

**FILED**

AO 91 (Rev. 11/11) Criminal Complaint

**UNITED STATES DISTRICT COURT** 2017 JUN -6 PM 5: 02

for the

Middle District of Florida

US DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
ORLANDO, FLORIDA

United States of America  
v.

Case No.

6:17-mj- 1461

RONNIE ROLLAND MONTGOMERY  
JOHN PIERRE MACK III

*Defendant(s)*

**CRIMINAL COMPLAINT**

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of at least May 2016 to the present in the county of Orange, and elsewhere, in the Middle District of Florida, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1349	Conspiracy to commit wire fraud.

This criminal complaint is based on these facts:

Continued on the attached sheet.

  
*Complainant's signature*  
 James Grundy, Senior Special Agent  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 6/6/2017

  
*Judge's signature*

City and state: Orlando, Florida

Karla R. Spaulding, United States Magistrate Judge  
*Printed name and title*

**STATE OF FLORIDA**

**COUNTY OF ORANGE**

**CASE NOS:** 6:17-mj-1461  
6:17-mj-1462  
6:17-mj-1463  
6:17-mj-1464

**MASTER AFFIDAVIT**

I, Senior Special Agent James Grundy, being first duly sworn, do hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. This affidavit supports an application for arrest warrants of Ronnie Rolland MONTGOMERY and John Pierre MACK III for violations of Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud) and an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises known as 55 West Church Street, Apartment 2712, Orlando, Florida 32801(hereinafter PREMISES 1); 140 Briarcliff Drive, Kissimmee, Florida 34758 (hereinafter PREMISES 2); and 1666 West Holden Avenue, Apartment 247, Orlando, Florida 32839 (hereinafter PREMISES 3), further described in Attachments A-1, A-2, and A-3, respectively, for things described in Attachment B. All properties are located in the Middle District of Florida.

2. I am a Senior Special Agent (SSA) with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI). I am currently assigned to the Office of Professional Responsibility (OPR), Office of the Resident Agent in Charge (RAC), San Diego, California. From June 2010, to April 2015, I worked as a Special Agent for DHS, HSI, San Diego, California. From January 2006 to June 2010, I worked as a Special Agent for the Drug Enforcement Administration, Los Angeles, California. I have a Bachelor of Science in Finance from San Diego State University, San Diego, California. I have received training from the Federal Law Enforcement Training Center in the area of cybercrimes, financial, and impersonation investigations. I have conducted investigations involving computer/cybercrimes. Throughout my tenure with HSI and DEA, I have participated in, and led, numerous investigations involving financial crimes and narcotics. As an OPR Senior Special Agent assigned to the RAC San Diego, I investigate criminal violations related to impersonation of law enforcement and related cybercrimes, including violations pertaining to conspiracy, in violation of Title 18, United States Code, Section 371, impersonating a law enforcement officer, in violation of Title 18, United States Code, Section 873, extortion through interstate communications, in violation of Title 18, United States Code, Section 875, receiving proceeds of

extortion, in violation of Title 18, United States Code, Section 880, blackmail, in violation of Title 18, United States Code, Section 912, wire fraud, in violation of Title 18, United States Code, Section 1343 and conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349. As a federal agent, I am authorized to investigate violations of laws of the United States and I am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. In preparation of this affidavit, I have discussed the facts of this case with other law enforcement agents, including officers within HSI and the Office of Professional Responsibility (OPR).

**PURPOSE OF AFFIDAVIT**

3. Based on the information below, I have probable cause to believe that Ronnie MONTGOMERY and John Pierre MACK III, committed violations of Title 18, United States Code, Sections 371 (conspiracy), 873 (blackmail), 875 (extortion), 880 (receiving the proceeds of extortion), 912 (impersonating a federal officer), 1343 (wire fraud), and 1349 (conspiracy to commit wire fraud). Based on the information below, I have probable cause to believe that evidence of the aforementioned crimes is maintained at PREMISES 1, 2 and 3, including on electronic and other storage media.

4. This affidavit is based upon information I have gained through training and experience, as well as upon information relayed to me by other individuals, including law enforcement officers. As this affidavit is being submitted for the purpose of securing search and arrest warrants, I have not included each and every fact known concerning this investigation but have set forth only the facts that I believe are necessary to establish probable cause to believe that there is evidence relating to potential violations of Title 18, United States Code, Sections 371, 873, 875, 880, 912, 1343 and 1349 at PREMISES 1, 2, and 3, and that a violation of Title 18, United States Code, Section 1349 was committed by MONTGOMERY and MACK III.

**FACTUAL BASIS FOR PROBABLE CAUSE**

5. On or about August 17, 2015, the Joint Intake Center (JIC) received a complaint from an individual (hereafter referred to as V1). V1 stated that an "agent" claiming to be from HSI's Cyber Crime Center (C3) contacted him and extorted money from him. V1 stated the "agent" identified himself as "Agent Charles Roberts" and demanded \$500 in order to mitigate a pending arrest warrant for V1. HSI agents found no record of an agent named "Charles Roberts" listed within HSI or C3. V1 sent \$500 per the "agent's" instructions via MoneyGram, from a Walmart in Marina, California. V1 stated the "agent" used phone number (407) 731-7186 to contact V1.

6. On November 24, 2015, I interviewed V1. V1 stated that during the month of July or August of 2015, he corresponded over email with a person that he believed to be an adult female. V1 met this person on the internet by responding to a personals post on Craigslist (a classified advertisements website).

7. V1 stated that approximately two days after his communications with this woman, he received a call from "911." When V1 answered, a male identified himself as "Charles Roberts," and claimed to be an "agent" assigned to the "C3 Child Exploitation Division" in Florida. The "agent" accused V1 of soliciting a minor on Craigslist and viewing a photo of the alleged minor. The "agent" claimed that he had an arrest warrant for V1 as a result of this violation and then proceeded to give detailed specifics about V1's employment.<sup>1</sup>

8. The "agent" told V1 that according to the C3 investigation, V1 had no prior criminal conduct and as a result, he spoke with a C3 supervisor who agreed to allow the warrant to be cleared if V1 promptly paid a \$500 fine. The "agent" emailed a copy of a "Warrant Purge" document to V1 reflecting what would be filed to nullify the warrant as long as the fine was paid. V1

---

<sup>1</sup> V1 thinks that "Agent Roberts" likely gained knowledge of his employment by querying V1's phone number, which is linked to V1's professional profile on the website LinkedIn.

stated the “Warrant Purge” displayed the DHS seal, a judge’s name, legal jargon related to child exploitation, and “Charles Roberts” was listed as an officer from the “C3” unit.

9. The “agent” directed V1 to go to any Walmart and told V1 to use MoneyGram to send the \$500, as MoneyGram was backed by the federal government and equipped to send the “agent” a secured payment. V1 completed the money transfer per the “agent’s” instructions. After V1 paid the fine, he took a closer look at the “Warrant Purge” and realized there were spelling errors in the document, and he came to believe it was a fraudulent document. The “agent” again tried to contact V1 to pay additional “fines,” but V1 did not respond. Instead, V1 reported the extortion to HSI in August of 2015.

10. On November 24, 2015, V1 provided a copy of an email he received from the “agent” on Saturday, August 1, 2015. The “agent” used the email address c3childexploitaiondivision@gmail.com [sic] to send a document to V1. The document displays the words “Warrant Purge” and reflects a payment of \$500. In summary, the “Warrant Purge” contains the DHS seal with the heading “IN THE DISTRICT COURT OF JUSTICE OF THE STATE OF California FIFTH DISTRICT August TERM 2015.” Within the body of the document, the investigating agent is identified as “detective

CHARLES ROBERTS EMPLOYED AND SWORN IN UNDER THE C3 CHILD EXPLOITATION UNIT.”

11. Based on the complaint filed by V1, my office launched an investigation into the suspect responsible for extorting money from V1. As a result of our investigation from 2015 through 2017, we identified numerous additional victims with similar complaints to that of V1. In addition, during the course of our investigation, we determined that the person claiming to be “Agent Charles Roberts” and/or “Special Agent Charles Roberts” was actually Ronnie MONTGOMERY. We learned that John Pierre MACK III and others known and unknown, assisted MONTGOMERY in this fraud. We also determined that MONTGOMERY used multiple other aliases to extort money from victims using the same scheme as described with V1. On several occasions, we used a cooperating victim to wire money to MONTGOMERY through multiple Walmarts in Osceola and Orange Counties (described below). Video footage from the Walmarts and surveillance efforts, compared to known photographs of MONTGOMERY and MACK III, identified both of them as being among the individuals who picked up the money sent by the victims.



**A. MONTGOMERY**

12. On February 16, 2016, I interviewed an additional victim (hereafter referred to as V2). V2 had also responded to an advertisement in the personals section of Craigslist in July or August of 2015. V2 gave an account similar to V1 about how he initially began communicating with a person he believed to be an adult female. He was then contacted by “Charles Roberts,” who identified himself as an “agent” with HSI’s C3 and accused V2 of soliciting a minor.

13. V2 confirmed he had also spoken with this “agent” on the phone, after receiving a call from phone number (407) 731-7186<sup>2</sup> during 2015. V2 said that thirty minutes before meeting with me on February 16, 2016, he had spoken to the “agent” who continued to identify himself as a “special agent” and asked V2 to let him know if any other federal law enforcement agencies approached V2. V2 also stated that “the agent” had changed his incoming telephone phone number several times since their initial phone conversation, but V2 said it was the same person, who V2 knew as “Special Agent Charles Roberts.”

---

<sup>2</sup> This is the same number that was used to contact V1. Area code (407) is based principally in Orlando, Florida, but also includes Orange, Osceola, and Seminole counties, which are all in the Middle District of Florida. Kissimmee is located in Osceola County.

14. V2 said he also sent money through MoneyGram to the “agent” to pay “fees” and “fines” as directed by the “agent.” Summons results from MoneyGram confirmed multiple transactions sent by V2 to “Charles Roberts” and picked up at a Walmart in Kissimmee, Florida. Specifically, on one occasion, V2 sent \$600 to a person named “Charles Roberts” on August 24, 2015. MoneyGram summons results reflected that someone named “Charles Roberts” using a telephone number of (407) 731-7186, (later determined to be MONTGOMERY as described herein), picked up the funds from the Walmart located at 904 Cypress Parkway, Kissimmee, Florida, on August 25, 2015. On August 26, 2015, MONTGOMERY posted a video, appearing to be self-produced, to a Facebook account named “Ronnie Montgomery.” The Facebook profile photograph for the account depicts MONTGOMERY. The video depicts MONTGOMERY picking up \$600 at an undisclosed Walmart in-store Money-Center. MONTGOMERY clearly states on the video, “this is basically like another day at the office for a dude....I done came here and took all your twenties in the last couple weeks.....The fruits of my labor I enjoy it while it’s still ripe.....I love making money.”

15. On February 18, 2016, I played the audio portion of MONTGOMERY's self-produced video posted to MONTGOMERY's Facebook account on August 26, 2015, to V1 and V2 (separately). Both V1 and V2 identified the voice on the recording as the caller known to them as "Agent Charles Roberts" and/or "Special Agent Charles Roberts" who posed as a Homeland Security agent.

16. On March 3, 2016, OPR SSA Jacqueline McBride accompanied Osceola County Code enforcement officers and met MONTGOMERY at his previous residence in Kissimmee, Florida, and during this meeting, she heard his voice. On March 11, 2016, she listened to a monitored consensual call between V2 and "Special Agent Roberts" and identified the voice of "Agent Roberts" as likely being the voice of MONTGOMERY, who was posing as an "agent" during the monitored call and extorting money from V2 during the call.

17. In early March of 2016, V2 received text messages from the man he knew as "Special Agent Roberts" from telephone number (760) 589-9145. "Special Agent Roberts" told V2 to send money in the form of two transactions, one for \$900 and one for \$300. "Special Agent Roberts" told V2 the fees included state and federal taxes and a "safe neighborhood fee." "Special Agent Roberts" instructed V2 that he should send one payment

utilizing the “Walmart to Walmart<sup>3</sup>” service and the other payment via MoneyGram, to a Walmart located in Kissimmee, this time addressed to “Wesley Baker.” On March 15, 2016, at the direction of HSI, and using official government funds, V2 sent two payments to “Wesley Baker,” one payment of \$900 using the Walmart to Walmart method and another \$300 payment via MoneyGram to a Walmart in Kissimmee, Florida.

18. On March 15, 2016, OPR SSAs conducted surveillance on MONTGOMERY at the Walmart located at 904 Cypress Parkway, Kissimmee, Florida. SSA McBride observed MONTGOMERY pick up the funds sent by V2 intended for “Wesley Baker.” Right after MONTGOMERY left the Walmart, HSI agents received transactional receipts from Walmart, detailing the money transactions sent from V2 to the name “Wesley Baker.” The receipt showed that MONTGOMERY placed an illegible signature on the receipts for the funds and the telephone number (760) 589-9145 on the store receipts for these transactions.

---

<sup>3</sup>I know based on my training and experience, that Walmarts have the capability to internally send funds from one Walmart location to another, making the funds available within ten minutes. This process is called a “Walmart to Walmart” transaction.

**B. MACK III**

19. On May 11, 2016, at the direction of HSI, and using official government funds, V2 made a payment of \$387 to a recipient named “Jake Sims” who received the payment on May 12, 2016, at a Walmart located at 8990 Turkey Lake Road, Orlando, Florida. Through subpoena research, I identified other payments sent to a “Jake Sims” by other probable victims. First, on May 12, 2016, someone claiming to be “Jake Sims” received a payment of \$957 at the Walmart located at 8990 Turkey Lake Road, Orlando, Florida. In addition, through summons research, SSA McBride identified a second payment received by someone claiming to be “Jake Sims” on June 2, 2016. Video surveillance of the transaction on June 2, 2016, which occurred at the Walmart store located at 3183 Vine Street, Kissimmee, Florida, depicts a person matching the physical characteristics of John Pierre MACK III entering the Walmart and receiving a payment of \$1940 in the name of Jake Sims. The person, believed to be MACK III, used a North Carolina Driver’s license (#xxxxxx943) issued in the name of Jake Sims. North Carolina records do not identify the license as a legitimate license issued by the State of North Carolina.

20. Through summons research, I identified a payment on May 18, 2016, made by another probable victim of the scheme. The payment for \$1567 was received in the name "Gary Stevens" at the Walmart located at 8990 Turkey Lake Road, Orlando, Florida. Video surveillance from May 18, 2016, at the Walmart on 8990 Turkey Lake Road, depicted a person exhibiting the physical characteristics of MONTGOMERY receiving the money, accompanied by a person exhibiting the physical characteristics of MACK III.

21. Through summons research, SSA Grundy identified a payment on May 16, 2016, made by an additional probable victim of the scheme. The payment for \$200 was received in the name "Gary Stevens" at the Walmart located at 8990 Turkey Lake Road, Orlando, Florida. Video surveillance from May 19, 2016, at the 8990 Turkey Lake Road Walmart, depicted a person exhibiting the physical characteristics of MONTGOMERY receiving the \$200 payment, accompanied by a person exhibiting the physical characteristics of MACK III. A still surveillance photograph depicted both individuals leaving the 8990 Turkey Lake Road Walmart's parking area in a vehicle matching the physical characteristics of a Dodge Challenger, dark in color.

22. Through summons research, I identified a payment on August 19, 2016, made by a probable victim of the scheme. The payment for \$600 was sent to the name "Gary Stevens" at the Walmart located at 5734 South

Orange Blossom Trail, Orlando, Florida. Video surveillance from August 19, 2016, at the 5734 South Orange Blossom Trail Walmart, depicted a person exhibiting the physical characteristics of MONTGOMERY receiving the money, accompanied by a person exhibiting the physical characteristics of MACK III. Video surveillance also depicted both persons departing the Walmart parking area in a vehicle matching the physical characteristics of a dark colored Dodge Challenger that appeared to be the same vehicle observed from the May 16, 2016, Walmart transaction.

23. Florida Department of Highway and Motor Vehicles (FL-DHBMV) shows a record indicating John Pierre MACK III owns a Blue, 2013, Dodge Challenger, assigned Florida license plate number Q21BB, registered to PREMISES 2.

24. On September 7, 2016, HSI interviewed a confidential source, after identifying him/her as being a member of MONTGOMERY and MACK III's scheme (hereafter referred to as CS1). Specifically, HSI determined that CS1 picked up funds sent by V2 during MONTGOMERY's extortion of V2. CS1 agreed to cooperate with the investigation. CS1 was not paid for his/her cooperation nor promised anything in return for his/her cooperation. CS1 advised agents that he/she has known MONTGOMERY for several years. CS1 said that beginning in 2014, through the date of our

interview, MONTGOMERY often worked in concert with MACK III, to extort money from victims solicited through personal advertisements on Craigslist and other on-line internet forums. CS1 stated MONTGOMERY and MACK III initially posed as females and would then impersonate law enforcement to extort payments from victims, who would pay the money to avoid prosecution for either prostitution or solicitation of underage females. CS1 stated MONTGOMERY, MACK III, and others would specifically impersonate agents working for the Cyber Crimes Center. CS1 also stated MACK III, a Florida National Guard Reservist, targeted military personnel because they possibly faced greater punishment for allegations of soliciting a minor.

25. U.S. Department of Defense records indicate John Pierre MACK III received a General Discharge, on October 19, 2016, from the Florida National Guard. A review of MACK III's Official Military Personnel File indicates he was discharged due to persistent absence without leave (AWOL). Additionally, agents saw that MACK's discharge papers were sent certified mail to the same address as listed on the 2013 Dodge Challenger vehicle records (PREMISES 2).

26. On May 4, 2017, I interviewed an additional victim (hereinafter referred to as V3). V3 stated in 2014 he met a female persona on the internet



site Chat Avenue. V3 provided the persona with his cellular phone number and received a telephone call thereafter from an unknown number. V3 said the conversation escalated into discussing sexual activities and approximately fifteen minutes after V3 began talking, the persona claimed she was sixteen years old. V3 questioned the persona and asked if they should keep talking, after which a man claiming to be "Mike Steverson" immediately got on the telephone line. "Agent Steverson" claimed to be a federal agent assigned to the Department of Justice and said V3 was under arrest for soliciting a minor on the internet. "Agent Steverson" told V3 he could mitigate the arrest and have the charges removed from his record by paying fines. However, "Agent Steverson" said that if payments were not made, agents would show up at V3's home and arrest him.

27. V3 said he made several payments at "Agent Steverson's" direction, ranging from \$300 to \$500, until they told him the violation was paid off. Approximately six months after paying his purported final fine (i.e. sometime in 2015), V3 received a call from someone named James or David (he could not recall specifics) who claimed to be a federal agent assigned to the Department of Homeland Security (DHS). The "agent" stated V3 owed an additional \$1,600 to DHS which was due immediately. V3 stated he made a payment of \$1,600 the same day, as instructed. In addition, V3 said

approximately two weeks after making the \$1,600 payment, he received a text message from "Agent Steverson" who demanded an additional \$1,900.

28. Through summons research, I identified a payment made by V3 on January 6, 2016, for \$387, received in the name "John Mack" at an unknown Walmart location in Florida. I also identified an additional payment from V3 on January 15, 2016, for \$287, also received by "John Mack" in Florida. Summons research also identified a payment made by a probable victim of the scheme on January 2, 2016, for \$1847, received by "John Mack," who listed his address as PREMISES 2, and used Florida Driver's license number M-200-475-91-345-0 as identification. Through queries of FL DHMV records, I found a current, valid Florida Driver's icense, M-200-475-91-345-0, issued to John Pierre MACK III, at PREMISES 2.

29. On April 3, 2017, V3 sent a payment for \$550 to the name "John Mack" to a Walmart located at 3838 South Semoran Boulevard, Orlando, Florida. Video surveillance from April 3, 2017 at the 3838 South Semoran Boulevard Walmart, depicted a male, matching the physical characteristics of MACK III, receiving the money and presenting U.S. Passport #xxxxxx895 as identification. U.S. Department of State application records indicate a U.S. Passport #xxxxxx895 is issued in the name "John Pierre Mack", at PREMISES 2.

30. Through summons research, I identified a payment on May 1, 2017, for \$250, sent by a probable victim of the scheme, to a recipient named James Dickson. The victim sent the payment to the Walmart located at 3183 West Vine Street, Kissimmee, Florida. Video surveillance from May 1, 2017, at the 3183 West Vine Street Walmart, depicted a male exhibiting the physical characteristics of MACK III, receiving the money.

31. On May 19, 2017, based on a telephone call from V3 and "Agent Steverson" V3 made a payment for \$588.50, to a "James Dickson" at a Walmart located at 3250 Vineland Road, Kissimmee, Florida, under the supervision of HSI. Video surveillance from May 19, 2017, from the 3250 Vineland Road Walmart, depicted a person exhibiting the physical characteristics of MACK III receiving the payment.

**C. SUBJECT PREMISES 1 & 2**

32. Through summons research on June 2, 2017, I obtained lease records for PREMISES 1. Lease records indicate John Pierre MACK III leased PREMISE 1 from October 19, 2016, through May 22, 2017, at which time the tenancy converted to a month to month occupancy. Records also contain an Intent to Vacate, written by John MACK III, received by the property management company on June 2, 2017, indicating MACK III intends to move out of PRMISES 1 on or before June 14, 2017. MACK III

requested that the security deposit refund for PREMISES 1 be sent to PREMISES 2. Lease records also list the 2013 Dodge Challenger, Florida license plate Q21BB, as one of the vehicles authorized to park at PREMISES 1.

33. CS1 told me that CS1 had observed during 2017 that MACK III utilizes a laptop computer, multiple cellular telephones, and hand written notes to facilitate perpetuation of the fraud scheme from PREMISES 1. CS1 also indicated that one of the laptops that MACK III used appeared to have a Hewlett Packard emblem below the screen of the laptop. CS1 further indicated that MACK III stated to CS1 that he never destroys his records (when referring to information contained in his laptop and his cellular telephones).

34. HSI conducted surveillance on PREMISES 1 and PREMISES 2 from June 1-6, 2017. Agents noted that MACK III would spend the night at PREMISES 2, then go to PREMISES 1 during the day, and return to PREMISES 2 at night. For example, in the early morning hours of June 1 and June 5, 2017, agents observed the 2013, Blue, Dodge Challenger, Florida registration number Q21BB, parked in the yard, in front of PREMISES 2. Additionally, on June 5, 2017, agents observed the same 2013, Blue, Dodge Challenger, Florida registration number Q21BB, at PREMISES 1 (in the

designated spot for apartment #2712). Based on my training and experience, I believe that MACK III is in the process of moving between two residences and is likely storing his possessions at both locations (PREMISES 1 and 2).

**D. PREMISES 3**

35. On May 25, 2017, CS1 provided agents information indicating Ronnie MONTGOMERY resided at PREMISES 3. CS1 stated MONTGOMERY resided there with his fiancé. CS1 further stated that in April or May of 2017, CS1 observed MONTGOMERY utilizing a laptop computer, in PREMISES 3 to facilitate the scheme.

36. Through summons research on June 2, 2017, I obtained lease documents for PREMISES 3. Lease records indicate that R.F. (MONTGOMERY's girlfriend's mother) leased PREMISES 3 for the period of January 27, 2017, to January 26, 2018. Records also indicate the keys to PREMISES 3 were issued to MONTGOMERY's girlfriend (hereafter A.F.) on January 31, 2017. Open source database information indicates a current address for A.F. of PREMISES 3.

37. Through Facebook research on June 4, 2017, I identified a Facebook profile for A.F. I believe this profile belongs to A.F. because the Facebook profile photograph matches the Florida Driver's License photograph of A.F. (Fxxxxxxx501-0). The Facebook profile states "engaged

to Ronnie Montgomery” and lives in Orlando, Florida. Also on the A.F. Facebook page is a photograph of A.F. adjacent to a photograph of Ronnie MONTGOMERY.

38. V2 previously reported to me that he received text instructions from “Agent Roberts” on October 28, 2016, to transmit a payment of \$450.50 to “A.F.”; however, the payment was blocked for an unknown reason and was resent successfully by V2, on the same day, to “Ronnie Montgomery” as instructed by “Agent Roberts.”

39. Through summons research, I identified multiple payments made by probable victims of the scheme received by “A.F.” All of the following payments were sent to and received by “A.F.”: (1) \$450 on October 1, 2016, at the Walmart located at 3101 West Princeton Avenue, Orlando Florida; (2)/(3)/(4) \$950 on January 26, 2017, \$400 on January 28, 2017, and \$257.18 on January 29, 2017, at the Walmart located at 1101 South Goldwyn Avenue, Orlando, Florida; (5) \$850 on January 30, 2017, at the Walmart located at 2801 South Orange Avenue, Orlando, Florida; and (6)/(7) \$850 on February 1, 2017, and \$850 on February 2, 2017, at the Walmart located at 1101 South Goldwyn Avenue, Orlando, Florida. For all seven of the above payments, A.F.’s Florida DHMV issued Driver’s License (Fxxxxxxx501-0) was used to pick up the money.

40. On June 4, 2017, CS1 provided information to me that he/she believed that Ronnie MONTGOMERY was still residing in PREMISES 3.

**TECHNICAL TERMS**

41. Based upon my training and experience, I use the following technical terms to convey the following meanings:

- a. **IP Address:** The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term--IP addresses, while other computers have dynamic—that is, frequently changed –IP addresses.
- b. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**COMPUTERS, ELECTRONICS STORAGE,  
AND FORENSIC ANALYSIS.**

42. As described above and in Attachment B, this application seeks permission to search for records that might be found in PREMISES 1, PREMISES 2, and PREMISES 3, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).



43. *Probable cause.* I submit that if a computer or storage medium is found in PREMISES 1, PREMISES 2, and PREMISES 3, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, whether deleted or viewed via the Internet. Electronic files downloaded to a storage medium 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 forensic tools. This is because 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 storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium 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.

- c. Wholly apart from user-generated files, computer storage media—in particular, a computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

44. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in PREMISES 1, PREMISES 2, or PREMISES 3 because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium 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 traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and

the times the computer was in use. Computer file systems can record information about the dates files that were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus,

spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information

incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not

present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- f. The individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium 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 medium for evidence of crime. From my training and experience, I believe that 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.



45. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain

evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


47. Because several people may share PREMISES 1, PREMISES 2, and PREMISES 3 as residences, it is possible that PREMISES 1, PREMISES 2, or PREMISES 3 will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the

warrant applied for would permit the seizure and review of those items as well.

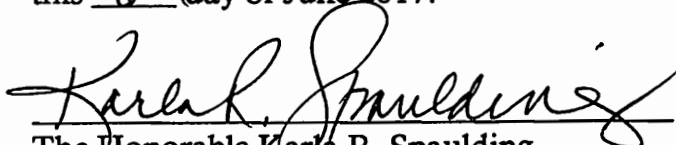
**CONCLUSION**

48. I submit that this affidavit supports probable cause to charge Ronnie Rolland MONTGOMERY and John Pierre MACK III with violating Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud), and that probable cause exists to search PREMISES 1, PREMISES 2, PREMISES 3 described in Attachments A-1, A-2, and A-3, respectively, and seize the items described in Attachment B.

WHEREFORE, I request that the court issue the requested warrants.

  
James Grundy, Senior Special Agent  
Homeland Security Investigations

Subscribed and sworn to before me  
this 6<sup>th</sup> day of June 2017.

  
The Honorable Karla R. Spaulding  
United States Magistrate Judge

**ATTACHMENT A-1**  
**(PREMISES 1)**

**Description of the Property and Premises to be Searched**

**55 West Apartment Complex**  
**55 West Church Street, Apt. 2712, Orlando, Florida, 32801**

The premises is located at 55 West Church Street, Apartment 2712, Orlando, Florida, 32801, on the property known as 55 West Apartments, at 55 W. Church Street, in Orlando, Florida.

PREMISES 1 is described as follows:

The apartment is a 1,288 square foot, two bedroom, two bathroom unit located on the 27<sup>th</sup> floor of a 31 floor, high rise luxury apartment complex at 55 West Apartments, 55 W. Church Street, Orlando, Florida.

**Photos on following pages**



**ATTACHMENT A-2**  
**(PREMISES 2)**

**Description of the Property and Premises to be Searched**

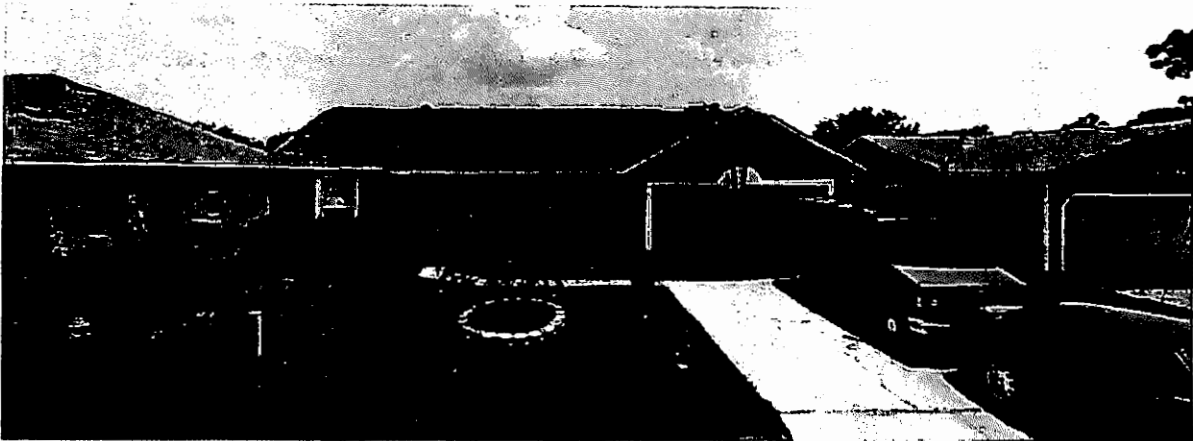
**140 Briarcliff Drive, Kissimmee, FL 34758**  
**(Legal Description: Poinciana V 2 NBD 3PB PPG 109 BLK 1256 LOT 8**  
**3/27/28)**

The premises located on the property known as 140 Briarcliff Drive, Kissimmee, Florida.

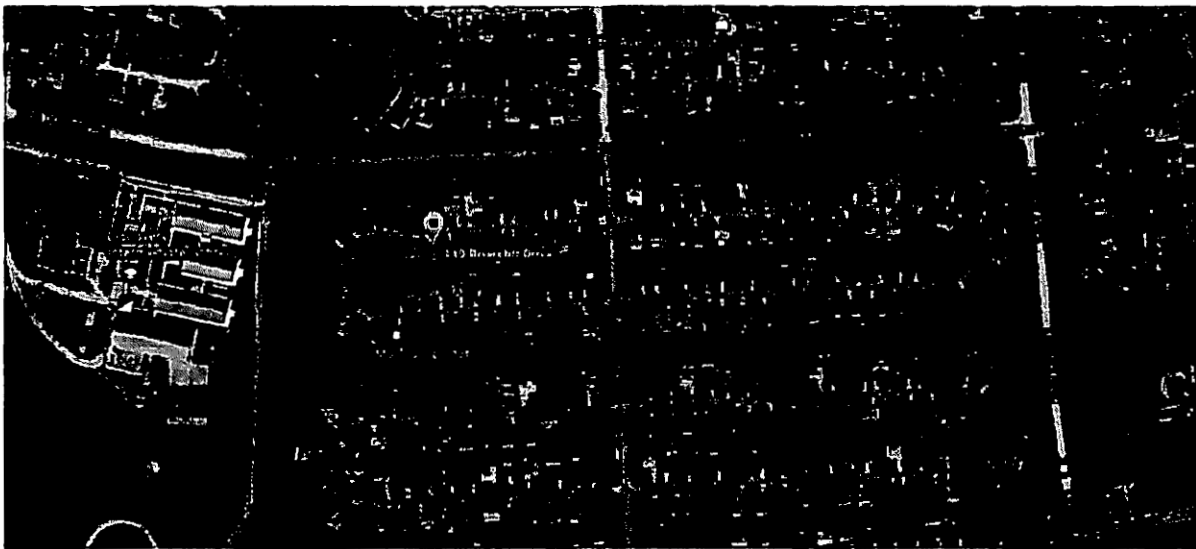
PREMISES 2 is described as follows:

The main residence is a 1614 square foot, three bedroom, two bathroom located on Briarcliff Drive in Kissimmee, Florida. It is a brown colored stucco one story single-family residence with white trim. The roof has lighter brown composite roof shingles. The house has an attached two-car garage with a white garage door. The residence has white numbers "140" displayed on the wall to the left of the garage door.

**Photos on following pages**



**AERIAL VIEW OF LOCATION OF TARGET RESIDENCE**





**ATTACHMENT A-3**  
**(PREMISES 3)**

**Description of the Property and Premises to be Searched**

**1666 West Holden Avenue, Apt 247  
Castilian Apartment Complex,  
Orlando, Florida 32839**

The premises is located at 1666 West Holden Avenue, Apartment 247, Orlando, Florida, 32839, on the property known as Castilian Apartments, whose main office address is 4700 Rio Grande Ave, in Orlando, Florida.

PREMISES 3 is described as follows:

The apartment is located in a large two-story multi-building complex apartment community with 304 units. Apartment 247 is located in the rear of Building 1666, on the first floor, with a unit number of "247" on a placard outside the door. The building is on 1666 West Holden Avenue, which is situated in the northwest corner of Castilian Apartment Complex located at 4700 Rio Grande Avenue, in Orlando, Florida.

**Photos on following pages**

Building Photo - Cashman Apartments in Orlando, Florida



**AERIAL VIEW OF LOCATION OF TARGET  
RESIDENCE**



**ATTACHMENT B**

1. All records and evidence relating to violations of Title 18, United States Code, Section 371 (conspiracy), Title 18, United States Code, Sections 873 (blackmail), 875 (extortion), 880 (receiving the proceeds of extortion), 912 (impersonating a federal officer), 1343 (wire fraud), and 1349 (conspiracy to commit wire fraud), from January 1, 2015, to the present, including:
  - a. Documents, records, evidence, and files, in whatever form, related to the above-listed offenses, the identification of co-conspirators, and the obstruction of this investigation.
  - b. Records and information relating to the email account:  
c3childexploitaiondivision@gmail.com
  - c. Records and information relating to the identity or location of co-conspirators, including, but not limited to, Ronnie Rolland MONTGOMERY, and John Pierre MACK III.
  - e. Financial Records - Records including, but not limited to, bank account records, deposit statements/slips, receipts, checks, ledgers, cash receipt books, bank statements, bank books, check books, check registers, savings pass books, withdrawal slips, certificate of deposit documents, wire transfers, cashier's checks, money orders, financial statements, credit applications, loan documents, loan payments, loan statements, invoices and/or bills for services, invoices and/or bills for expenditures, and other records of income and expense.
  - f. Accounting Records - Accounting records, specifically financial statements, ledgers, journals, check registers, notes, correspondence and other books in electronic and paper form.
  - g. Cash - Any and all cash proceeds.
  - h. Off-site Locations - Documents and records pertaining to any off-site locations to store records, including (1) safe deposit box keys, records, and receipts, and (2) rental agreements and invoices for storage facilities.
  - i. Other Documents and Correspondence - Documents, notes, e-mails, letters, facsimiles, text messages, photographs, correspondence, or any other type of communication among any potential co-

conspirators or between any co-conspirators and potential victims regarding the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Computer"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indication how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER, or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;

j. records of or information about the COMPUTER's Internet activity, including firewall caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including and form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes and physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

**ATTACHMENT B**

1. All records and evidence relating to violations of Title 18, United States Code, Section 371 (conspiracy), Title 18, United States Code, Sections 873 (blackmail), 875 (extortion), 880 (receiving the proceeds of extortion), 912 (impersonating a federal officer), 1343 (wire fraud), and 1349 (conspiracy to commit wire fraud), from January 1, 2015, to the present, including:
  - a. Documents, records, evidence, and files, in whatever form, related to the above-listed offenses, the identification of co-conspirators, and the obstruction of this investigation.
  - b. Records and information relating to the email account: c3childexploitaiondivision@gmail.com
  - c. Records and information relating to the identity or location of co-conspirators, including, but not limited to, Ronnie Rolland MONTGOMERY, and John Pierre MACK III.
  - e. Financial Records - Records including, but not limited to, bank account records, deposit statements/slips, receipts, checks, ledgers, cash receipt books, bank statements, bank books, check books, check registers, savings pass books, withdrawal slips, certificate of deposit documents, wire transfers, cashier's checks, money orders, financial statements, credit applications, loan documents, loan payments, loan statements, invoices and/or bills for services, invoices and/or bills for expenditures, and other records of income and expense.
  - f. Accounting Records - Accounting records, specifically financial statements, ledgers, journals, check registers, notes, correspondence and other books in electronic and paper form.
  - g. Cash - Any and all cash proceeds.
  - h. Off-site Locations - Documents and records pertaining to any off-site locations to store records, including (1) safe deposit box keys, records, and receipts, and (2) rental agreements and invoices for storage facilities.
  - i. Other Documents and Correspondence - Documents, notes, e-mails, letters, facsimiles, text messages, photographs, correspondence, or any other type of communication among any potential co-

conspirators or between any co-conspirators and potential victims regarding the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Computer"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indication how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER, or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;

- j. records of or information about the COMPUTER's Internet activity, including firewall caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
  - k. contextual information necessary to understand the evidence described in this attachment.
3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including and form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes and physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.