SEALED

AO 106 (Rev. 04/10) Application for a Search Warrant

FILED

SEP 12 2013

JULIE A. RICHARDS, CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

1 White AT&T Samsung Galaxy Note, Model No. SGHI717, Serial No. R21C25LHDMR, IMEI No. 352013050527388; AND
1 iPhone, Model No. A1387, Serial No. C38H5ESADTD3, IMEI/MEID No. 99000109045220, FCC ID No. BCG-E2430A

Case No. 5:13mj1904

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A and the Affidavit, both incorporated herein by reference

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B and the Affidavit, both incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 472	Passing, uttering, publishing, selling, possessing, and concealing counterfeited U.S. currency.

The application is based on these facts:

See Affidavit and Attachments A-B, all incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Joshua Pruett, SA, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: 11 SEPT. 2013

Judge's signature

City and state: Raleigh, North Carolina

James E. Gates, US Magistrate Judge
Printed name and title

SEALED

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

I, JOSHUA PRUETT, a Special Agent with the United States Secret Service in Raleigh, being duly sworn, depose and state the following:

A. IDENTITY AND EXPERIENCE OF AFFIANT

1. Your affiant, Joshua Pruett, is a Special Agent with the United States Secret Service (USSS), and has been so employed since March of 1998. I am currently assigned to the Raleigh Resident Office. In my capacity as a Special Agent (SA), I routinely investigate violations of federal law, specifically financial crimes and fraud. As a USSS agent, I have frequently encountered and investigated subjects responsible for possessing, passing, and manufacturing counterfeit United States Federal Reserve Notes (CFT FRNs).

B. PURPOSE OF THE AFFIDAVIT

2. This affidavit is submitted in support of an application to seize and search the contents of certain electronic storage devices ("ESDs"), defined below, that are presently in the custody of the USSS at the Raleigh Resident Office, located at 4700 Falls of Neuse Road, Suite 295, Raleigh, within the Eastern District of North Carolina. The ESDs came into the possession of the USSS as a result of a consent search of a vehicle, executed by the Granville County Sheriff's Office,

pursuant to a traffic stop on Interstate 85 near exit 193 in Granville County, North Carolina.

3. Based on my investigation to date, and that of other investigators, as set forth in this affidavit, it is my belief that the items to be searched, specifically, the ESDs referenced herein, are likely to contain evidence of violations of Title 18, United States Code, Section 472, which makes it a crime to knowingly and with intent to defraud:

- Pass, utter, publish, or sell, or
- With like intent bring into the United States or
- Keep in possession or conceal any falsely made, forged, counterfeited, or altered obligation or other security of the United States.

4. The information in this affidavit is based on my personal knowledge and information provided to me by other law enforcement officers. This information is provided for the purpose of establishing probable cause. This information is not a complete statement of all the facts related to this case.

C. **ITEMS TO BE SEARCHED / ELECTRONIC STORAGE DEVICES**

5. Your affiant seeks authority to search the following ESDs in the custody of the USSS, each of which was originally seized by the Granville County Sheriff's Office as part of a consent search incident to a traffic stop. The ESDs were in the possession of suspects Deshawn Chancy and Taurean Ghee and were

located both on their persons and within a red Chevrolet Camaro in which they were traveling. Each of these items is tagged with USSS Case Number J-133-711-23332-002. The items to be searched are set forth below:

- 1 White AT&T Samsung Galaxy Note, Model No. SGHI717, Serial Number No. R21C25LHDMR, IMEI No. 352013050527388; and
- 1 iPhone, Model No. A1387, Serial No. C38H5ESADTD3, FCC ID No. BCG-E2430A.

The above ESDs have been in the possession, custody, and control of the USSS since January 23, 2013. At present, the batteries on the ESDs are completely discharged.

6. On February 4, 2013, on the government's application, the Court authorized the search of the above ESDs, together with an additional ESD (a Black Micro 2GB pq1 SD card). However, the above ESDs, the Samsung Galaxy Note and iPhone, were subsequently found to be password-protected and locked. To date, efforts by USSS personnel to access these mobile devices have been unsuccessful as a result. The condition of the devices has not changed during this intervening time period.

D. INITIAL INVESTIGATION OF SUSPECTS GHEE AND CHANCY

7. On June 8, 2012, your affiant received an anonymous tip from a male caller who contacted the USSS Raleigh Resident Office stating an individual named Taurean Ghee was in

possession of a large quantity of $50 CFT FRNs. The caller reported that Ghee frequents a barbershop located on Trawick Road next to the Star Bar in Raleigh, NC. At this barbershop, Ghee spends time with the owner named "Brian" and they both are believed to be involved in the sale of these $50 CFT FRNs.

8. On June 11, 2012, the Raleigh Resident Office began to identify a significant rise in $50 CFT FRNs being passed in this district. These notes were being turned over to the USSS by area financial institutions, merchants, and other law enforcement agencies. Two of the notes were passed as payment for car repairs at two separate businesses, both claiming to have received them from an individual identified as Taurean Ghee. The first business was Colonial Tire and Automotive located at 2105 Highway 54E, Durham, NC 27713. They reported receiving three $50 CFT FRNs from Ghee on May 14, 2012 as payment to repair a 2008 Honda Accord license plate "YNH 8478," belonging to Deandra Antoinette Walker of 2311 Lancer Drive. It was later learned that Deandra Antoinette Walker is Ghee's wife. The second business was Meineke Car Care located at 3908 Western Blvd, Raleigh, NC. A 2008 Honda Accord was also repaired as part of this payment.

9. On June 12, 2012, USSS SA Reynolds, of the Charlotte Field Office, contacted your affiant and notified him that the Concord Police Department (CPD) had identified several suspects

responsible for passing $50 CFT FRNs at area Wal-Mart stores to purchase numerous Apple iPads. These items were ultimately returned to various Wal-Mart stores in exchange for genuine U.S. currency. The CPD identified the three suspects and obtained warrants for their arrest. Two of the suspects were identified as Lamel Truesdale and Deshawn Chancy. SA Reynolds forwarded the Raleigh Resident Office a list of the serial numbers appearing on the $50 CFT FRNs in his case. When compared to the batch of $50 CFT FRNs recently received by the Raleigh Resident Office, several serial numbers were identified as being the same.

10. On June 23, 2012, after being arrested in Raleigh, North Carolina, on the previously detailed open warrants for passing CFT FRNs in Concord, North Carolina, Lamel Truesdale was interviewed by USSS SA Craig Korcz. The following are among the statements made by Truesdale during this interview:

- Truesdale makes $1500 every two weeks for washing cars for an individual identified only as "Brian"
- Taurean Ghee is the main organizer of the CFT FRN scheme in the Raleigh area
- Deshawn Chancy is the next person under Ghee in the hierarchy of the CFT FRN scheme in the Raleigh area and Chancy drives a Red BMW 528

- Chancy usually hangs out a place called the Star Bar and that this is where there is CFT in the Raleigh area

E. INVESTIGATION LEADING TO ESDs TO BE SEARCHED

11. On January 23, 2013, Granville County Sheriff's Deputy Josh Freeman contacted your affiant regarding a vehicle stop in progress. Deputy Freeman stopped a vehicle traveling southbound on Interstate 85 near exit 193 for failure to move over for a law enforcement vehicle. The vehicle was a red Camaro registered to Enterprise Leasing Company and it was being driven by Deshawn Chancy with Taurean Ghee riding in the passenger seat. Deputy Freeman spoke with Chancy regarding the circumstances surrounding his recent travels and issued him a citation for the traffic violation.

12. At that time, Deputy Freeman noticed the odor of marijuana emanating from the vehicle and questioned Chancy about the smell. Chancy admitted that the smell was from marijuana smoked earlier that day. Chancy then gave Deputy Freeman consent to search his vehicle. Deputy Freeman discovered, among other items, approximately 20 Percocet pills bundled with an elastic band in a used fruit snack wrapper, along with $100 bills that he suspected as being counterfeit Federal Reserve Notes. Following this discovery, Deputy Freeman contacted your affiant to assist with this investigation.

13. At that time, your affiant and Special Agent Alan McDonald responded to the Granville County Sheriff's Office substation in Creedmoor, North Carolina, where Ghee and Chancy were being detained. Your affiant examined the bills recovered by Deputy Freeman while SA McDonald conducted a secondary search of the vehicle.

14. From the initial search conducted by the Granville County Sheriff's and the secondary search conducted by SA McDonald, the following items of note and the locations in which they were found were among the items discovered:

- miscellaneous documents found throughout the vehicle and on both suspects' persons to include retail store receipts for merchandise purchased with $100 and approximately $200 in cash;
- an iPhone belonging to Ghee and a Samsung Galaxy Note belonging to Chancy
- a micro SD Card found secreted in Chancy's wallet
- One $100 CFT FRN and $1,840.00 in genuine currency found in Ghee's front left pants pocket
- Twenty-seven $100 CFT FRNs and approximately 20 Percocet found in a brown paper bag, secreted in the headliner above the driver's seat, of which Chancy admitted ownership

- Three $100 CFT FRNs and $150 in genuine currency found in Chancy's wallet

- Two $100 CFT FRNs and $21 in genuine currency found in the interior pocket of a blue winter coat lying on the back seat of the vehicle, which was later identified as Ghee's coat by both Chancy and Ghee

15. Your affiant and SA McDonald were able to determine that thirty-three (33) of the $100 notes were counterfeited due to the fact that the watermark of the presidential portrait appeared inconsistent with those of genuine U.S. currency. Additionally, your affiant contacted Senior Investigative Assistant Lisa Johnson who then conducted a search of the USSS Counterfeit Tracking Application (CTA) database and determined that these thirty three (33) $100 CFT FRNs were part of the Russian/Israeli note classified as circular note C-23332. This determination was based on the quality of genuine note features that were present, as well as the consistent combination of currency identifiers. Additionally, it should be noted that the USSS CTA database demonstrated that over 2,500 of these $100 CFT FRNs have been passed in the Raleigh and Wilmington Resident Offices, both within the Eastern District of North Carolina, from September 11, 2011 through the present.

16. At that time, your affiant and SA McDonald interviewed Deshawn Chancy. To start, your affiant read Chancy the Warning

of Rights listed on the Warning and Consent to Speak form (SSF 1737B). Chancy stated, "I understand my rights," and agreed to speak with law enforcement but refused to sign the Waiver portion of this form.

17. Without notifying Chancy of the locations in which all of the $100 CFT FRNs were found, Chancy was then asked about a blue coat found on the backseat of the vehicle in which he and Ghee were riding. Chancy claimed that the coat belonged to Ghee, unaware that $100 CFT FRNs were found in the interior pocket.

18. Chancy then acknowledged ownership of the brown paper bag containing the Percocet and the $100 CFT FRNs discovered in the headliner of the vehicle. He explained that he received the CFT FRNs from an unknown individual to whom he sold earrings and a necklace in New York. He met this individual through a friend of his named "G" who helped him by posting his jewelry for sale on Craigslist.com. Chancy would not provide a description of the unknown buyer, nor could he provide a name or any other identifiable information for his friend "G".

19. When questioned further about details surrounding this sale and his acquisition of these CFT FRNs, Chancy first stated he met the unknown individual at the food court by the Chinese food establishment in Green Acres Mall located in Nassau County, New York. He stated this could be corroborated because he

purchased a pair of pants from Macy's prior to the transaction occurring. SA Pruett informed Chancy that law enforcement should be able to obtain surveillance video of the transaction from mall security. Chancy then explained that he did not meet "in" the mall but in the mall's parking deck near the food court. SA Pruett then stated that it is common for malls to have surveillance cameras in their parking decks and that surveillance footage should still be obtainable. Chancy then said that the exchange did not take place at that time; rather, instead of meeting the unknown individual at his red Camaro to complete the sale at that time, he met him in a black Camaro in the parking deck and led him to a nearby Applebee's where his Camaro, which contained the jewelry for sale, was located. Chancy did not clearly explain who the black Camaro belonged to or how it became involved in this incident but indicated that there were others present other than he and Ghee. Once at the Applebee's, Chancy stated he retrieved the jewelry, met with the unknown individual, and exchanged the jewelry for what he believed to be a total of $3,000 in $100 bills and the recovered bundle of Percocet in this sale. Chancy explained that he was confident in his recollection because he knew it was an even $3,000 that he was given. Additionally, he remembered removing and counting out $200 worth of these $100 bills and placing them in his pocket with the rest of his currency. Chancy was later

confronted with the fact that there was $300 in $100 CFT FRNs that was found mixed in with his genuine currency. Chancy explained this by stating he possibly made a mistake when counting out the bills. He also maintained that he was positive he only received $3,000 and that at no time did he do anything else with these notes other than putting the $200 or $300 in his pocket.

20. At that point, Chancy was confronted with the numerous inconsistencies in his version of recent events, as well as the events surrounding the $50 CFT FRN investigation that demonstrated his involvement, and he was asked if he would like to cooperate with law enforcement to help make amends for any wrongdoings. At that time, Chancy stated he would give law enforcement all of the information that would be needed for these investigations if he could, in turn, be promised that he would not be prosecuted and that he could leave at that moment. Your affiant explained that he could not make him that promise but any cooperation he would give would be relayed to the United States Attorney's Office for further consideration. Chancy indicated that he would not provide any further information at that time since his request could not be met. Your affiant then asked Chancy to provide a description of the person from whom he received the $100 CFT FRNs and Chancy began by stating it was a

black male. He then stopped and refused to provide any further description of the individual.

21. Continuing with this investigation, your affiant and SA McDonald interviewed Taurean Ghee. To start, your affiant read Ghee the Warning of Rights listed on the Warning and Consent to Speak form (SSF 1737B). Ghee signed the form and stated he understood his rights and was willing to speak with agents regarding this matter.

22. Ghee began by explaining that he and Chancy were pulled over by the Granville County Sheriff's Office as they were returning from a trip to New Jersey/New York. Ghee recalled they had left North Carolina for this trip on the previous Monday, January 21, 2013, and that they left to return to North Carolina earlier that day, Wednesday, January 23, 2013. The purpose for this trip was so that they could appear in court for a Driving Without a License charge they had received the week prior on a previous trip to New Jersey/New York.

23. Ghee then explained that while in New York/New Jersey, on Tuesday, January 22, 2013, he and Chancy traveled to a parking lot (not garage) near the Garden State Mall where Chancy called an unidentified male to meet him in furtherance of selling some of his jewelry. According to Ghee, no other individuals were present at that time other than him and Chancy. Sometime later, a dark-complexioned black male, in his mid-

twenties, with a medium build and short cut black hair, driving a Honda or Nissan compact car arrived at the parking lot. Chancy and this unidentified black male both got out of their respective vehicles and completed the sale. Ghee stated he could not hear anything that was being said but claimed he saw the black male hand Chancy the subject bills in exchange for his jewelry. Chancy in turn took the bills, balled them up and put them in his pocket. Ghee believed that Chancy received $3,150 or $3,250 in this exchange. Ghee claimed that he had no contact whatsoever with the unidentified black male.

24. Initially, Ghee stated that once Chancy received the bills and put them in his pocket, he no longer saw them. Then after further questioning related to his possible possession of these notes, Ghee stated he received $150 to $200 from Chancy to gamble with that evening. Ghee claimed that he gambled and won a couple of hundred dollars, ending up with $300 and change which he placed in his pants pocket. When asked if he was certain of this, Ghee reiterated that he "definitely" put the money he gambled with in his pants pocket. At this point, Ghee maintained that he was not involved with any criminal activity and then provided SA Pruett with limited personal history information.

25. Ghee then explained that the $1,840.00 in genuine currency found in his pants pocket was money he received in

furtherance of his bail bonds business. It should be noted that a search of the North Carolina Department of Insurance web-based search revealed that Taurean Ghee's bail bondsman's license lapsed in August 2012.

26. Ghee was then confronted with the fact that he has been the target of a USSS investigation into $50 CFT FRNs long before this incident with the $100 CFT FRNs. Ghee denied any wrongdoing and indicated that he had nothing further to add to these USSS investigations and stated that he was confident Chancy would take ownership of any CFT FRNs found in this incident. He made this claim without any certainty of where the CFT FRNs were all located, to include those found in his coat pocket and in his pants pocket. The interview was concluded at that time.

27. Following this interview with Ghee, your affiant spoke again with Chancy regarding his willingness to cooperate with this investigation. Chancy indicated that if he were released and allowed to keep his car, phone, and money that he would be able to "keep the ball rolling" and lead law enforcement to the source from whom he could purchase additional $100 CFT FRNs. Chancy would not provide any details pertaining to this source at that time. He explained that he would need his phone and money to set up another buy in New York, indicating that the necessary contact numbers were contained in the phone. After

discussing the facts of this case, the agents and deputies from the GCSO agreed to forgo charging Chancy at that time in furtherance of this investigation into the source of CFT FRNs in New York. It was then explained to Chancy that he would not be charged at that time so that he could attempt to get law enforcement additional leads in this matter. It was also explained that his currency and phone would be held for further investigation. Chancy indicated a willingness to cooperate and departed the GCSO annex at that time in the red rental Camaro.

28. Within thirty minutes of Chancy departing the annex, he contacted your affiant on a secondary cell phone and inquired about Ghee's status. In this and a subsequent telephone conversation between your affiant and Chancy over the next forty-eight hours, Chancy stated that he could purchase additional $100 CFT FRNs from the "Jews" in New York for $0.50 on the dollar and that these purchases are typically made in $5,000 increments. He also expressed concern over the genuine currency seized from him and Ghee stating that this was other people's money, and that he and Ghee were either using it in furtherance or as the proceeds of a CFT FRN scheme.

E. STATEMENT OF PROBABLE CAUSE TO BELIEVE ITEMS TO BE SEARCHED CONTAIN EVIDENCE OF CRIMES

29. Based upon the facts set forth above and my independent review of the evidence, there is probable cause to

believe that Deshawn Chancy and Taurean Ghee were operating a scheme to purchase, possess, and/or distribute CFT FRNs in violation of Title 18, United States Code, Sections 472.

30. Based upon my training and experience as a law enforcement officer, I have learned how CFT FRN operations are commonly conducted. Typically, a scheme to purchase, possess, and/or distribute counterfeit Federal Reserve Note operates based on a network of co-conspirators operating in different roles. Suspects who purchase, possess, and/or distribute CFT FRNs must first obtain the contraband notes by either manufacturing them or receiving them from a manufacturer/supplier. Once obtained, these contraband notes are then uttered for profit or are provided to other individuals who will in turn utter them for profit, providing the "middle man" with a portion of the profits obtained. It should also be noted that, based on your affiant's experience, it is common for suspects involved in criminal activity to secrete items of contraband in unconventional storage places, to include the headliner of a vehicle.

31. Additionally, based upon your affiant's training and experience as a law enforcement officer, I know that cellular telephones and other ESDs, such as Micro SD Cards, are commonly used by suspects operating a CFT FRN operation. First, the cellular telephones are used to communicate with other co-

conspirators involved in this scheme. Those suspects responsible for purchasing, possessing, and/or distributing CFT FRNs will make contact with co-conspirators via text messaging or via the telephone numbers stored in their contact lists. This communication is often in furtherance of negotiating the terms of the illegal transactions, receiving/delivering the CFT FRNs, or in managing the distribution or uttering of these CFT FRNs by other co-conspirators. Second, it is common that cellular telephones and other ESDs such as Micro SD Cards are used to store images of the CFT FRNs as well as images of other co-conspirators along with the CFT FRNs or merchandise purchased using the CFR FRNs involved in the scheme. These images are often used in e-mail or text communications to demonstrate the quality and quantity of the CFT FRNs involved, and to illustrate the "fruits" of the scheme.

32. In this case, both suspects have been linked to the purchase, possession, and/or distribution of CFT FRNs in several instances. Both were found in a vehicle containing a total of $3,300 in $100 CFT FRNs that can be attributed to both suspects. These notes were determined to be counterfeit based on the quality of genuine note features that were present, as well as the consistent combination of currency identifiers identical to the Russian/Israeli note classified as circular note C-23332 in the USSS CTA database. The statements provided by both suspects

explaining the origin of these CFT FRNs were inconsistent, thus bringing the credibility of their claims that they possessed no criminal intent into question. The fact that the majority of the notes were found secreted in the headliner of the vehicle suggests criminal intent on the part of the suspects. Additionally, suspect Chancy indicated that the two were involved in the purchase of $100 CFT FRNs from a source in New York, and that they were conducting this operation in conjunction with other unnamed individuals.

33. As noted above, the two previously listed phones and Micro SD Card were found in the suspects' vehicle. Both suspects acknowledged that cellular telephone communication was involved in the acquisition of the notes in question. Based on your affiant's training and experience, cellular telephones are frequently used in furtherance of CFT FRN cases to communicate with other co-conspirators in furtherance of the purchase, possession and sale/distribution of CFT FRNs. Additionally, these items along with the Micro SD Card discovered may have been used to store, transmit, or receive images of CFT FRNs and other co-conspirators in furtherance of or as a result of this scheme. There is probable cause to believe that the aforementioned cellular telephones and Micro SD Card were used in furtherance of a CFT FRN offense and will contain telephone

records that are evidence of crimes both known and unknown to investigators.

34. Finally, as noted above, the various ESDs were discovered at the scene of the search and all are capable of storing electronic data, including but not limited to evidence of the purchase, possession, and/or distribution of CFT FRNs. The data on each of these devices is voluminous and can easily be transferred from one device to another via various means. As such, a detailed electronic search of the ESDs is required as discussed in the following section.

F. SEARCH OF THE ESDs

35. There is probable cause to believe that suspects Chancy and Ghee also used the cellular telephones and related electronic storage devices found at the scene to collect, store, maintain, retrieve, conceal, transmit, and use electronic data relating to these offenses in the form of electronic records, documents, and materials, including those used to facilitate communications, each of which constitutes both the means of committing and evidence of the offense. These materials are all therefore subject to seizure and search pursuant to Rule 41 of the Federal Rules of Criminal Procedure, and may be retained as evidence and as instrumentalities used in the commission of a crime for a reasonable period of time and

must be examined, analyzed, and tested to preserve their evidentiary value.

36. **The volume of evidence**. As noted, electronic storage devices such, as hard disk, diskettes, tapes, Micro SD Cards, and CD or DVD ROMs laser disks, can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks to months, depending on the volume of data stored.

37. **Technical requirements.** Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert or experts should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even "hidden", erased, compressed, pass-word protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (either from external

sources or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit (CPU). In addition, the analyst needs all the system software (operating systems interfaces and hardware drives) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

38. **The compatibility of peripheral devices and software.** The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or OI/OO) devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above.

39. **Computer Search Protocol.** Your affiant states that the proposed search will be executed according to the Computer Search Protocol referenced in Attachment C to the Application.

G. CONCLUSION

Based on the information outlined above, there is probable cause to believe that the items listed in Attachment A to this affidavit, which are currently in the custody of the USSS at its

evidence vault in Raleigh, North Carolina, contain evidence of violations of Title 18, United States Code, Section 472 (Uttering Counterfeit Obligations or Securities). Therefore, your affiant respectfully requests that a search warrant be issued for the search of the ESDs contained in Attachment A, and to seize the items set forth in Attachment B, pursuant to the Computer Search Protocol referenced in Attachment C.

Assistant United States Attorney Adam Hulbig has reviewed this affidavit.

Joshua Pruett, Special Agent
United States Secret Service

Sworn to and subscribed by me this 11th day of September, 2013.

United States Magistrate Judge James E. Gates
Eastern District of North Carolina

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched consists of the following Electronic Storage Devices:

a. 1 White AT&T Samsung Galaxy Note, Model No. SGHI717, Serial No. R21C25LHDMR, IMEI No. 352013050527388 and

b. 1 iPhone, Model No. A1387, Serial No. C38H5ESADTD3, IMEI/MEID No. 99000109045220, and FCC ID No. BCG-E2430A.

These Electronic Storage Devices are currently located at the USSS Raleigh Resident Office, 4700 Falls of Neuse Road, North Tower, Suite 295, Raleigh, NC 27609.

This warrant authorizes the forensic examination of these Electronic Storage Devices for the purpose of identifying electronically stored data described in Attachment B.

ATTACHMENT B

EVIDENCE/ITEMS TO BE SEIZED

This Warrant authorizes (i) the search of the items listed in Attachment A for only the following and (ii) authorizes the seizure of the items listed in Attachment A only to the extent they constitute the following:

(a) evidence of violations of 18 U.S.C. § 472 ("subject violations"); or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT C

Computer Search Protocol

1. Definition of "Computer." Unless otherwise defined in the warrant, "computer" means any electronic, magnetic, optical, electro-chemical, or other data processing device performing logical or storage functions, and includes any information storage facility, communications facility, or other equipment or media directly related to or operating in conjunction with such device. "Computer" also includes the system software (*e.g.*, operating systems, interfaces, hardware drivers), applications software, and related instruction manuals or other documentation and data security devices (*e.g.*, passwords, keycards) needed to conduct the search authorized by the warrant. "Media"as used in this definition means all forms of material or devices that are capable of storing or preserving electronic information (*i.e.*, data of any kind).

2. On-Site Search. To the extent practicable, the computer described in the warrant shall be analyzed at the search site (*i.e.*, the location identified in the warrant) and not seized for analysis off-site. Alternatives to seizure for purposes of analysis off-site that may be considered by the government include, but are not limited to, the following:

(a) identification of a knowledgeable person at the search site who could assist the government in locating information subject to the warrant;

(b) use by the government of its own expert at the search site to locate the information subject to the warrant;

(c) creation at the search site of an electronic mirror image of those parts of the computer that are likely to contain information subject to the warrant and subsequent analysis of such mirror image copy off-site in lieu of the computer.

3. Seizure for Analysis Off-Site. If any computer subject to the warrant cannot practicably be analyzed at the search site, the warrant allows for seizure of such computer and its removal from the search site to a laboratory, controlled environment, or other off-site location for purposes of analysis. Such off-site analysis shall be completed as promptly as practicable. In the event of such seizure, the government shall furnish to the issuing Magistrate Judge every 30 calendar days after the warrant is returned a status update regarding the analysis being conducted, including an estimate of the additional time needed to complete the analysis. These updates shall continue to be submitted until the analysis is complete or

until further order of the court. If upon completion of the off-site analysis the government determines that the computer and the information stored in it are not subject to permanent seizure as contraband (*i.e.*, property used in furtherance of criminal activity), fruits of criminal activity, or on other grounds, the government shall return the computer to the person from whom or from whose premises it was taken. Such return shall be made as soon as practicable after completion of the analysis but in no event more than 10 calendar days thereafter unless a longer time is allowed by court order or agreement of the parties.

4. Seizure as Contraband or Instrumentality. The government may permanently seize a computer and information stored therein that the government identifies (in connection with either an on-site or off-site search) as contraband, fruits of criminal activity, or otherwise subject to permanent seizure if the warrant allows for such permanent seizure. If the warrant does not authorize such permanent seizure, the government shall obtain another warrant supported by probable cause authorizing permanent seizure before effecting it. If the computer had initially been seized only for purposes of analysis off-site, the government shall notify the issuing Magistrate Judge of its determination to permanently seize the computer and/or

information stored therein and may request that its ongoing obligation to report on its analysis of such computer cease.

5. Storage of Information on Seized Computer. The government shall make a copy of all information stored on the computer as soon as practicable after the computer's seizure except as otherwise provided by the warrant. Such copy shall not be analyzed by the government except as reasonably necessary to confirm that it is an accurate copy, but shall be retained until further order of the court as a record of the state of the computer and the information therein prior to any subsequent analysis by the government. **The government shall not reconfigure the computer until such copy has been made.**

6. Return of Information from Seized Computer. If any person from which or from whose premises a computer is seized either for off-site analysis or permanently so requests in writing, the government shall provide to the person within a reasonable time of the request copies of any requested information not subject to permanent seizure (as contraband, fruits of criminal activity, or on other grounds) that may reasonably be necessary or important to the continuing functioning of the person's legitimate activities. If the government withholds any information requested, it shall within a reasonable time of the request identify to the person making

the request the information being withheld and the reasons for withholding it.

7. Search Methodology. In conducting the search authorized by this warrant, whether performed on-site or off-site, the government shall make reasonable efforts to utilize a computer search methodology to search for and seize only that information which is identified in the warrant as subject to such search or seizure. The search methodology may include, but is not limited to, the following techniques:

(a) surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

(b) "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

(c) "scanning" storage areas to discover and possibly recover recently deleted data;

(d) scanning storage areas for deliberately hidden files; or

(e) performing key word searches through all electronic storage areas to determine whether

occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

8. Unopened Email. Except as expressly provided in the warrant, the warrant and this protocol do not authorize the opening and search of the contents of any kind of unopened electronic mail. In the absence of express authorization in the warrant, no opening and search of unopened electronic mail shall be conducted without a separate search warrant supported by probable cause.

9. Inventories: When a computer has been seized for analysis off-site, the government shall comply with Fed. R. Crim. P. 41(f) in the following manner:

(a) Initial Inventory. Following the on-site search and seizure, the government shall prepare the usual Rule 41(f) inventory of not only the property and items seized by it pursuant to the warrant, but also the information, which has, at that date, been identified as seized pursuant to the warrant. This inventory shall identify each computer that will be subject to further off-site analysis. For example, if the government makes an on-site mirror image of a computer for use in an

off-site analysis, the government need only list the making of the mirror image in the return, with an indication that it is subject to further searching pursuant to this warrant. The listing of any information that is seized from the computer off-site will then be made in the final inventory. The government shall give a copy of the warrant and this initial inventory of property seized to the person from whom or from whose premises the property was taken and make a return to the court, all as provided by Rule 41(f). Because of the nature of electronic or computer information, the listing of seized information in either the initial or final inventory may be made by copying the seized information to a computer diskette, compact disc (*i.e.*, CD), DVD, or like storage device and submitting it along with an affidavit which describes the contents of the storage device.

(b) Final Inventory. After completing the off-site analysis of the computer, the government shall prepare a final inventory of information seized during the off-site analysis. The government

shall deliver a copy of the final inventory to the person from whom or from whose premises the computer was taken and make a return of the original final inventory to the court. The court will then attach this final inventory to the original search warrant and initial inventory as an addendum.

10. Copy of Protocol to Searching Personnel. Counsel for the government shall take reasonable steps to ensure that a copy of this protocol is provided to the person or persons who perform the search authorized by this warrant.

11. Superseding Effect. This protocol supersedes any contrary terms set forth in the application for the search warrant, the supporting affidavit, or any attachments thereto.

SEALED

SEP 12 2013

JULIE A. RICHARDS, CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

IN RE: ORDER REQUIRING APPLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. ~~5:13-mj-1093~~ 5:13mj1904-2 APPLICATION Filed Under Seal

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby moves this Honorable Court pursuant to the All Writs Act, 28 U.S.C. § 1651, for an Order requiring Apple, Inc. ("Apple") to assist in the execution of a federal search warrant by bypassing the lock screen of an iOS device, specifically, an Apple iPhone.

BACKGROUND

The United States Secret Service (USSS) currently has in its possession an iOS device that is the subject of a search warrant issued by this Court on February 4, 2013.[1] The iOS device is an iPhone with Model No. A1387, Serial No.

[1] The Court ordered the search warrant to be executed on or before February 18, 2013 (Case No. 5:13-mj-1093). To account for the subsequent passage of time, the government has submitted - contemporaneously with the filing of the instant motion - a second search warrant application for this iOS device and one other cellular phone device (a Samsung Galaxy Note). The renewed application is identical in all material respects to the one which was presented to the Court on February 4, 2013.

C38H5ESADTD3, IMEI/MEID No. 99000109045220, and FCC ID No. BCG-E2430A (the "iOS device").

Initial inspection of the iOS device following the issuance of the search warrant revealed that it is locked. Because the iOS device is locked, law enforcement agents are not able to examine the data stored on the iOS device as commanded by the search warrant.

Apple, the creator of the iOS operating system and producer of the iOS device, may have the capability of bypassing the iOS device's lock and thereby retrieving data stored on the iOS device that is not currently accessible to USSS. This Application seeks an order requiring Apple to use any such capability, so as to assist agents in complying with the search warrant.

DISCUSSION

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under

appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice… and encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of *New York Tel. Co.*, this Court has the authority to order Apple to use any capabilities it may have to assist in effectuating the search warrant.

The government is aware, and can represent, that in other cases, courts have ordered Apple to assist in effectuating search warrants by unlocking other iOS devices under the authority of the All Writs Act. Additionally, Apple has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the iOS device be examined for evidence identified by the warrant. Examining the iOS device without Apple's assistance, if it is possible at all, would

require significant resources and may harm the iOS device. Moreover, the order is not likely to place any unreasonable burden on Apple.

Respectfully submitted this 10th day of September, 2013.

THOMAS G. WALKER
United States Attorney

ADAM F. HULBIG
Assistant United States Attorney
Criminal Division
310 New Bern Avenue, Suite 800
Raleigh, North Carolina 27601
Telephone: (919) 856-4530
Fax: (919) 856-4487
Email: adam.hulbig@usdoj.gov

SEALED

FILED

SEP 12 2013

JULIE A. RICHARDS, CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

IN RE: ORDER REQUIRING APPLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. 5:13mj1904-2 **ORDER**

Before the Court is the government's motion for an order requiring Apple, Inc. ("Apple") to assist law enforcement agents in the search of an Apple iOS device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Apple assist law enforcement agents in the examination of the iPhone with Model No. A1387, Serial No. C38H5ESADTD3, IMEI/MEID No. 99000109045220, and FCC ID No. BCG-E2430A (the "IOS Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Apple shall provide reasonable technical assistance to enable law enforcement agents to obtain access to unencrypted data ("Data") on the iOS Device.

FURTHER ORDERED that, to the extent that data on the iOS Device is encrypted, Apple may provide a copy of the encrypted data to law enforcement, but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data;

FURTHER ORDERED that Apple's reasonable technical assistance may include, but is not limited to, bypassing the iOS Device user's passcode so that the agents may search the iOS Device, extracting data from the iOS Device and copying the data onto an external hard drive or other storage medium that law enforcement agents may search, or otherwise circumventing the iOS Device's security systems to allow law enforcement access to Data and to provide law enforcement with a copy of encrypted data stored on the IOS Device;

FURTHER ORDERED that although Apple shall make reasonable efforts to maintain the integrity of data on the iOS Device, Apple shall not be required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents.

DATED this 11th day of SEPTEMBER, 2013.

United States Magistrate Judge James E. Gates
Eastern District of North Carolina

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

IN RE: ORDER REQUIRING GOOGLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. 5:13mj1904-1 **ORDER**

Before the Court is the Government's motion for an order requiring Google, Inc. ("Google") to assist law enforcement agents in the search of an Android device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Google assist law enforcement agents in the examination of the Samsung Galaxy Note with Model No. SGHI717, Serial No. R21C25LHDMR, and IMEI No. 352013050527388 (the "Android Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Google shall, if necessary, reactivate the Google account associated with the Android Device;

FURTHER ORDERED that Google shall: (1) provide a single password reset for the Android Device; (2) provide the new password to the law enforcement officer executing the search warrant; and (3) upon unlocking the Android Device, again reset the Google account password promptly upon notice that the imaging of the Android Device is complete, without providing it

to the law enforcement officer or agency so as to prevent future access;

FURTHER ORDERED that the reset process need not be unobtrusive to the subject, the subject may receive notice to one or more accounts of the reset, and such notice is not a violation of any seal or nondisclosure requirement;

FURTHER ORDERED that the law enforcement agent executing the search warrant is prohibited from using or attempting to use the new password to attempt to access the subject's online accounts other than as synchronized on and stored in memory within the Android Device at the time of execution of the warrant.

DATED this 11 day of SEPTEMBER, 2013.

United States Magistrate Judge James E. Gates
Eastern District of North Carolina

SEALED

FILED

SEP 12 2013

JULIE A. RICHARDS, CLERK
US DISTRICT COURT, EDNC
BY _____ DEP CLK

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

IN RE: ORDER REQUIRING GOOGLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT	Case No. 5:13mj1904-1 APPLICATION Filed Under Seal

The United States of America, by and through the United States Attorney for the Eastern District of North Carolina, hereby moves this Honorable Court pursuant to the All Writs Act, 28 U.S.C. § 1651, for an Order requiring Google, Inc. ("Google") to assist in the execution of a federal search warrant by bypassing the lock screen of an Android device, specifically, a Samsung Galaxy Note.

BACKGROUND

The United States Secret Service (USSS) currently has in its possession an Android device that is the subject of a search warrant issued by this Court on February 4, 2013.[1] The Android device is a Samsung Galaxy Note with Model No. SGHI717, Serial No. R21C25LHDMR, and IMEI No. 352013050527388 (the "Android

[1] The Court ordered the search warrant to be executed on or before February 18, 2013 (Case No. 5:13-mj-1093). To account for the subsequent passage of time, the government has submitted - contemporaneously with the filing of the instant motion - a second search warrant application for this Android device and one other cellular phone device (an iPhone). The renewed application is identical in all material respects to the one which was presented to the Court on February 4, 2013.

device"). Initial inspection of the Android device following the issuance of the search warrant revealed that it is locked. Because the Android device is locked, law enforcement agents are not able to examine the data stored on the Android device as commanded by the search warrant.

Google, the creator of the Android operating system and producer of the Android device, may have the capability of bypassing the Android device's lock and thereby retrieving data stored on the Android device that is not currently accessible to USSS. This Application seeks an order requiring Google to use any such capability, so as to assist agents in complying with the search warrant.

The United States requests that the Court order that Google, if necessary, must reactivate the Google account associated with the Android device for the limited purpose of complying with the search warrant.

Further, the United States requests that Google be directed to: (1) provide a single password reset for the Android device; (2) provide the new password to the law enforcement officer executing the search warrant; and (3) upon unlocking the target Android device, again reset the Google account password promptly upon notice that imaging of the phone is complete, without providing it to the law enforcement officer or agency so as to prevent future access.

Further, the United States represents that the reset process may not be unobtrusive to the subject and that the subject may receive notice to one or more accounts of the reset. Accordingly, the United States requests that the Court order that any such notice is not a violation of any seal or nondisclosure requirement.

Finally, the United States does not seek authority to use the new password to attempt to access the subject's online accounts other than as synchronized on, and stored in, memory within the Android device at the time of execution of the warrant, and it does not object to the Court prohibiting such use of the password to be provided by Google.

DISCUSSION

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service*, 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position

to frustrate the implementation of a court order or the proper administration of justice… and encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of *New York Tel. Co.*, this Court has the authority to order Google to use any capabilities it may have to assist in effectuating the search warrant for the Android device by unlocking the Android device.

The government is aware, and can represent, that in other cases, courts have ordered Google to assist in effectuating search warrants by unlocking other Android devices under the authority of the All Writs Act. Additionally, Google has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the Android device be examined for evidence identified by the warrant. Examining the Android device without Google's assistance, if it is possible at all,

would require significant resources and may harm the Android device. Moreover, the order is not likely to place any unreasonable burden on Google.

Respectfully submitted this 10th day of September, 2013.

THOMAS G. WALKER
United States Attorney

ADAM F. HULBIG
Assistant United States Attorney
Criminal Division
310 New Bern Avenue, Suite 800
Raleigh, North Carolina 27601
Telephone: (919) 856-4530
Fax: (919) 856-4487
Email: adam.hulbig@usdoj.gov