A, your affiant is requesting to seize and view information that could be contained on the fixed drive (hard drive) of various computers that are owned and operated by the **Colorado City Fire District/ Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department.** You affiant is also aware of the fact that the computers that are owned and operated by the **Colorado City Fire District/Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department** could be part of the critical infrastructure for the operation of **Colorado City Fire District/Department/ Hildale Fire District/Department/Colorado City-Hildale Fire District/Department.** Your affiant would then request authority to have an investigator trained in computer forensics and/or civilian computer forensic technician download/copy/image/mirror/ clone the hard drives of the computers owned and operated by the noted agencies. The computers would then be left in place and the copied information would be retained for later examination.

Your affiant would also request that the court grant the authority for an investigator trained in computer forensics and/or civilian computer forensic technician to view the seized hard drives, as well as other seized storage devices and electronic media as outlined in Attachment A, only for the data, files and information as outlined in Attachment A.

Your affiant knows by training and experience that the records, documents and items sought under Attachment A are the type of items that should be maintained in the normal course of business for the noted entities. Your affiant also knows that it is common for many persons in a supervisors and/or management capacity to keep computerized copies and or records of the noted items at their homes and transfer these files back and forth via internet and/or various other electronic storage devices as noted. Your affiant feels that there it is probable to believe that the items being sought could be located in the homes of **Jacob "Jake" L. Barlow** and **David William Darger** as well as the fire stations.

In addition to the above prior noted information supplied by your affiant, your affiant has contacted and consulted with Special Agent Kempley of the Arizona Attorney Generals Office

regarding this investigation and as such your affiants advises of the following.

After conferring with Kempley, Affiant is aware that in conducting a search of a computer system, locating particular records, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is not unusual for even a home computer system to contain one terabyte (1000 gigabytes) or more of data storage capacity on its hard drive, with additional records stored in the form of CD, DVD, external hard drive, flash media or other removable media. One terabyte of data is equivalent of over 476 million pages of information, if it was printed out. If those pages were stacked on top of each other, it would be the equivalent of almost 110 Sears Towers or if stacked end to end, would cover over 529 football fields. A one terabyte hard drive could contain as many as 900 full-length movies or 900,000 songs. The volume of data stored on many digital 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.

Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices 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 also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched.

Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that can be neatly segregated from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of

the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment.

Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device cannot be segregated from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment.

Digital device users can attempt to conceal data within digital devices 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 that the file contains text. Digital device 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. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Specialized forensic tools and personnel who have been trained in this field may be need to be utilized to access these files. Therefore, a substantial amount of time might be necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in slack space, which can include unused sectors and clusters at the end of the actual data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. 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 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.

Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will permit retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate

alteration of the records.

It is also common to store records in compressed formats, which require that appropriate software to uncompress each record before it can be viewed. It would be extremely difficult to secure the system on the premises during the entire period of the search, which can take days, or even weeks, depending upon the technical problems encountered.

Accompanying software must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software. It can be necessary to have the software which was used to create data files and records, in order to gain access to their contents. In addition, without examination, it is impossible to determine that storage media purporting to contain a standard commercially available software program has not been used to conceal evidence instead. System documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain and copy the records authorized to be seized.

Kempley is aware that because computer users often do not upgrade obsolete systems, situations can arise in which it is impossible to read storage media except upon the system which created it. The use of specialized software may be necessary to image and access these items.

A user may intentionally alter his system in order to prevent the records from being read by others. Based on the ways in which various types of computer technologies operate in storing or processing records, in Kempley's experience, it is common to find that specific records authorized to be seized are inextricably mixed or without difficult or extremely time consuming procedures are inseparable from other records, programs, or files (similar to a bound volume book containing financial records, addresses, a diary, and notes, for example). In that event, the storage medium containing items to be seized will copied as a forensic image and in later analysis, only the items authorized to be seized will be disclosed, printed out or otherwise copied for evidentiary purposes.

In order to determine which records those are, it is necessary to use the appropriate software to "open" and view the contents of each file; the file name in the directory is not a reliable indicator of the nature of its contents, especially where there may be a desire on the user's part to conceal certain records.

It is likely that any digital device seized will contain data of non-evidentiary value belonging to both the target and third parties. This review of this non-evidentiary data will be minimized to the extent that it falls within the scope of the warrant. Specialized computer forensic software will be utilized to narrow the files and remnants of files by employing the use of search terms and other filters to comply with the scope of the warrant. Only those files or remnants of files that appear to fall within the scope of the warrant will be provided to the case agent for further review. In computer forensics, hashing is a way to represent a piece of digital data (i.e. a file, a folder, a logical volume, a physical volume) with a unique numerical value by applying a mathematical algorithm to the data. When applied, a hash will generate a mathematical representation similar to a fingerprint. Two files with exactly the same bit patterns should hash to the same value using the same hashing algorithm. Hashing tools can be utilized to help exclude non-evidentiary items such as operating system files. There will be no use of hashing tools to

search for known contraband such as child pornography without specific authorization by the court supported by probable cause. Should evidence of other crimes be discovered in "plain view" while conducting a lawful search of the data, further search authorization will be sought from the court.

There is no need for the extra expense of a "wall" and "review team" or "filter team" in this matter as there is no known spouse, attorney, clergy, or physician privileged materials of the target or third parties expected to be located. In the event that such materials are located, they will be segregated and not viewed by the investigators. Therefore, it is appropriate for computer forensic examiners from the Attorney General's Office and/or the DPS Computer Forensics Lab at which they are assigned to forensically process these digital devices.

Based on the Affiant's experience both as an investigator and as a computer user, it is common for individuals who have computers or "electronic calendar\address books" to store in the memories of those devices their records of financial transactions and expenses, correspondence notes, memoranda, telephone and address databases, calendars, appointments, business and personal records of all types.

It is quite common for people with a home computer to advertise merchandise for sale, order goods and services, exchange correspondence and files, and pay their bills electronically.

Because of the convenience of storing a large volume of records electronically, it is your Affiant's experience that people store computer records for much longer periods than they would if they had to maintain the same volume of records in paper form. Kempley has examined computers which proved to contain computer evidence five years old and older. Because of the volume of stored material and the fact that the files authorized to be seized may not be readily identifiable from their filenames, and are unlikely to be stored together but instead dispersed throughout the entire hard drive(s), searching for and extracting specific files would be extremely time-consuming and may not even be technically possible without the special tools and resources of a forensic environment.

At present, your Affiant has no intention of reading any electronic mail other than that of email pertaining to the specific violations listed in this affidavit. In the course of the continuing investigation, if it appears that there is probable cause to believe that the electronic mail of the target or of other persons may contain evidence of other offenses; further application will be made to this court. It is requested that computer forensic examiners from the Arizona Attorney General's Office or the DPS Computer Forensics Lab be granted authorization to make "forensic images" of the server, hard drives, computer system and storage media including diskettes, CDs, DVDs or other media for forensic analysis and other items as noted in the items to be seized list.

After recovery of any hidden, deleted or erased data, computer forensic examiners will determine which files, communications, graphical images, multimedia items or documents found in the system constitute evidence of the offenses enumerated above. Evidence copies of the items relating to these offenses will be created and retained for further proceedings by the Arizona Attorney General's Office and or Arizona Department Of Public Safety. Only those items

described in the search warrant relating to the offenses will be copied. After completion of the evidence copies, the "forensic images" will be retained in evidence storage for later discovery and trial purposes. None of the contents of the forensic images, other than those which may be required for prosecution, will be displayed to any person other than the computer forensic specialist, case agents and prosecutor, or otherwise disclosed, used or copied.

The forensic examiner will document and save for future evidence review purposes: (1) a record of the content of the searches performed, and (2) a record of the matches found.Only those records, communications, etc. identified through this procedure and which, upon review, prove to be among those authorized to be seized, will be copied, displayed, printed out, or disclosed. Upon completion of the system analysis, the backup copies and forensic images will be impounded for future evidentiary and discovery purposes.

If the digital devices are seized pursuant to the search warrant (as opposed to being imaged on scene), the computer forensic personnel will initially search the digital device within a reasonable amount of time not to exceed 90 days from the execution of the search warrant. If, after conducting such an initial search, the case agents/computer forensic personnel determine that a digital device contains any data falling within the list of items to be seized pursuant to the search warrant the state will retain the digital device for further analysis. If the state needs additional time to determine whether the digital device is an item that contains any data falling within the list of items to be seized pursuant to this search warrant, it may seek an extension of the time period from the Court within the original 90 day period from the execution of the search warrant.

Upon completion of the forensic analysis, the forensic image, storage media, hard drive, etc. from which those evidence copies were made will be secured for future comparison with the evidence copies.

In the event that items seized are later determined not to contain data of evidentiary value, those items will be returned to the owner. The state may retain a forensic copy of the evidence in the event that the investigation reveals additional information that would require further review of those evidence items.

Affiant believes that the following information demonstrates good cause, pursuant to A.R.S. §13-3917 for permitting this warrant to be served at any time of the day.

Wherefore affiant prays that a search warrant issue commanding that an immediate search be made for the person, property or things herein described, of the persons, premises and building, and vehicles described, and that the same be arrested, or retained in the custody of affiant or in the custody of the agency which affiant represents and disposed of according to law, pursuant to A.R.S. § 13-3920.

W.T. Flanagan

Affiant
Investigator W.T. Flanagan
Mohave County Attorneys Office

Gary L Engels

Affiant
Investigator G. Engels
Mohave County Attorneys Office

SUBSCRIBED AND SWORN to before me this 4th day of April, 2010

R. Williams
Judge
Of Mohave County Superior Court

ATTACHMENT A

ITEMS TO BE SEIZED

Documents generated between August 1, 2004 and April 4, 2010 that deal with:

1: The expenditure and management of public monies and funds of and by the **Colorado City Fire District/Colorado City Fire Department/ Hildale Fire District/ Hildale Fire Department/ Hildale-Colorado City Fire District/Department, and/or any other name combination thereof, ("CCFD"),** as well as such documents and records as noted under paragraphs # 2-9, and generated, maintained and/or stored by the **CCFD**; such documents being in any format including, but not limited to, paper form or electronic/ digital format.

2: Salary and other compensation information of **Jacob "Jake" L. Barlow** and **David William Darger**, including but not limited to: W-2s, tax returns and forms, pay stubs, salary reports. Purchase receipts, credit card receipts, invoices, inventory sheets, reports, ledgers, spread sheets that denote items/equipment/furniture purchased by **CCFD** and/or funds expended by **CCFD** and/or expended by **Jacob "Jake" L. Barlow** and **David William Darger**.

3: Documents from **CCFD** denoting: travel and/or training, including, but not limited to: travel vouchers; travel receipts; invoices; travel claims; room-hotel-motel receipts; the names of parties who submitted any of the above for payment and/or reimbursement; certificates of training; brochures; flyers; letters; memos; training class rosters; and/or lists of subjects who attended training; group and/or class photos that could identify subject(s) at training.

4: Documents from **CCFD** dealing with the dispatching of fire department personnel, volunteers, and units, including, but not limited to: call logs; radio logs; trip sheets; dispatch logs; dispatch sheets; event logs; pager logs; incident logs. This includes: paper documents, documents in electronic/digital format, and audio recordings of transmissions between units, dispatch and personnel.

5: Monthly statements from financial institutions (including, but not limited to, Banks and Credit Unions), including, but not limited to: credit card statements; debit card statements; investment statements, and/or deposit and/or withdrawal slips and records for accounts in the name of **CCFD** and/or **Jacob "Jake" L. Barlow** and **David William Darger.** Including the authority to photograph, copy, and/or record any credit cards, financial cards, debit cards or the like associated with CCFD found on or in the possession of or at the residence of **Jacob "Jake" L. Barlow** and **David William Darger.**

6: List of employees and/or volunteers of **CCFD**, including names and radio call signs and/or employee numbers and/or other identifying numbers used by the **CCFD** to refer to an employee. Address books, rosters, spreadsheets, ledgers, whether in paper/printed and/or electronic/digital format.

7: Electronic / Digital Storage devices, including, but not limited to: CD's; DVD's; built-in computer hard drives (Fixed disk); portable storage devices, such as external hard disks,

ATTACHMENT A

ITEMS TO BE SEIZED

portable hard drives, thumb drives, flash drives, as well as floppy disks, diskettes, tape drives, tapes; and/or I-pods, that are in the possession and/or custody of and/or found at **CCFD** and/or that are in the possession and/or custody of **Jacob "Jake" L. Barlow** and **David William Darger.**

8: Documents either in paper form and/or electronic/digital format, including, but not limited to: audio and video recordings that would deal with **CCFD** meetings, including minutes of the meetings, resolutions, agendas for the meetings, purchase authorizations, and/or other types of documentation including policy and procedure for **CCFD** that would be used to denote the conducting of **CCFD** business.

9: Correspondence in paper and/or electronic/digital format, including, but not limited to: e-mails; memos; letters; notes; and/or other communications created by, received by, and/or sent by **Jacob "Jake" L. Barlow** and/or **David William Darger** dealing with any subject matter as noted in paragraphs 1-9 above.

10: Operating manuals, directions, instructions used in the operation of the various electronic devices, computers and media storages devices that are located and or seized. As well as such similar documents used for the use of various computer related software, programs to included but limited to Turbo Tax

And authorization to:

11: Photograph and/or video record the noted locations to be searched and the various items of property and/or equipment as located at those locations to be searched.

12: Image/copy/download, clone and examine the data, files, records and/or stored information from such devices as noted in paragraphs 1-9 above, as outlined in the Affidavit for Search Warrant.

COSTCO WHOLESALE

#672 ST GEORGE UT

Seasons Greetings & Happy Holidays

MEMBER #333362334000

5 @ 8.29			
	16889	KS TRAIL MIX	41.45 C
	28245	TRIPLE CHEX	6.99 C
	28245	TRIPLE CHEX	6.99 C
	28245	TRIPLE CHEX	6.99 C
	414314	VNTYHR NAPKN	7.99 A
	20474	ALMOND ROCA	8.69 C
	77421	SPIRAL HAM	25.76 C
	77421	SPIRAL HAM	24.98 C
	235883	BUNGEE	19.89 A
4 @ 6.49			
	323038	OLIVES	25.96 C
8 @ 11.69			
	151679	KS BELGIAN	93.52 C
10 @ 7.99			
	196651	CREPES TUN	79.90 C
	196651	CREPES TUN	7.99 C
VOID			
	196651	CREPES TUN	7.99-C
8 @ 9.79			
	218749	FRUIT MEDLEY	78.32 C
7 @ 17.39			
	219824	SMKD SALMON	121.73 C
	591	APPLE JUICE	5.99 C
	27380	KS JUICE	6.99 C
6 @ 5.99			
	603707	DILL PICKLES	35.94 C
	18328	CASHEWS	10.89 C
	114015	SAHALEVALDOS	8.99 C
	408306	CANON MP20HD	39.99 A
	12648	KS CUTLERY	8.99 A
6 @ 9.99			
	885567	CHOCOLATES	59.94 C
	962005	HLTHY CHOICE	9.95 C
4 @ 5.99			
	428437	XEROX PAPER	23.96 A
	958403	92BRT PAPER	27.49 A
	248046	SHEET PROT	8.99 A
	12648	KS CUTLERY	8.99 A
		SUBTOTAL	806.26
A	6.25%	TAX	9.14
C	4.25%	TAX	28.05
		TOTAL	[redacted]
VF	American Express		843.45

XXXXXXXXXXX1003 SWIPED
Seq#: 002831 Ref#: 545332
American Express Resp: AA

APPROVED
AMOUNT: $843.45

0672 004 0000000070 0337

CHANGE .00

TOTAL NUMBER OF ITEMS SOLD = 76
CASHIER: TOM H. REG# 4
[redacted] 19 0672 04 0337 70

ATTACHMENT B

Warehouse: 672
Sales Date: 12/22/08 Reg#: 6 Trans Type: Tender
Time: 17:47 Tran#: 421 Tender:
Total: 636.44 Operator: 123 Block:
Member #: 000333362334000 BARLOW, JAKE Mbr Type: Business
Tax: 35.08 Resale Total:

FSA/ EBT	Item	Description	Amount	Units
	12224	KS TRAIL MIX W/M&M 4LBS	32.07	3
	333075	SNACKSTERS 100CAL 30/22.2	31.96	4
	318523	LOC MARIA CREPES MILK AND	71.64	12
	25436	KS 21/25 CK SHRIMP 16/2#	79.96	4
	77421	KS SPIRAL HAM 4/9 LB RW	19.30	1
	77421	KS SPIRAL HAM 4/9 LB RW	20.52	1
	325795	SMARTPARTS 10.4" (T-DAY)	419.97	3
	368023	SMARTPARTS 10.4" DGTL FRM	120.00-	3-
	97705	FRESH HEN TURKEYS	11.70	1
	97705	FRESH HEN TURKEYS	11.49	1
	97705	FRESH HEN TURKEYS	11.47	1
	97705	FRESH HEN TURKEYS	11.28	1
		AMEX Card	636.44	

*** END OF REPORT ***

ATTACHMENT C