IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	CASE NO. 2:13-cr-144-MEF-TFM
	)	[wo]
EDMUND MCCALL	)	

RECOMMENDATION OF THE MAGISTRATE JUDGE

I. INTRODUCTION

Pursuant to 28 U.S.C. § 636(b)(1) this case was referred to the undersigned United States Magistrate Judge for review and submission of a report with recommended findings of fact and conclusions of law. On August 22, 2013, the Grand Jury for the Middle District of Alabama returned an indictment against Antonio Harris ("Harris") and defendant, Edmund McCall ("McCall" or "Defendant"). Count 1 of the Indictment alleges McCall and others conspired to use the mail and wire communications to execute a scheme and artifice to defraud the United States by filing false, federal income tax returns from 2010 through October 29, 2012. Count 2-6 of the Indictment alleges McCall and others executed the scheme and artifice to defraud the United States by 5 wire communications between January 16, 2012 and March 7, 2012. Counts 7 and 8 of the Indictment allege Harris and McCall engaged in identity theft and aggravated identity theft in relation to wire fraud. Counts 9 through 12 of the Indictment alleges Harris, McCall and others presented false claims against the United States by filing false tax returns between January 16, 2012 and February 29, 2012.

Counts 13 through 15 of the Indictment allege Harris filed false claims against the United States by filing false tax returns between January 30, 2013, and February 9, 2013.

On October 23, 2012, Postal Inspector J.D. Tynan ("Agent Tynan") applied for and received a search warrant to search the premises located at 2736 Ivy Chase Loop, Montgomery, AL 36117. The search warrant application was to search for evidence related to false claims against the United States (18 U.S.C. § 287), identity theft (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), wire fraud (18 U.S.C. § 1343), bank fraud (18 U.S.C. § 1344) and attempts to commit bank fraud (18 U.S.C. § 1349). The search warrant affidavit contains details from a historical investigation into each of the 6 enumerated crimes listed in the application. Generally, the affidavit traces how McCall and others, from 2007 through April, 2012, engaged in credit card fraud, bank fraud, and filing fraudulent tax returns from his residence 2736 Ivy Chase Loop, Montgomery, AL 36117

The Court convened an evidentiary hearing on the motion on December 4, 2013. Based on the evidence presented to the Court, arguments of the parties, and for the reasons stated herein, the Magistrate Judge recommends that the Motion to Suppress (Doc. 26) be **DENIED**.

II. FACTS

The facts relied on by the Magistrate Judge to issue the search warrant are contained in the affidavit in support of the search warrant. The affidavit is attached as Enclosure 1. In a nutshell, the first portion of the affidavit alleges that the investigation and a series of

interviews and proffer sessions between 2007 and 2012 reveal that McCall and others were engaged in credit card fraud and filing false federal tax returns. The affidavit reveals that McCall and others used two methods to commit credit card fraud. In the first method, the conspirators stole credit cards from the United States Mail and then executed a sophisticated scheme to obtain identification information about the intended recipient of the credit card which enabled the conspirators to use the fraudulently obtained credit cards to obtain money. In the second method, McCall and others obtained identification information about actual persons and then used the identification data to receive credit cards from various banks which the conspirators in turn used to obtain money.

III. ISSUE

McCall raises one issue for judicial review:

(1) Whether the search warrant affidavit was void for staleness.

IV. DISCUSSION

A. The Good Faith Exception allows admission of the evidence

The United States argued, without rebuttal from McCall, that the fruit of the search falls within the good faith exception. *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). The Magistrate Judge concurs. The Eleventh Circuit has interpreted the *Leon* "good faith exception" to stand for the principle that "courts generally should not render inadmissible evidence obtained by police officers acting in reasonable reliance upon a search warrant that is ultimately found to be unsupported by probable cause." *United States*

v. Martin, 297 F.3d 1308, 1313 (11th Cir. 2002) (citing *Leon*, 468 U.S. at 922, 104 S.Ct. at 3405). The *Leon* "good faith exception" applies in all but four circumstances:

> (1) where "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth";
>
> (2) "where the issuing magistrate wholly abandoned his judicial role in the manner condemned in";
>
> (3) where the affidavit supporting the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and
>
> (4) where, depending upon the circumstances of the particular case, a warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

Id. (citing *Leon*, 468 U.S. at 923, 104 S. Ct. at 3405) (internal quotation marks omitted).

Agent Tynan presented the facts which he and other law enforcement officers knew to a neutral and detached Magistrate who determined there was probable cause to believe that evidence of the crimes enumerated in the application would be found in McCall's home. Suppression therefore would not serve to deter any police misconduct. To the contrary, the entire body of Fourth Amendment law inasmuch as the exclusionary rule is concerned with respect to the most sacrosanct place -the home- is to encourage the police to disclose to a neutral and detached Magistrate the information known to law enforcement and the logical inferences to be drawn from the information which will in turn allow the judicial officer to make a probable cause determination. Other than staleness, McCall posits no reason that the warrant was improper. For reasons discussed herein, the Magistrate Judge finds the affidavit

did not rest on stale information or information so stale that a law enforcement officer could not reasonably rely upon the warrant.

Probable cause is a requirement placed upon government officials to justify intrusions upon private interests that are protected by the Fourth Amendment. *See Ornelas v. United States*, 517 U.S. 690, 695, 116 S. Ct. 1657, 1661, 134 L. Ed. 2d 911 (1996). The Supreme Court has found that precisely articulating what "probable cause" means is not possible because it is a "commonsense, nontechnical" concept that involves "'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" *Id.* (quoting *Brinegar v. United States,* 338 U.S. 160, 175, 69 S.Ct. 1302, 1311, 93 L.Ed. 1879 (1949)). The Supreme Court has stated that probable cause exists "where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found." *Id.* at 696, 116 S. Ct. at 1661 (citing *Brinegar*, 338 U.S. at 175–176, 69 S.Ct. at 1310–1311; *Illinois v. Gates*, 462 U.S. 213, 238, 103 S.Ct. 2317, 2332, 76 L.Ed.2d 527 (1983)); *see also United States v. Blasco*, 702 F.2d 1315, 1324 (11th Cir. 1983) ("Probable cause exists where the facts and circumstances within the collective knowledge of the law enforcement officials, of which they had reasonably trustworthy information, are sufficient to cause a person of reasonable caution to believe an offense has been or is being committed").

Prior to issuing a warrant, an impartial judicial officer must determine whether the police have probable cause to make an arrest, conduct a search, or seize "evidence, [. . .]

instrumentalities, fruits of crime, or contraband." *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301, 87 S. Ct. 1642, 1647, 18 L. Ed. 2d 782 (1967). The judicial officer is required to make an independent assessment of all of the facts and circumstances that are present in the warrant application, which includes the supporting affidavit(s), to determine if it "contains a sufficient amount of information to support a finding of probable cause." *Martin*, 297 F.3d at 1317. The evidence presented in the warrant application must provide the judicial officer with a "substantial basis" to determine that probable cause exists. *Jones v. United States*, 362 U.S. 257, 269, 80 S. Ct. 725, 735, 4 L. Ed. 2d 697 (1960) *overruled on other grounds by U. S. v. Salvucci*, 448 U.S. 83, 100 S. Ct. 2547, 65 L. Ed. 2d 619 (1980).

The facts relied upon by the Magistrate Judge to issue the warrant at bar are not in dispute, and are subjected to attack solely on grounds of staleness. Staleness is not subject to formulaic definition but rather turns on the facts and circumstances present. *See United States v. Harris*, 20 F.3d 445, 450 (11th Cir. 1994). Generally, ongoing criminal activity presents less of a staleness question. *United States v. Cherna*, 184 F.3d 403, 410 (5th Cir. 1999); United States v. Bervaldi, 226 F. 3d 1256 (11th Cir. 2000). Even when information becomes stale subsequent developments may refresh or revive the otherwise stale information. *United States v. Adames*, 56 F. 3d 1043, 1046 (8th Cir. 2002). The totality of the affidavit establishes that McCall and others have allegedly engaged in ongoing fraudulent activity from 2007 through 2012. Victim interviews a mere 5 days before the issuance of the warrant indicated that false tax returns were filed from McCall's residence. The scheme set

out in the affidavit leads the Magistrate Judge to conclude the criminal activity under investigation was ongoing, sophisticated and that evidence of the fraud under investigation, particularly electronic records would likely exist well past the time the Magistrate Judge issued the search warrant.

V. CONCLUSION

Accordingly, it is the RECOMMENDATION of the Magistrate Judge that the Defendants' *Motion to Suppress* (Doc. 26) be DENIED.

It is further ORDERED that the parties file any objections to the this Recommendation on or before **January 3, 2014.** Any objections filed must specifically identify the findings in the Magistrate Judge's Recommendation to which the party is objecting. Frivolous, conclusive or general objections will not be considered by the District Court. The parties are advised that this Recommendation is not a final order of the court and, therefore, it is not appealable.

Failure to file written objections to the proposed findings and recommendations in the Magistrate Judge's report shall bar the party from a *de novo* determination by the District Court of issues covered in the report and shall bar the party from attacking on appeal factual findings in the report accepted or adopted by the District Court except upon grounds of plain error or manifest injustice. *Nettles v. Wainwright*, 677 F.2d 404 (5th Cir. 1982); *see Stein v. Reynolds Securities, Inc.*, 667 F.2d 33 (11th Cir. 1982); *see also Bonner v. City of Prichard*, 661 F.2d 1206 (11th Cir. 1981, *en banc*) (adopting as binding precedent all of the decisions

of the former Fifth Circuit handed down prior to the close of business on September 30, 1981).

DONE this 19th day of December, 2013.

/s/ Terry F. Moorer
TERRY F. MOORER
UNITED STATES MAGISTRATE JUDGE

Enclosure 1

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

The undersigned, being duly sworn on oath, deposes and says: Fraudulent filing of Federal Income Tax returns and 2736 Ivy Chase, Montgomery, Alabama.

1. I, James D. Tynan, (Affiant) have been a United States Postal Inspector for over 10 years. I am currently assigned to the U.S. Postal Inspection Service Office in Montgomery, AL. As a Postal Inspector, I enforce federal laws relating to postal offenses. I investigate, among other things, incidents where the United States Mail is used for the purpose of transporting non-mailable matter, burglaries and robberies of post offices, credit card fraud, obstruction of mail, mail theft and identity theft.

2. This affidavit is made in support of an application for a search warrant of the residence, automobiles, curtilage, mail boxes, and any and all computers, cell phones, and or digital media located at 2736 Ivy Chase Loop, Montgomery, Alabama 36117 for evidence of violations of Title 18, United States Code, Section 287 (False Claims); Title 18, United States Code Section, 922(n), (Possession of a Firearm by a Prohibited Person); Title 18, United States Code, Section 1028A (Aggravated Identity Theft); Title 18, United States Code, Section 1029 (Fraud and Related Activity in Connection with Access Devices); Title 18, United States Code, Section 1343, (Wire Fraud); Title 18, United States Code, Section 1344 (Bank Fraud); and Title 18 United States Code, Section 1349 (Conspiracy to Commit Bank, Mail, and Wire Fraud). This case is a joint investigation among the U.S. Postal Inspection Service (USPIS), the U.S. Postal Service Office of the Inspector General (USPS-OIG), the U.S. Secret Service (USSS), and the Internal Revenue Service-Criminal Investigative Division (IRS-CID).

3. The following information has been personally obtained by me or has been provided to me by other members of law enforcement, fraud investigators, the IRS's Atlanta Scheme Development Center ("ASDC") and various victims. I have not included every fact known to me about this case; rather, I have limited this Affidavit to those facts relevant to the issuance of a Search Warrant.

4. This affidavit will show that Edmund McCall (McCall) was the leader of a well-organized group of individuals involved in an ongoing criminal enterprise with a common central location of 2736 Ivy Chase Loop in Montgomery, Alabama. 2736 Ivy Chase Loop is owned by and is McCall's residence. The investigation has also shown that at various times a number of the primary subjects of this investigation have used 2736 Ivy Chase Loop (McCall's residence) as their residence.

5. The subjects who have been so far identified as being part of this ongoing conspiracy are:

Edmund L. McCall aka Trey;
Roscoe McCall, a/k/a Razz;
Alonzo McCall;
Rosie Lee Murphy;
Daryl Murphy, a/k/a Debo;
Corey Harris, a/k/a Tazz;
Nakeshia Moore aka Keisha;
Andrew Milton Williams, a/k/a Drew, a/k/a Paul, a/k/a Loco;
Broderick R. Brown;
Vanessa Gordon; and
Rhashema Deramus

6. This case involves McCall, the previously mentioned subjects, and others stealing mail and credit information, obtaining fraudulent credit accounts, and fraudulently obtaining merchandise and cash from retail stores and banks. McCall and others are also involved in committing identity theft and filing fraudulent income tax returns to receive tax refunds from the United States Government. On October 18, 2012, McCall, Rosie Lee Murphy, Corey Harris, Nakeisha Moore, Andrew Williams, and Vanessa Gordon were all been indicted in case number 2:12cr204-MEF for conspiracy to commit bank and wire fraud in violation of Title 18 United States Code 1349, and several counts of Bank Fraud in violation of Title 18 United States Code 1344, and Aggravated Identity Theft in violation of Title 18 United States Code 1028A. This indictment is currently under seal and is awaiting execution of the arrest warrants.

Fraud involving credit cards operating from 2736 Ivy Chase, Montgomery, Alabama.

7. Through a series of interviews and proffers between 2007 and 2009, co-defendants Rose Murphy (Murphy) and Andrew Williams (Williams) provided detailed information on how McCall ran the scheme, and operated it from his residence located at 2736 Ivy Chase Loop, in Montgomery, Alabama.

8. Affiant has learned through these proffers and interviews, and speaking with other witnesses and reviewing records that as part of the ongoing credit card criminal enterprise, McCall, the identified subjects, and others used Spoof Card's and Intelius.com's services. Spoofcard is a technology source that allowed one to change an outgoing phone number as well as one's voice. With the use of a Spoofcard, a male voice could be changed to a female voice. Also, when one placed a call from a phone, the Spoofcard would change the phone number so that it would appear on the receiving end caller id as a different phone number. Intelius.com is a people search website which for a fee would allow access to biographical

information of individuals, including the person's name, age, social security numbers and date of birth.

February 21, 2008, interview with Rose Murphy

9. Murphy explained to Affiant that a woman named Vanessa Gordon (Gordon) worked at the Shakespeare Station U.S. Post Office which services zip code 36106, and sometimes at the South Station U.S. Post Office which services zip code 36116. Both of these post offices are in the city of Montgomery, Alabama. Gordon reportedly held out mail which contained credit cards and placed them in an unused or dummy post office box which the co-conspirators had a key to. Murphy explained that the normal procedure was that Roscoe McCall (Roscoe) picked up the mail from the post office box and brought it to McCall.[1] McCall had three computers in his house, one desk top and two laptops. Once McCall received the stolen mail and the credit card numbers he would use one of the computers at his residence to access Intelius.com. McCall would input the victims' name and address into the database and would then obtain their birth date and address.

10. McCall would then call Corey Harris (Harris) in Atlanta and would pass the victims' personal information along with the stolen credit card numbers to him. Harris in turn would then call his wife Nakeisha Moore (Moore) who worked at Georgia Natural Gas. Moore would run a credit check on the victims and obtain the social security numbers and other related information. Moore passed the information to Harris who passed the information to McCall. Murphy related that when McCall had the name, address, social security number, and phone number of the victims, he would then use his Spoof Card account, call the credit card companies and activate the cards. The fraudulently obtained cards were then sent to various addresses, including McCall's residence, all without the consent and knowledge of the victims'.

[1] Roscoe is McCall's cousin.

11. Murphy witnessed McCall order credit cards online from HSCB and Citibank approximately two weeks before Valentine's Day 2008. Murphy stated that she had made several trips to Atlanta to pick up the identifying information from Harris to deliver to McCall. Murphy said Harris sometimes put the information into a hand held device that was locked by a password. Murphy said she brought the device to McCall in Montgomery. McCall typed in a password to retrieve the biographical information Harris' wife had obtained on the victims. Murphy stated it was her understanding that if someone entered an incorrect code on the device, it would lock the user out *(most likely, this device is encrypted in some manner)*.

May 23, 2008 interview with Rose Murphy

12. On May 23, 2008, Rose Murphy contacted Affiant and reported that prior to her calling him she had been inside McCall's residence at 2736 Ivy Chase Loop. Murphy witnessed McCall go into the master bath and open the tank part of the toilet and pull out a grey credit card. She witnessed him go underneath the sink and pull something out of a brown box and immediately stick the item in his pocket. Murphy also reported that she witnessed McCall get an ID card out of a box that holds DVDs.

June 5, 2008 interview with Andrew Williams

13. On or about June 5, 2008, Williams confessed to Affiant that at McCall's request he set up UPS box located at 2731 E. Blvd, Box 124, in Montgomery, Alabama to receive credit cards for McCall. He stated that McCall ordered the majority of the credit cards. Williams set up the box in the name of Donald Watkins. Williams said that McCall taught him how to do order credit cards by "walking him through it" on his laptop computer. Williams gave the following information which was consistent with Murphy's earlier statements: a) The normal procedure was that Roscoe picked up the mail from the post office box and brought it to McCall; b) McCall would then call Harris in Atlanta and would pass victim's personal

information along with the stolen credit card numbers to him; c) Harris would call Moore who worked at Georgia Natural Gas, and she would run a credit check on the victims and obtain the social security numbers and other related information; d) Moore passed the information to Harris who passed the information to McCall; and e) Once McCall had the name, address, social security number, and phone number of the victim, he would then use his Spoof Card account to call the credit card companies and activate the cards.

14. The investigation revealed that Moore was employed by (GNG) through Alliance Data Service. Between on or about April and June 2008, GNG had Moore's work computer forensically examined by Norcross Group. Multiple credit reports and similar information was the remnants of an apparent instant message which related to the access and purchase of personal information were found on her computer. They also found a message on her computer which stated in part that "I heard what happened to you and Taz…I am willing to restart our old deal of $50 for every ss and dob that you give me from a name and address, I can afford to give you up to $1500 per month if you want the work."

April 24, 2009 through June 23, 2009 proffer sessions with Rose Murphy

15. During proffer sessions in 2009, Murphy reported that she had seen McCall with $40,000 cash which he obtained from gambling and dice, making fake IDs, and filing fraudulent income tax refund checks. He was also involved in a scam involving PayPal, and he purchases reloadable visa cards as part of the scheme to defraud. Murphy stated that she has seen guns in McCall's residence and described a safe built into the wall of the closet in the master bedroom. Murphy described McCall's plans to damage his computers if the "feds kicked in his door."

Fraudulent filing of Federal Income Tax returns from 2736 Ivy Chase, Montgomery, Alabama.

16. During 2010 and 2011, Secret Service and IRS-CID worked an investigation on Rhashema Deramus (Deramus) who was involved in stealing identities and filing false tax returns. On or about August 29, 2012, Deramus entered a plea of guilty to a number of fraud related charges under case number 2:11-cr-0198. Deramus participated in a number of proffer meetings between November 2011 and January 2012. According to Deramus, McCall suggested to her that she use Tax Act software to prepare the tax returns. Deramus also claimed she witnessed a skinny black male, Jay LNU, in McCall's residence preparing tax returns on a computer. Deramus stated that McCall stores personal identifying information on a thumb drive and instructed Deramus that she should do the same. Deramus said that she witnessed McCall's thumb drive inserted into his computer at his residence while the skinny black male, Jay LNU, was preparing tax returns.

17. Deramus reported that McCall suggested that she use Card Flex as the depository for tax refunds. McCall explained to Deramus that he started a fake company and contracted with Card Flex to provide payroll cards for fake employees, and then he had refunds deposited on those cards. McCall sold Deramus ten cards for $1,000. Deramus had tax refunds deposited to McCall's cards, but when she went to cash out the cards, there was no money on the cards. Deramus stated that McCall ripped them off, having transferred the money off the cards.

June 27, 2012 proffer with Rose Murphy

18. During a proffer session on July 27, 2012, Murphy stated that McCall and other individuals were currently into income tax fraud and using pre-paid cards. Murphy claimed they used Green Dot cards in 2009 but went away from those to Wal-Mart type pre-paid cards. Murphy stated that McCall has some sort of electronic device in which he stores income tax fraud related information and that he has this device buried in the back yard of his home near a real mean dog. Murphy said the last time she was actually inside of

McCall's residence was August 2011 but the last time she was at the house was May 24, 2012.

19. On or about October 11, 2012, IRS-CID Agent Chris Forte, received subpoenaed records from Charter Communications bearing on the Internet Protocol (IP) address 68.190.23.66. Charter records showed that IP address 68.190.23.66 was assigned to McCall at 2736 Ivy Chase Loop, Montgomery, Alabama 36117 from at least March 4, 2012 through May 23, 2012. During that time IRS records provided by the ASDC indicated that at least 21 federal income tax returns were filed from McCall's IP Address for the year 2011. The 21 returns filed from the IP Address claimed a total of $31,067 in refunds. All of the returns listed Georgia addresses and wage amounts between $8,900 and $10,200 and all claimed a refund. On or about October 19th, 2012, ASDC verified that all 21 tax refunds were generated using fictitious wages and are false.

20. On or about October 18 and 19, 2012, Agent Forte interviewed at least two guardians of individuals whose names income tax returns were filed from McCall's IP Address. Victim one's tax return was received by the IRS on March 6, 2012. Victim two's tax return was received by the IRS on April 2, 2012. Both of these individuals parents stated that they had not filed or authorized the filing of tax returns for tax year 2011 in their child's names and Social Security numbers, had not received the refunds generated by those returns, and that the returns were false. Each of these returns generated a refund in the amount of $1,467. Charter was able to confirm that the IP Address was assigned to Edmund McCall when both tax returns were received by the IRS.

21. Numerous false returns were filed from McCall's IP address at 2736 Ivy Chase Loop, in Montgomery, Alabama as recently as April 18th, 2012. Therefore, the computer or computers used to file those returns are likely at 2736 Ivy Chase Loop, Montgomery, AL

36117, along with other instrumentalities, evidence, and fruits related to those offenses. Additionally, based on my training and experience, individuals involved in a false refund scheme are likely to keep proceeds of the scheme, property derived from the proceeds, records and other evidence about the proceeds and transaction with the proceeds in their residence and vehicles.

22. Based on information received from Agent Forte, the following information about computers and electronic storage is relevant to this affidavit:

a. As described in Attachments A and B, this application seeks permission to search McCall's Residence and to seize any records found on the Premises, in whatever form they may be found. I submit that if a computer or other electronic medium is found on the Premises there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

b. As described above, I am aware that a computer or computers was used to file false tax returns, and there is probable cause to believe that such computers are McCall's Residence and will contain evidence about those filings.

c. According to Agent Forte, when an individual uses a computer to file false tax returns electronically, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. A computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

d. Based on discussions with Agent Forte, I have learned that 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 downloaded to a hard drive can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home 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.

e. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space--that is, in space on the hard drive that is not currently being used by an active file--for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

f. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often 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 or if a user takes steps to delete them.

23. Based upon the facts set forth in this affidavit, computer hardware, software, related documentation, passwords, data security devices and data were integral tools of these crimes and constitute the means of committing a crime as they are instrumentalities and evidence of the violations designated. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them, and Rule 41(e)(2)(B) specifically directs that warrants authorizing the seizure of electronic storage media or electronically stored

information include authorization for a later review of the material.

24. Based on my training and experience, and information provided by Special Agent Forte from a Computer Investigative Specialist with ten years of experience in the filed that there are several reasons why computer storage devices, related input and output peripheral devices, cellular telephones, smart phones, PDA's, software, documentation, and data security devices (including passwords) often must be seized to permit a subsequent, more thorough search and analysis by qualified computer experts in a laboratory or other controlled environment.

25. Therefore, it will be necessary to seize the computers that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

26. Searching computer systems for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these

difficulties, law enforcement intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

CONCLUSION

27. Based on the foregoing, I submit that probable cause exists to believe that instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Sections 287, 922(n), 1029, 1028A, 1343, 1344, and 1349, are presently located at the Premises. Therefore, I respectfully request that this Court issue a warrant to search the Premises, as further described in Attachment A, for instrumentalities, fruits, and evidence of crime as listed in Attachment B and to seize those items. Additionally, permission is sought to seize any computer hardware, computer software, and computer-related documentation located at the Premises described in Attachment A. A Computer Investigative Specialist will be used to initially conduct, to the extent necessary and possible, an on-site preview, and subsequently, to conduct an off-site, thorough forensic analysis, by using whatever data analysis techniques may be necessary to seize the evidence, fruits, and instrumentalities listed in Attachment B. Some of the terms used in Attachment B are further defined in Attachment C.

28. In addition to items stored on computers, and other such electronic devices, based on my training and experience and the facts set forth in this affidavit, it is my understanding that offenders of various fraud violations frequently keep documentation of their fraudulent activities. This crime sometimes involves computers, printers, fax machines, paper, and any other associated computer equipment. It is also my understanding there is a high likelihood that assorted mail items, applications, notes, documents, letters, correspondence, checks, charge cards, merchandise, receipts, billing statements, cash and other classes of mail matter will be found in McCall's located at 2736 Ivy Chase Loop, Montgomery, AL 36117. It is rare that all the names of victims are known at the time of the execution of search warrants

and often other victims are identified during the search. It is also my understanding that it is highly likely that items purchased with the fraudulent credit cards will be in the residences. Based on my experience, it is normally a possibility to trace an item back to a purchase location by obtaining serial numbers and other identifying items. It is also a normal occurrence that individuals who purchase large ticker items, like a plasma television, would keep records of the purchase, even it were fraudulent, in their home and/or their vehicles.

29. Also, based on my experience, I have found that offenders of these types of violations often do not realize the incriminating nature of some items they purchase or maintain. Often offenders attempt to dispose of some items they feel is incriminating by shredding documents, throwing items away at locations other than there own, as well as other methods. Offenders often do not realize the evidentiary value of their own bank and phone records, manuals and documents of purchases of large items, warranty information of merchandise, hotel and travel records, gambling receipts and records as well as other items. These items are normally maintained in the offenders' residence and are normally maintained for a long period of time.

30. Based on my training and experience and the facts set forth in this affidavit, I submit there is probable cause to believe that evidence of false claims, credit card, bank, mail, and wire fraud exists along with income tax fraud and is located at the residence of Edmund "Trey" McCall located at the address of 2736 Ivy Chase Loop, Montgomery, Alabama 36117. I respectfully request the issuance of a search warrant for the residence, automobiles, curtilage, and any and all computers, cell phones, and or digital media located at 2736 Ivy Chase Loop, Montgomery, Alabama 36117.

ATTACHMENT A – PLACE TO BE SEARCHED

The place to be searched is 2736 Ivy Chase Loop, Montgomery, Alabama 36117, including any abutting yard and any structures on the property, curtilage, automobiles, mail boxes, and any and all computers, cell phones, and or digital media located in 2736 Ivy Chase Loop, Montgomery, Alabama. The residence is a red brick home with white columns on the front of the home. The residence has a white front door with a glass window in the middle of the door. A photograph of the residence is attached below.

ATTACHMENT B – ITEMS TO BE SEIZED

The items to be seized constitute fruits, instrumentalities, and evidence of crimes, for the period of approximately 2005 through the present, including, to wit: Title 18, United States Code, Section 287, False, fictitious or fraudulent claims; Title 18, United States Code, Section 641, Public money, property, or records; Title 18, United States Code, Section 1343, Fraud by wire, radio, or television; and Title 18, United States Code, Section 1028, Fraud and related activity in connection with identification documents, authentication features, and information. Specifically, the items to be seized are:

1. Computer hardware, computer software, computer passwords and data security devices, computer related documentation, cameras (including digital and video, as well as DVR and video surveillance equipment), "Smart" telephones, cellular phones and other mobile devices, and electronic storage devices, used as an instrumentality or containing evidence of such offenses, including:
    a. Evidence of identity, including who used or owned the computer, such as user accounts, logs, registry entries, Internet usage records, usernames, logins, passwords, e-mail addresses and online identities, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;
    b. Evidence of on-line statements, solicitation, persuasion, or inducement, such as online chats in chat rooms and internet websites, electronic mail, diaries, address books, names, and lists of names and addresses of individuals contacted;
    c. Evidence of knowledge and intent, such as Internet activity, caches, browser history, and cookies, bookmarked or favorite web pages, search terms entered into Internet search engines, and user typed web addresses;

2. Books, records, documents, bills, receipts, data, images, videos or information relating to such offenses, including, but not limited to, any records or documents or other evidence regarding
    i. the filing of tax returns,
    ii. identity information (including but not limited to names, social security numbers, and dates of birth),
    iii. financial or other transactions involving fraudulently obtained funds, including any information regarding currency, checks (including U.S. Treasury checks), money orders, debit cards, stored value cards, or other financial instruments relating to illicit proceeds, including the use or spending of such proceeds (including but not limited to the purchase of vehicles).
3. Any federal or state income tax returns, tax return information, supporting information and documentation, including all drafts and final productions, along with all Individual Income Tax Declarations (Form 8453), Forms W-2, Forms 1099, Wage and Tax Statements, Refund Anticipation Loan applications or agreements, and similar forms, filed or not filed, and supporting work papers used in preparation of tax returns.
4. Any debit cards, Treasury checks, assorted U.S. currency, or other proceeds of the offenses.
5. Assorted mail items, applications, notes, documents, letters, correspondence, checks, charge cards, merchandise, receipts, billing statements, cash and other classes of mail matter.
6. Any firearms.

ATTACHMENT C – DEFINITIONS

The following definitions apply to this Affidavit and Attachments to this Affidavit:

a. "Computer," means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" in accordance with Title 18, United States Code, Section 1030(e)(1).

b. "Computer hardware" means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, self-contained laptop or notebook computers, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, keys and locks).

c. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware

may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

d. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including but not limited to P2P software.

e. "Internet Protocol address" or "IP address" means a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

f. "Online Chat Room" is defined as the real time visual interface which displays messages and responses of participants who are using online chat. Chat rooms are usually devoted to specific topics such as US politics; however, there are a number of general chat rooms which are devoted to any issue the participants wish to bring up. Participants usually communicate by typing their contributions into a simple text box line by line. The primary use of a chat room is to share information via

text with a group of other users. New technology has enabled the use of file sharing and webcams to be included in some programs and almost all Internet chat rooms or messaging services allow users to display and/or send pictures.

ATTACHMENT D

Which are (state one or more bases for search set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

false, fictitious or fraudulent claims,

concerning a violation of Title 18, United States Code, Section 287;

possession of a firearm by a prohibited person,

concerning a violation of Title 18, United States Code, Section 922(n);

aggravated ID theft,

concerning a violation of Title 18, United States Code, Section 1028A;

fraud with an access device,

concerning a violation of Title 18, United States Code, Section 1029, and

fraud by wire, radio, or television,

concerning a violation of Title 18, United States Code, Section 1343, and

bank fraud,

concerning a violation of Title 18, United States Code, Section 1344, and

conspiracy to commit bank, mail and wire fraud,

concerning a violation of Title 18, United States Code, Section 1349.