

FILED

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

2019 OCT 29 PM 2: 22

Middle District of Florida

United States of America

v.

DANIEL ZIRK

Case No.

6:19-mj-1775

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 September 25, 2019 in the county of Osceola in the
Middle District of Florida, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. § 2113(a)

Attempted bank robbery.

18 U.S.C. § 924(c)

Use of Firearm in furtherance of crime of violence.

This criminal complaint is based on these facts:

See attached Affidavit

☐ Continued on the attached sheet.


Complainant's signature

Brandon Bottom, FBI Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: 10-29-2019


Judge's signature

City and state: ORLANDO, FLORIDA

THOMAS B. SMITH, U. S. Magistrate Judge

Printed name and title

STATE OF FLORIDA

CASE NO. 6:19-mj- 1775 through 1779

COUNTY OF ORANGE

MASTER AFFIDAVIT

I, Brandan Bottom, being duly sworn, state the following:

Agent Background

1. I am a Task Force Officer with the Federal Bureau of Investigation ("FBI"), and have been since April 2013. I have been employed by the Orlando Police Department ("OPD") since May 2005 and am assigned to the OPD Criminal Investigations Division. Prior to being a TFO, I was assigned to the Orlando Police Department TAC unit. During this time I was responsible for investigating street level violent crime while being tasked to locate and arrest violent offenders. I have received extensive training pertaining to investigating criminal street gangs and violent crime organizations. I have participated in investigations involving, among other offenses, armed robbery, conspiracy, murder, witness tampering, home invasion, human trafficking, and money laundering.

2. I have also conducted investigations concerning the identification of co-conspirators through the use of interviews, telephone records and bills, financial records, ledgers, photographs, and other documents. I have also investigated violent robbery crews, and drug trafficking organizations, and other criminal organizations. I am experienced with the use of cellular telephone analysis and

current violent crime trends. I have also participated in the debriefings of arrested individuals who later cooperated with the United States Government.

3. My training and experience as an Orlando Police officer and an FBI TFO, together with the facts set forth herein, form the basis of my opinions and conclusions in this affidavit.

4. The information set forth herein is based on the following: (a) my own personal observations; (b) information that I received from other law enforcement officers involved in this investigation, including by reviewing official reports prepared by other law enforcement officers; (c) interviews of witnesses and the review of reports summarizing the interviews of witnesses; and (d) information provided to me by law enforcement officials who met with and interviewed said witnesses.

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a criminal complaint and search warrants, I have not set forth each and every fact that I learned as a result of this investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause that a violation of federal law has been committed. Unless otherwise noted, all statements of other persons described in this affidavit are set forth in substance and in part, rather than verbatim.

Purpose of Affidavit

6. As set forth below, there is probable cause to believe that on or about September 25, 2019, in the Middle District of Florida, DANIEL ZIRK ("ZIRK")

committed violations of 18 U.S.C. § 2113(a) (attempted bank robbery) and 18 U.S.C. § 924(c) (use of firearm in furtherance of crime of violence).

7. I also make this Affidavit in support of an application for a warrant to search the premises known as 436 Hallcrest Avenue, Spring Hill, Florida 34608 (the "PREMISES"), which are further described in Attachment A, for the things described in Attachment B.

8. I also make this Affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (321) 230-6458 ("SUBJECT PHONE 1") that is stored at premises controlled by AT&T, a wireless telephone service provider headquartered at 208 S. Akard St. Dallas, TX 75202. The information to be searched is described in Attachment C. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require AT&T to disclose to the government copies of the information further described in Section I of Attachment D. Upon receipt of the information described in Section I of Attachment D, government-authorized persons will review the information to locate items described in Section II of Attachment D.

9. I also make this Affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (352) 631-0614 ("SUBJECT PHONE 2") that is stored at premises controlled by T-Mobile, a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The information to be searched is described

in Attachment E. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment F. Upon receipt of the information described in Section I of Attachment F, government-authorized persons will review the information to locate items described in Section II of Attachment F.

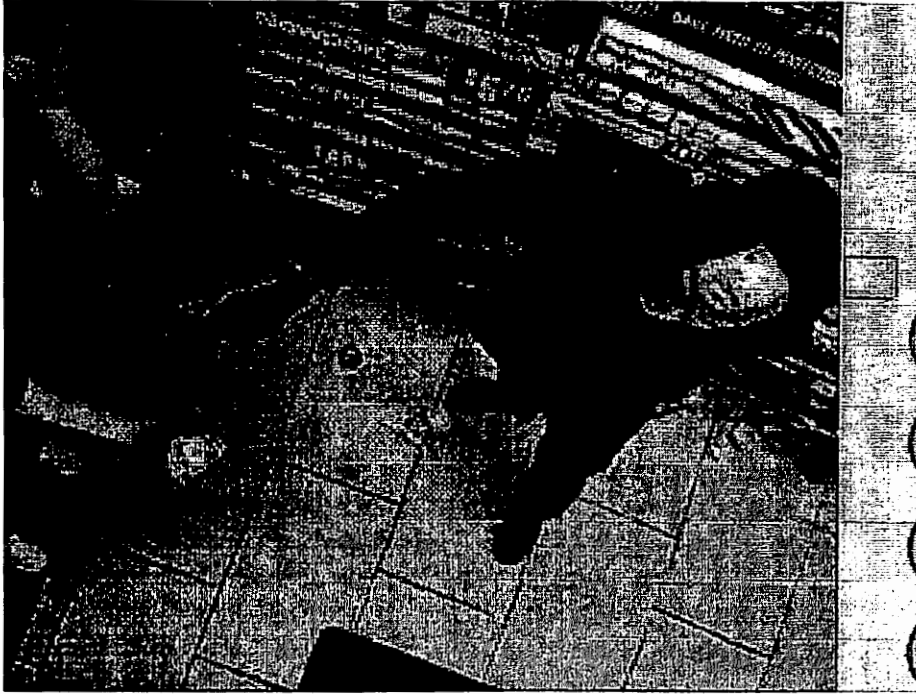
10. Lastly, I also make this Affidavit in support of an application for a search warrant authorizing a forensic examination of the physical Samsung Galaxy S10+ cellular telephone assigned call number (321) 230-6458 (the "Device"), further described in Attachment G. As set forth below, this Device was seized by the Fort Myers Police Department incident to ARMSTRONG's arrest on August 30, 2019. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment H.

Probable Cause Basis

Robbery of 7-11 on June 14, 2019

11. On June 14, 2019, the Lee County Sheriff's Office (LCSO) responded to a reported robbery at a 7-11 located at 17930 North Tamiami Trail, North Fort Myers, Lee County, Florida. Deputies arrived on scene and met with a victim named L.S. L.S. informed the responding deputy that her and a co-worker, A.N., observed a black male, later determined to be JOHN ARMSTRONG JR.

(“ARMSTRONG”), run into the 7-11 wearing all black clothing and a blue and white mask (pictured below).



12. ARMSTRONG was armed with a firearm and demanded that both L.S. and A.N. put their hands up. ARMSTRONG demanded money from A.N. who was behind the counter. A.N. froze and ARMSTRONG jumped over the counter. ARMSTRONG then struck A.N. in the head with the firearm he was carrying, causing a laceration to the bottom corner of A.N.’s left eye. L.S. opened both registers for ARMSTRONG and gave ARMSTRONG the money in the registers. ARMSTRONG took the money and exited the store. L.S. hit the panic button to alert the police and called 911.

13. As responding deputies were arriving, they observed a knife sitting on the ground outside the front door of the 7-11. The knife had a black handle and a

silver blade with a white sheath over the blade. The knife was photographed and collected for evidence along with video surveillance of the robbery. LCSO Detective Thomas Rall arrived on scene and spoke with the victims. While on scene, Detective Rall collected DNA swabs and requested that the knife be sent to the laboratory for forensic testing. Images and information about the robbery were sent to Crime Stoppers, a community program that allows people to provide anonymous information about criminal activity. A couple days after the robbery, an anonymous tip was received stating that ARMSTRONG was the person who robbed the 7-11. Based on the height and weight descriptions provided by the witness, Detective Rall believed ARMSTRONG could have conducted the robbery of the 7-11 on June 14, 2019.

14. On August 26, 2019, Detective Rall received a report from the Florida Department of Law Enforcement (FDLE) regarding the knife collected at the scene of the June 14, 2019 robbery. The knife had been processed for latent fingerprints and during the processing a latent fingerprint was discovered. By comparing ARMSTRONG's known fingerprints with the fingerprint recovered from the knife, FDLE determined that the latent fingerprint recovered off the knife belonged to ARMSTRONG. On August 28, 2019, Detective Rall reviewed the surveillance video of the robbery. While reviewing the surveillance footage, Detective Rall observed that the knife that was collected fell off of ARMSTRONG's person as he entered the 7-11 to rob it.

15. ARMSTRONG has prior felony convictions for carrying a concealed firearm (2007), and aggravated battery (2009), a case in which he similarly hit the victim in the face repeatedly with his firearm.

Robbery of Bank of Ozarks on July 31, 2019

16. On July 31, 2019, at approximately 8:43 a.m., the Punta Gorda Police Department responded to the Bank of Ozarks located at 3855 Tamiami Trail, Punta Gorda, Florida in reference to a bank robbery. At 8:36 a.m., a black male armed with a silver semi-automatic handgun forced entry into the bank after catching a teller who was arriving for work at the front door. The male ordered this teller, together with another teller who was already inside the bank, to the vault, telling the tellers to fill a bag and a backpack with cash. The male then ordered the tellers into the bank's bathroom and instructed the tellers to stay in the bathroom for two minutes. The tellers exited the bathroom and called the police. The male stole approximately \$151,000 as a result of that robbery.

17. Video surveillance taken from the bank depicts what appears to be a black 2006 Lincoln Zephyr (pictured below) parking at a location near the bank at approximately 7:47 a.m., *i.e.* less than an hour before the robbery. A male, whose height and build was consistent with ARMSTRONG's height and build, was then seen approaching the bank and hiding in the bushes near the front door. Immediately after the robbery, the black Lincoln can be seen leaving the area. It is believed that the black Lincoln, which as explained below is identical to a vehicle

belonging to ARMSTRONG's girlfriend, TANYA LEGG ("LEGG"), was the getaway vehicle.



Relationship between ARMSTRONG and LEGG

18. Between October 4, 2019 and October 7, 2019, ARMSTRONG and LEGG, a white, 43-year-old female, were both observed living at 150 Herron Road, North Fort Myers, Florida 33903 ("150 Herron Road"). In addition, according to the Florida Driver and Vehicle Identification Database (DAVID), ARMSTRONG and LEGG both have the same address listed on their driver's licenses of 14151 Warner Circle, North Fort Myers, Florida, which address is approximately one mile as the crow flies from 150 Herron Road.

19. A Florida Department of Corrections report provides further evidence that ARMSTRONG and LEGG are in a relationship: According to this report, on July 8, 2015, when ARMSTRONG was in State custody, LEGG called the Florida Department of Corrections Inspector General's District 10 office using a fake

name. LEGG alleged that she had information on crimes being committed inside the Dade Correctional Institution and wanted to report those crimes on behalf of a current inmate, John ARMSTRONG. A preliminary investigation revealed the true identity of the caller as being LEGG, who at that time was listed as ARMSTRONG's girlfriend on his jail visitation logs. LEGG later admitted her identity and indicated she was calling on behalf of ARMSTRONG.

20. In addition, as set forth below, law enforcement has obtained some of the text messages exchanged between LEGG and ARMSTRONG between September 28, 2019 and October 4, 2019. These text messages show that LEGG and ARMSTRONG had a sexual relationship.

Arrest of John ARMSTRONG on State Charge on August 30, 2019

21. On August 30, 2019, ARMSTRONG fled on foot after crashing a Chevy Blazer that was registered to LEGG's daughter into another vehicle and killing one of the occupants of the vehicle that he struck.¹ After crashing the Blazer, ARMSTRONG was arrested on the robbery charge. At the time of his State arrest on August 30, 2019, ARMSTRONG was in possession of a Samsung Galaxy S10+ cellular telephone assigned telephone number 321-230-6458 (SUBJECT PHONE 1/the Device). At the time it was recovered, this Device was registered to LEGG and was serviced by AT&T. The Device was seized incident to ARMSTRONG's arrest on August 30, 2019 by the Fort Myers Police Department,

¹ In a prior affidavit, I stated that ARMSTRONG crashed the Chevy Blazer while evading arrest. I have since learned that ARMSTRONG is not believed to have been evading arrest when he crashed the Chevy Blazer, but he did flee on foot after the crash.

which has since transferred custody of the phone to the FBI. ARMSTRONG bonded out of jail on the State charge on September 4, 2019.

Purchase of Backpacks and Black Long-Sleeved Dress Shirts in Tampa, Florida by ARMSTRONG, LEGG, and ZIRK on September 22, 2019

22. On September 22, 2019, a debit card belonging to ARMSTRONG was utilized at two Walmart stores in the Tampa Bay Area. The first transaction was conducted at a Walmart Supermarket located at 1505 North Dale Mabry Highway, Tampa, Florida. While at the Walmart Supermarket, ARMSTRONG, LEGG, and a male whom I later identified as DANIEL ZIRK ("ZIRK") were captured on surveillance purchasing two black button-down dress shirts. ARMSTRONG, LEGG, and ZIRK were also captured on video surveillance walking throughout the store together. A photograph taken by that video surveillance system is shown below; ARMSTRONG is the shorter male with a black shirt with large letters and ZIRK is the taller male wearing an orange hat.



23. Later on September 22, 2019, ARMSTRONG, LEGG, and ZIRK were captured on video surveillance together at another Walmart Supermarket located at 8220 North Dale Mabry Highway, Tampa, Florida. While at this store, LEGG was observed on video surveillance purchasing a black hat and two black backpacks. This video surveillance also captured images of ZIRK's shoes, which are white with a distinct darker pattern visible close to the soles of the shoes.



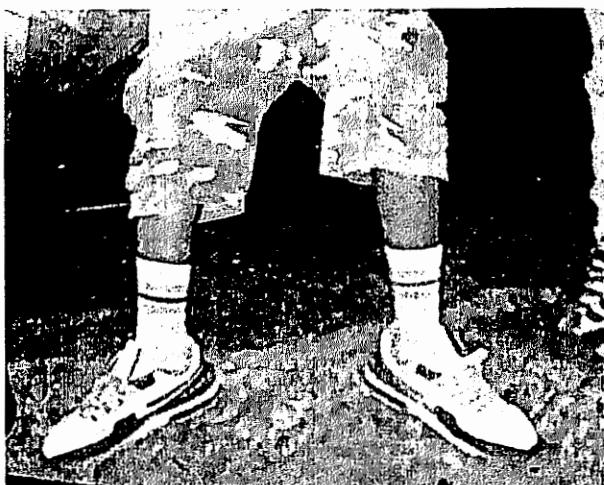


24. A check of surveillance footage of the Walmart parking lot at 8220 North Dale Mabry Highway showed all three subjects exit the store, walk through the parking lot, and enter a black 2006 Lincoln Zephyr bearing Florida tag IK13BB.



25. Further DAVID checks revealed that the black 2006 Lincoln Zephyr bearing Florida license plate IK13BB is registered to LEGG's daughter at 14151 Warner Circle, North Fort Myers, Florida—the same address which ARMSTRONG and LEGG listed as their address on their driver's licenses. As set forth below, moreover, LEGG later stated that the vehicle belongs to LEGG.

26. A photograph later obtained from LEGG's cellular telephone depicts ARMSTRONG, ZIRK, and a third male individual standing in front of the black Lincoln. In this photograph, which appears to have been taken on the same day as the Wal-Mart visits, ARMSTRONG and ZIRK are wearing the same clothing, headgear, and jewelry that they were wearing in the video surveillance taken at the Wal-Mart. Moreover, in the photograph, the distinctive darker pattern near the soles of ZIRK's shoes is clearly visible:



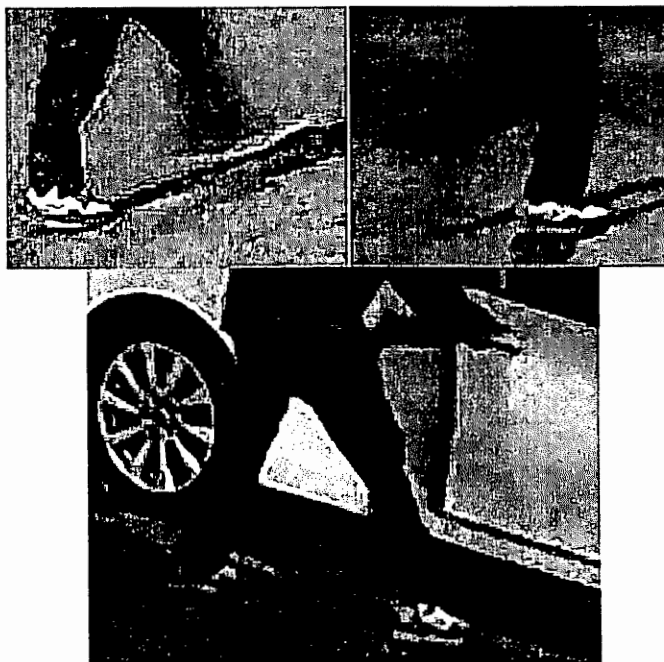
Carjacking on September 25, 2019

27. On September 25, 2019, the Orange County Sheriff Office (OCSO) responded to 6750 Forest City Rd., Orlando, Florida in response to a carjacking. At approximately 4:30 a.m., A.L. was sitting in a four-door white 2018 Toyota Camry, Florida license plate XXX5P, at the 7-11 located at 6750 Forest City Road, Orlando, Florida. While sitting in the vehicle, A.L. was approached by black male, later determined to be ZIRK, who was wearing a gray shirt to cover his face and black sunglasses.

28. The black male (ZIRK) approached A.L.'s vehicle and entered the vehicle from the front passenger's side door. ZIRK proceeded to take out a black handgun and pointed it at A.L. and demanded A.L.'s cellular telephone. ZIRK instructed A.L. to exit the vehicle while pointing the weapon at A.L. A.L. complied and exited the vehicle. ZIRK then jumped into the driver's seat of the vehicle and drove away.

29. Surveillance footage from the 7-11 shows that just prior to the carjacking, a black sedan with large, aftermarket rims drove by the 7-11 approximately three times. Moments after the black sedan passed the 7-11 the final time, the male later determined to be ZIRK can be seen on surveillance footage running from the roadway to A.L.'s vehicle. As ZIRK approaches the vehicle a light blue colored shirt can be seen sticking out from under a black, hooded top, as well as white shoes with a distinct darker-colored pattern near the sole of the shoe. The pattern on the shoes matches the pattern seen on ZIRK's shoes in the

Wal-Mart surveillance footage three days earlier, as well as in the photograph recovered from LEGG's phone. As the male later determined to be ZIRK left the scene in A.L.'s white Toyota Camry, he followed a black sedan with large aftermarket rims.²



² In a prior affidavit, I mistakenly stated that the black sedan followed the white Camry. In fact, the white Camry followed the black sedan.

30. A.L.'s vehicle was equipped with a GPS tracking device that monitored the location of the vehicle after it was stolen. Investigators gained access to this information which assisted investigators in locating footage of the vehicle captured by a red light camera at the intersection of Pine Hills Rd. and Clarcona Ocoee Rd. In the image, the stolen vehicle is located directly behind the black four-door sedan with large aftermarket rims.



31. Later on September 25, 2019, A.L. tracked her iPhone (which she had left inside of the vehicle), using the application "Find My iPhone," which showed that her phone was located in the parking lot of the PNC Bank, located at 8321 Champions Gate Blvd., Davenport, Florida.

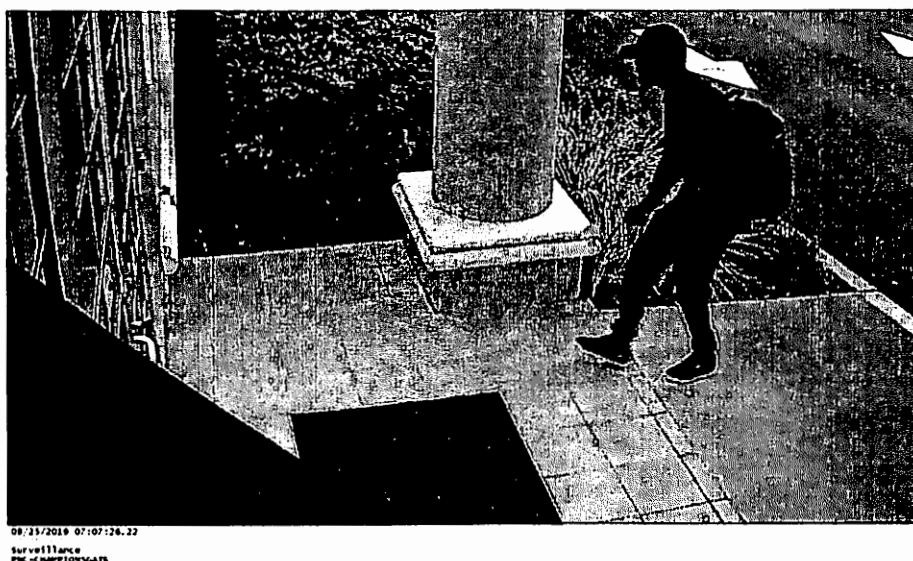
Attempted Bank Robbery of PNC Bank on September 25, 2019

32. On September 25, 2019, at approximately 8:32 a.m., the Osceola County Sheriff's Office received a call from a female who witnessed two armed males robbing the PNC Bank located at 8321 Champions Gate Blvd. in Davenport. Deputies arrived on scene about ten minutes later and spoke to the employees at the bank. The witnesses were interviewed and stated that two males, later determined to be ARMSTRONG and ZIRK, entered the bank and attempted to rob them.

33. Video surveillance and witness testimony showed that the males forced one of the bank employees into the bank at gunpoint. The shorter male (ARMSTRONG) was in possession of a silver handgun while the taller male (ZIRK) possessed a black handgun and wore a red bandana around his neck. Both males demanded that the vault be opened. The employee told both ARMSTRONG and ZIRK that she could not open the vault alone, and shortly thereafter the bank alarm went off. At this time ARMSTRONG and ZIRK panicked and ran out of the bank.

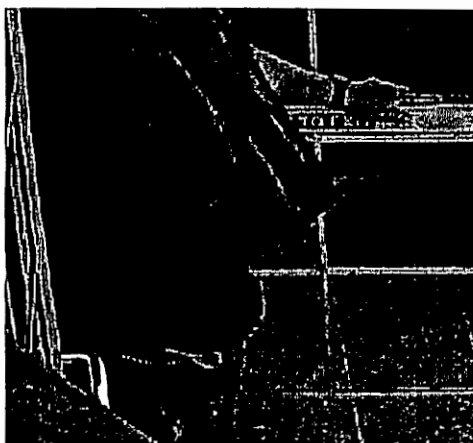


34. Video surveillance further showed that the two males arrived in a white Toyota Camry. When ARMSTRONG approached the bank, ARMSTRONG was unmasked and was not wearing gloves, and he was wearing a long-sleeved black dress shirt and was carrying a black backpack. ARMSTRONG crouched down and snuck into the bushes to wait for the employees to arrive.



35. When the taller male (ZIRK) entered the bank he was wearing a mask that covered his face but he could be seen wearing the same white shoes that he had been wearing earlier that morning at the time of the carjacking, and in the photo obtained from LEGG's phone, which have a unique design near their soles. ZIRK was also wearing a light blue shirt underneath a black jacket, which was what the suspect who committed the carjacking (ZIRK) had been wearing earlier that morning.

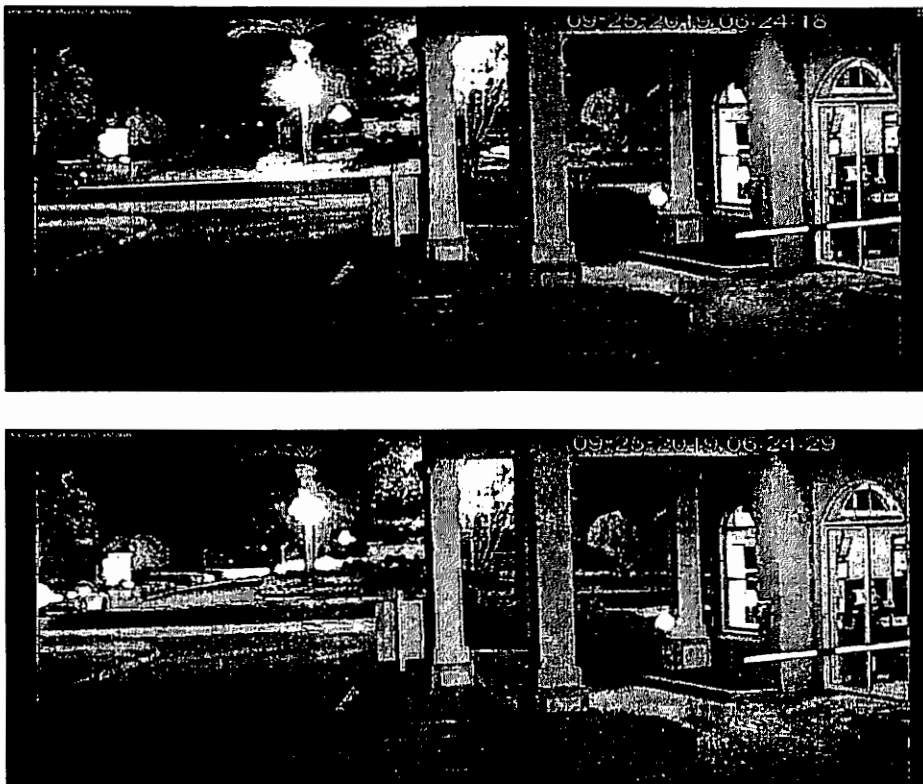




36. ZIRK was wearing multiple layers of clothing. In addition to his black jacket and blue undershirt, ZIRK, like ARMSTRONG, was observed wearing a black dress shirt and was carrying a black backpack while hiding in the bushes prior to the employees arriving at the bank. These black dress shirts and black backpacks appeared identical to those that ARMSTRONG, ZIRK, and LEGG had purchased at the Wal-Mart in Tampa three days earlier.



37. Surveillance video also showed that the white Toyota Camry arrived in the area of the bank at about 6:30 a.m. immediately behind a black four-door sedan with aftermarket rims.



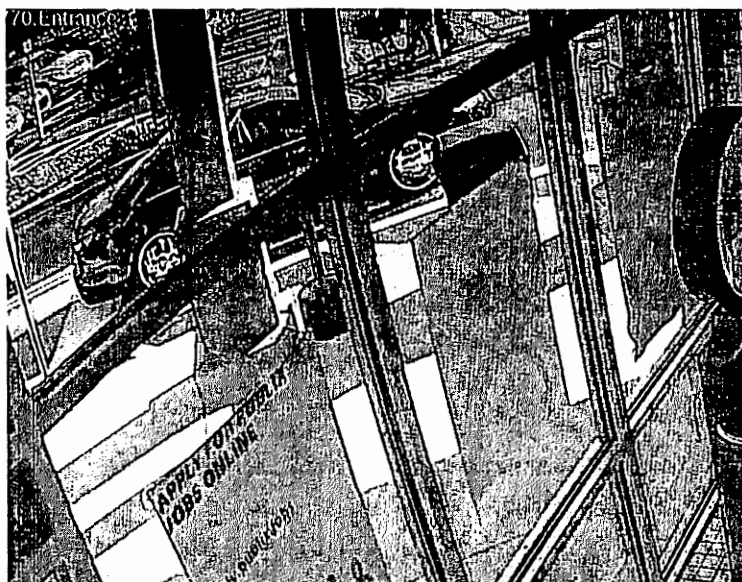
38. After the bank robbery, ARMSTRONG and ZIRK fled in the white Toyota Camry. The black four-door sedan was not visible on the surveillance at this time.



39. Surveillance footage from a nearby neighborhood on Masters Boulevard showed the Toyota fleeing. The video surveillance showed the vehicle making a U-turn prior to entering a parking lot. Officers from the Osceola County Sheriff's Office who went to this parking lot located the abandoned 2018 white Toyota Camry bearing Florida tag XXX5P, the same Toyota Camry that had been stolen from A.L. The location where the Toyota Camry was abandoned is approximately one mile away from the PNC bank.

40. During the investigation of the bank robbery, a witness who wished to remain anonymous approached investigators and stated that he had observed a black 2006 Zephyr with large aftermarket rims parked in the parking lot by the bank from approximately 4:00 to 6:00 p.m. the day prior to the robbery. The witness stated that nobody ever exited the vehicle while the vehicle was parked.

41. On September 24, 2019, at approximately 5:12 p.m., video surveillance footage from a nearby Publix supermarket depicted a black 2006 Lincoln Zephyr with aftermarket rims driving through the parking lot where the bank is located.



Robbery of BB&T Bank on September 26, 2019

42. On September 26, 2019, at approximately 7:51 a.m., two males, later determined to be ARMSTRONG and ZIRK, utilized handguns to rob the BB&T Bank located at 151 N State Road 434, Altamonte Springs, Florida. On the morning of the robbery, the two males hid in the bushes beside the bank entrance

prior to the bank opening. A BB&T bank employee subsequently arrived at the bank, cleared the bank per the bank's opening procedures, and signaled to another bank employee who was parked in the parking lot that the bank was clear. The employee exited her vehicle in the parking lot and walked to the front doors of the bank. As she approached the doors of the bank, the two male suspects exited the bushes and pointed their handguns at her. The males yelled at the employee inside of the bank not to warn the police or they would kill the female bank employee. The robbers demanded that the female employee unlock the bank doors and threatened to kill her if she did not comply. The female unlocked the doors and the male suspects followed the employee into the bank at gunpoint. They threatened to kill the employees if they did not comply.

43. The male suspects demanded that the bank employees move to the bank safe and open it using their keys. The suspects took the contents of one of the opened drawers from the safe, including approximately \$22,000 in cash, as well as personal possessions belonging to the bank employees, including car keys. The male suspects then entered the white vehicle of one of the bank employees using the keys they stole and fled.

44. Video surveillance taken from the bank and surrounding businesses captured the stolen white vehicle fleeing. This surveillance shows that as the white vehicle fled, a black, Lincoln four-door sedan with large aftermarket rims left the parking lot of an adjacent business. Both the stolen white vehicle and the black Lincoln can then be observed driving to a nearby closed business's parking lot. As

the black Lincoln passed in front of the Home Depot, Investigators were able to see into the vehicle and noticed the white arm of the driver and what appeared to be a red shirt with a large graphic on the front. As set forth below, this shirt appeared to be the same shirt that LEGG was seen wearing in security footage taken the previous day at a 7-11 and at a WaWa gas station.



45. Officers from the Altamonte Police Department located the stolen bank employee's vehicle just off Laurel Street at the back entrance to the closed business. A Seminole County Sheriff's Office blood hound subsequently conducted a track from the vehicle. The canine tracked approximately 10 feet.

46. The video surveillance taken by the BB&T Bank surveillance system captured the clothing of the males who committed the robbery. The blue shoes that ARMSTRONG was wearing as he jumped into the bushes during the attempted bank robbery of the PNC Bank were identical to the shoes worn by the male believed to be ARMSTRONG during the BB&T Bank robbery. The white shoes

with a unique design near their soles that ZIRK was wearing during the carjacking and during the attempted robbery of the PNC Bank appear to be the same shoes worn by the male believed to be ZIRK during the BB&T robbery, and appear to be identical to shoes that ZIRK was seen wearing in the photograph on LEGG's phone and in surveillance at a 7-11 on September 25, 2019 (see below). In addition, the Eastsport black backpacks carried by ARMSTRONG and ZIRK during the attempted PNC Bank robbery appear identical to the backpacks that the males believed to be ARMSTRONG and ZIRK were carrying during the BB&T bank robbery. Additionally, the silver handgun that ARMSTRONG was holding during the BB&T Bank robbery appears identical to the silver handgun used by ARMSTRONG in the previous bank robberies at the Bank of Ozarks and PNC Bank.





Interstate Nexus

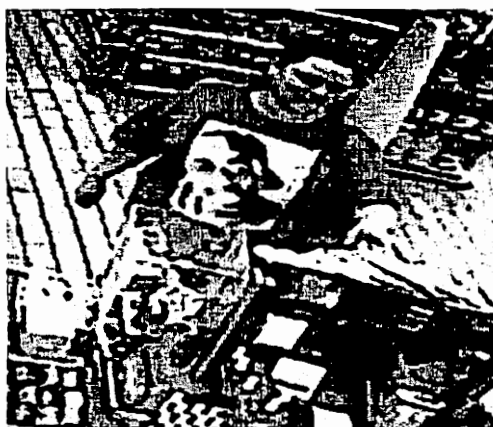
47. Each of the banks listed above was insured by the Federal Deposit Insurance Corporation at the times of the aforementioned incidents.

Additional Identification of ARMSTRONG, ZIRK, and LEGG

48. Further analysis of the data tracker from A.L.'s stolen Toyota Camry showed that approximately 45 minutes after the vehicle was stolen, the stolen vehicle parked near a residence located at 3725 Guinyard Way, Orlando, Florida at approximately 5:14 a.m. on September 25, 2019. The vehicle remained parked at this location for approximately 45 minutes. Investigators conducted a canvass of surrounding neighborhood businesses for surveillance footage. Investigators located video surveillance of a black four-door sedan with large aftermarket rims arriving at a 7-11 located at 3555 Vineland Road Orlando, Florida at

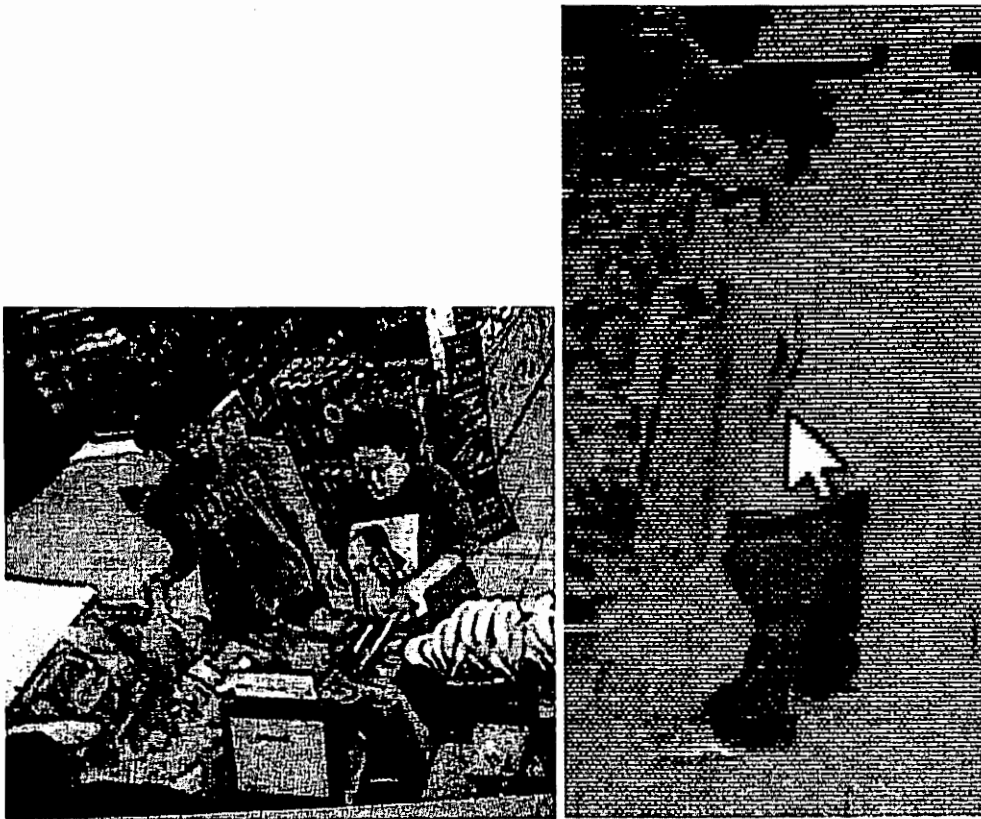
approximately 5:41 a.m. The 7-11 is located approximately one mile from the location on Guinyard Way where the stolen vehicle parked.

49. In the video surveillance, LEGG exited the black sedan and entered the store, where she purchased two bananas and \$4.50 worth of gas. She used a Suncoast Credit Union debit card that was later identified through bank records as belonging to ARMSTRONG, to complete the purchase. Within the bank records obtained, investigators discovered telephone number 239-672-3888. The subscriber of this telephone was determined to be LEGG.



50. Investigators also located video surveillance which shows that on September 25, 2019, at approximately 10:06 a.m. (*i.e.* approximately 1.5 hours after the attempted PNC Bank robbery), LEGG completed an EBT transaction at a 7-11 convenience store located at 5942 International Drive, Orlando, Florida in the amount of \$28.29. Surveillance footage from the store clearly shows LEGG and ZIRK. ZIRK's height, weight, and build are consistent with the height, weight, and build of the male who entered the PNC and BB&T banks with ARMSTRONG. ZIRK is wearing white shoes with a distinct design near their

soles that appears identical to the white shoes with the same design worn by the male during the carjacking and robberies earlier that morning. Additionally ZIRK is wearing a light blue shirt that is the same color as the shirt that can be seen protruding from underneath the black top of the male believed to be ZIRK during the carjacking and robbery of the PNC Bank.



51. Investigators also located video surveillance which shows that later on September 25, 2019, at approximately 6:54 p.m., a black Lincoln four-door sedan with large chrome rims pulled into the WaWa gas station located at 919 W. State Road 436, Altamonte Springs, FL. The WaWa gas station is located on the northwest corner of S.R. 436 and S.R. 434 in Altamonte Springs Florida directly

opposite the BB&T Bank mentioned above. Surveillance footage shows LEGG exit the front passenger seat and enter the store. Two males, the taller of which is wearing white shoes, can be seen exiting the vehicle and standing outside of it while LEGG enters the store.



**Cellular Analysis for LEGG and ARMSTRONG's Phones during the
Carjacking and Robbery of PNC Bank on September 25, 2019**

52. As explained, the carjacking of T.L.'s vehicle occurred on September 25, 2019, at approximately 4:30 a.m., and the robbery of the PNC Bank occurred that same morning at approximately 8:32 a.m. Cellular telephone analysis was conducted on the telephone number ending in 3888 belonging to LEGG. On September 25, 2019 at approximately 4:31 a.m., LEGG's telephone number connected to a tower in the vicinity of the carjacking that occurred at 6750 Forest City Road, Orlando. At approximately 5:09 a.m., LEGG's phone made an outgoing call to phone number 352-631-0614 (SUJECT PHONE 2), which as set forth below belongs to ZIRK, at which time LEGG's phone connected to a tower in the vicinity of 3725 Guinyard Way, Orlando, the location at which the stolen vehicle was parked. Between 7:05 a.m. and 8:25 a.m. LEGG's phone number connected for approximately 12 calls and texts to a tower in the vicinity of 8321 Champions Gate Blvd., namely the location of the bank. For instance, LEGG's phone number connected to the tower in the vicinity of 8321 Champions Gate Blvd. for an incoming phone call at approximately 8:25 a.m. from a phone number ending in 2515 (which as set forth below belongs to ARMSTRONG) that lasted for approximately six minutes. Following the 8:25 a.m. phone call, the next phone call

on LEGG's telephone occurred at 9:21 a.m., which connected to a tower approximately 15 miles northwest of the bank robbery location.

53. As explained below, evidence shows that ARMSTRONG was in possession of the phone assigned phone number ending in 2515. In addition, the telephone records of LEGG, including phone calls between her and the number ending in 2515 at the time that ARMSTRONG and ZIRK were hiding in the bushes outside of the PNC Bank and the BB&T Bank, provide further evidence that the number ending in 2515 is used by ARMSTRONG.

54. On September 25, 2019 at approximately 4:38 a.m., ARMSTRONG's telephone number ending in 2515 connected to a tower in the vicinity of the carjacking which occurred at 6750 Forest City Road, Orlando. Specifically, ARMSTRONG's phone number connected to the tower in the vicinity of 6750 Forest City Road, Orlando for an outgoing phone call at approximately 4:40 a.m. to ZIRK at phone number 352-631-0614 (SUBJECT PHONE 2), following which ARMSTRONG then received an incoming call from ZIRK. Notably, these calls were during the time period when the carjacker (ZIRK) was the sole occupant of the stolen Camry and was following the black Lincoln. At approximately 5:14 a.m. and then again at 6:02 a.m., ARMSTRONG's telephone number ending in 2515 connected to a tower in the vicinity of 3725 Guinyard Way, Orlando, the location in which the stolen vehicle was parked. At approximately 7:19 a.m., 7:29 a.m., and 8:25 a.m., ARMSTRONG's telephone number then connected to a tower in the vicinity of 8321 Champions Gate Blvd, namely the location of the bank. All

three calls were calls between ARMSTRONG's phone and the phone number ending in 3888 belonging to LEGG, and were during the time that ARMSTRONG and ZIRK were hiding in the bushes outside of the bank.

Cellular Analysis for LEGG and ARMSTRONG's Phones during the Robbery of BB&T Bank on September 26, 2019

55. As explained, the robbery of the BB&T Bank occurred on September 26, 2019 at approximately 7:51 a.m. Between 6:13 a.m. and 7:47 a.m. on September 26, 2019, the cellular phone number belonging to LEGG connected to a tower in the vicinity of the BB&T Bank located at 151 N. State Road 434, Altamonte Springs for approximately 20 calls and texts. Following a 7:47 a.m. text, the next call from LEGG's phone was at 8:44 a.m., at which time the phone connected to a tower located approximately nine miles south of the bank robbery location.

56. Similarly, between 7:01 a.m. and 7:46 a.m. on September 26, 2019, telephone number ending in 2515, belonging to ARMSTRONG connected to a tower in the vicinity of the BB&T Bank for approximately four calls. Following the 7:46 a.m. call, the next phone call was at 8:24 a.m., at which time the phone connected to a tower located approximately eight miles south of the bank robbery location.

Further Cellular Analysis and Location of Black Lincoln

57. On October 4, 2019 starting at approximately 1:57 a.m., telephone pings placed the cellular telephone ending in 3888 belonging to LEGG at the 150

Herron Road, North Fort Myers, Florida. This locational pinging had an accuracy level of within seven meters or less. Investigators began conducting surveillance on the residence and located the black 2006 Lincoln Zephyr bearing Florida license plate IK13BB parked at the residence. On October 4, 2019, investigators observed ARMSTRONG get into the black Lincoln after exiting the residence and drive to a Suncoast credit union located near the residence. After visiting the Suncoast, ARMSTRONG returned to the residence.





58. Further cellular site analysis shows that by September 26, 2019, at approximately 8:37 p.m., both LEGG's telephone assigned the call number ending in 3888, and ARMSTRONG's telephone assigned the call number ending in 2515, had returned from the Orlando area to North Fort Meyers, Florida. Since returning to the North Fort Myers area in the evening of September 26, 2019, the telephone assigned the number ending in 2515 remained within the Fort Myers area of Florida.

59. On October 6, 2019, at approximately 4:14 p.m., investigators observed ARMSTONG exit the front door of the residence at 150 Herron Road, enter the black 2006 Lincoln Zephyr bearing Florida tag IK13BB, and drive away from the residence. ARMSTONG then travelled south across the Caloosahatchee River and into Fort Myers. As ARMSTRONG travelled south, the telephone number ending in 2515 changed towers from north of 150 Herron Road to south of the Caloosahatchee River in the immediate area ARMSTRONG was now located. Continued surveillance showed that as Armstrong moved east through Fort Myers the telephone number ending in 2515 also moved to a tower further east. At approximately 5:44 p.m., ARMSTRONG returned to 150 Herron Road in the black Lincoln Zephyr, at which time the phone number ending in 2515 returned to the original tower north of Herron Road to which the phone number had been connecting prior to ARMSTRONG leaving 150 Herron Road. Thus, based on my training and experience, ARMSTRONG was in possession of the phone assigned the telephone number ending in 2515, traveled with this phone to another location, and then brought the phone back with him to 150 Herron Road.

Text Messages Exchanged between ARMSTRONG, LEGG, and ZIRK between September 28, 2019 and October 4, 2019

60. On October 4, 2019, Verizon wireless complied with a State-issued warrant for cellular records for telephone number 239-286-2515 (the phone number assigned to ARMSTRONG's phone). The records obtained from Verizon included

text message content for the period of September 28, 2019 to October 4, 2019 (but did not include text message content for any other time period).

61. On September 28, 2019, at approximately 4:59 a.m., LEGG sent an outgoing text from the phone number ending in 3888 to ARMSTRONG at the phone number ending in 2515 that said, "*After the side of you I seen this week I'm afraid to beat you up for calling me stupid mouth anymore.....lmao.*" ARMSTRONG replied, "*Wat side.*" LEGG then advised, "*The devil side.*" Based on my training, experience and knowledge of the investigation, I believe LEGG watched ARMSTRONG commit the two armed bank robberies and a carjacking over the course of two days on September 25th and 26th ("*After the side of you I seen this week*"). Because LEGG observed the violence that ARMSTRONG is capable of first-hand, she made the comment that she should be scared of what ARMSTRONG is capable of doing. ARMSTRONG asked LEGG to clarify ("*wat side*") and LEGG then advised that ARMSTRONG has an evil side to his personality ("*The devil side*").

62. In addition, according the Verizon records, on October 4, 2019, at approximately 5:21 a.m., LEGG sent an outgoing text to ARMSTRONG that stated, "*I meant what I said Ryde, die or kill for you. I promise you that.*" ARMSTRONG then responded at approximately 5:22 a.m. "*Tknow u gone ride*" [sic]. LEGG then sent ARMSTRONG a text at approximately 5:25 a.m. that stated "*Nobody is gonna ride. . . . we run or die together if it comes to that. . . .*"

63. The text message records for September 28, 2019 through October 4, 2019 obtained from Verizon further showed that on October 1, 2019, at

approximately 11:13 p.m., ARMSTRONG sent a text to SUBJECT PHONE 2, which as set forth below belongs to ZIRK, in which ARMSTRONG stated “*You good nigga?*” On October 2, 2019 at 2:21 a.m., ZIRK responded “*Yea I’m good.*” At 2:32 a.m., ARMSTRONG stated “*Ok.*” At 2:41 a.m. ZIRK texted “*Everything hood ?*” [sic], to which ARMSTRONG responded “*Yea.*” At 2:42 a.m. ZIRK responded “*Iight be safe phonk. I’m bouta go to sleep.*” At 2:43 a.m. ARMSTRONG responded “*Fosho. . . keep a low profile.*” (emphasis added; ellipsis in original).

Arrest of LEGG and ARMSTRONG on October 7, 2019

64. During the afternoon of October 7, 2019, the United States obtained a federal criminal complaint and arrest warrant for ARMSTRONG as well as federal search warrants to search the premises at 150 Herron Road and the black Lincoln Zephyr. In the evening of October 7, 2019, investigators conducting surveillance observed ARMSTRONG and LEGG loading up their belongings into two vehicles—the black Lincoln Zephyr and a 2004 gray Infiniti bearing Florida tag HNUT46. Due to the amount of belongings being loaded into the vehicles by ARMSTRONG and LEGG, they appeared to be leaving that location permanently or for an extended time period. ARMSTRONG and LEGG then left the premises at 150 Herron Road, at which time ARMSTRONG was driving the gray Infiniti and LEGG was driving the black Lincoln. ARMSTRONG and LEGG then drove to a gas station on Pondella Road in North Fort Myers, Florida, where they were arrested.

65. Upon LEGG's arrest, she immediately requested that someone call her daughter. LEGG told FBI TFO Brandan Bottom that her phone was sitting on the front passenger seat of her vehicle, the black Lincoln Zephyr. TFO Bottom retrieved LEGG's cellular phone from the vehicle and placed it in front of LEGG. LEGG then told TFO Bottom that the password to open her telephone was "1218," following which she showed him which contact in the phone was her daughter. This phone was later determined to be the cellular phone referenced above assigned the call number ending in 3888.

66. Special Agent (SA) Kevin Kaufman, FBI, advised LEGG of her "Miranda Rights," at which time LEGG requested a lawyer. SA Kaufman searched the black Lincoln Zephyr bearing Florida license plate number IK13BB that LEGG drove to the gas station. While searching the vehicle, SA Kaufman located, among other things, a silver firearm on the front passenger floor of the vehicle. The firearm was located in an unzipped black and pink bag. The firearm was photographed in place and then was removed from the bag. The firearm was loaded with approximately nine rounds of .22 caliber ammunition. The firearm appears to be the same silver firearm seen in surveillance video of the Bank of the Ozarks, PNC, and BB&T bank robberies that ARMSTONG used to commit those robberies.

67. During a search of the vehicle that ARMSTRONG was driving and of which ARMSTRONG was the sole occupant, the 2004 gray Infiniti, law enforcement found a relatively new black Eastsport backpack that appears to be

one of the same backpacks that LEGG purchased at the Walmart store on September 22, 2019, and that was then seen in surveillance video of the attempted PNC Bank robbery and the BB&T Bank robbery. Inside the backpack was a duel compartment lunchbox containing a scale, baggies, approximately 75.4 grams of suspected cocaine, approximately 65 grams of suspected marijuana, and approximately 77.4 grams of small blue pills believed to be MDMA.

68. Law enforcement also located the cellular telephone assigned the call number ending in 2515 on the front, driver-side floorboard of ARMSTRONG's vehicle and another cellular telephone on the front passenger seat of ARMSTRONG's vehicle. Both these phones are "prepay" phones, which in my training and experience are often the type of phones used by individuals involved in criminal activity, as such types of phones do not require verified subscriber information and thus cannot be traced back to those engaged in the crime. Further investigation into the toll records for the gray Infinity in which these two prepay phones were located has revealed that this vehicle traveled, with the black Lincoln, to Fort Myers, Florida from Orlando, Florida on September 26, 2019, approximately three hours after the robbery of the BB&T Bank.

69. Approximately 30 minutes after SA Kaufman first spoke with LEGG, LEGG requested to speak to SA Kaufman again. Prior to the interview, LEGG was asked to confirm that she had been advised of her "Miranda Rights," and she stated she understood her rights and wanted to speak to SA Kaufman again. During the interview, LEGG told SA Kaufman that the 2006 black Lincoln Zephyr

registered in the name of LEGG's daughter belongs to LEGG. LEGG stated that the contents of the vehicle also belonged to LEGG. LEGG was asked about the silver firearm located inside the vehicle. LEGG stated that the firearm belongs to her and that she purchased it off the street for approximately \$200. LEGG, who had apparently overheard law enforcement officers speaking about needing to execute a search warrant at 150 Herron Road, also stated that law enforcement did not need to search that house and that everything they needed was in her vehicle. Law enforcement officers executed a Federal search warrant at 150 Herron Road that same day but did not find any items of evidentiary value at that location. An interview conducted with the home owner, R.C. at 150 Herron Road, revealed that LEGG had been living at that location with her boyfriend ARMSTRONG. R.C. advised that LEGG would watch R.C.'s children while she was at work and had been doing so for the last month. When questioned further, R.C. advised that LEGG and ARMSTRONG did not stay at the residence from September 22, 2019, through the morning of September 26, 2019.

70. Following ARMSTRONG's arrest, TFO Brandan Bottom, FBI, advised ARMSTRONG of his "Miranda Rights," at which time ARMSTRONG advised that he understood his rights and agreed to speak with law enforcement. ARMSTRONG denied robbing any banks, stating that he is a drug dealer and sells drugs. When asked where the money taken from the banks was located, ARMSTRONG again denied having any knowledge of bank robberies, but told

TFO Bottom that he could get him the money he was looking for if he was released and allowed to work for law enforcement.

Analysis of Contents of LEGG's Cellular Telephone

71. Following the arrest of LEGG and ARMSTRONG on October 7, 2019, I sought and was granted a federal search warrant for LEGG's cellular telephone ending in 3888 and for the two cellular telephones³ recovered from ARMSTRONG's vehicle. Although LEGG appeared to have deleted some of her text history for the dates of September 24, 2019 through September 26, 2019, an analysis of the contents of LEGG's cellular telephone showed a detailed google search history for the dates of September 25, 26, and 27, 2019. On September 25, 2019, the following searches were conducted on LEGG's phone:

- what time is daybreak in Orlando, Florida
- take me to PNC
- take me to PNC ChampionsGate
- ozk near me
- banks close to me
- take me to Altamonte springs
- masked pair robs Osceola bank employees
- 2 armed men sought after bank robbery
- pnc bank robbed in championsgate fl
- ozk banks near casselburry fl
- take me to forest city road
- bb&t near me

On September 26, 2019, the following items were listed in the search history of LEGG's cellular telephone ending in 3888:

³ Law enforcement officers are still working on gaining access to the contents of ARMSTRONG's cellular telephones, which are password protected.

- Banks near me
- Ozk banks near casselburry fl
- Other banks near me

On September 27, 2019 the following items were listed in the search history of

LEGG's cellular telephone ending in 3888:

- PNC bank robbed on championsgate fl
- Masked men in stolen car robbed champio...
- 2 armed men sought after bank robbery ne...
- Championsgate bank robbery: osceo...
- Surveillance photos of BB&T Bank robbery
- Bb&t bank robbed in fottest city road
- Altamonte springs police, Osceola County...
- Police Seek BB&T bank robbery suspect

A further search of the contents of LEGG's telephone revealed the photograph included above in paragraph 26 showing ARMSTRONG, ZIRK, and another male individual in front of LEGG's black Lincoln. This photograph was documented in the phone as a screenshot that the phone user took from Instagram on September 28, 2019, so the photograph was taken no later than September 28, 2019, and as explained above was presumably taken on or about September 22, 2019, when ZIRK and ARMSTRONG were observed wearing the same outfits.

72. While reviewing the contents of LEGG's cellular telephone I checked for messages between LEGG and cellular number 352-631-0614 (SUBJECT PHONE 2), due to the fact that this was the phone number with which LEGG and ARMSTRONG communicated frequently during crucial periods of the offenses in question, such as when the stolen Camry was following the black Lincoln on September 25, 2019. I discovered that the cellular telephone number 352-631-0614

(SUBJECT PHONE 2) was saved in LEGG's phone under the contact name "Moneyredd." A check of text messages revealed the following communication between "Moneyredd" and LEGG on September 26, 2019 starting at 10:20 a.m. and ending at 10:27 a.m., *i.e.* approximately 2.5 hours after the completion of the final robbery:

Moneyredd: They said they can't do it

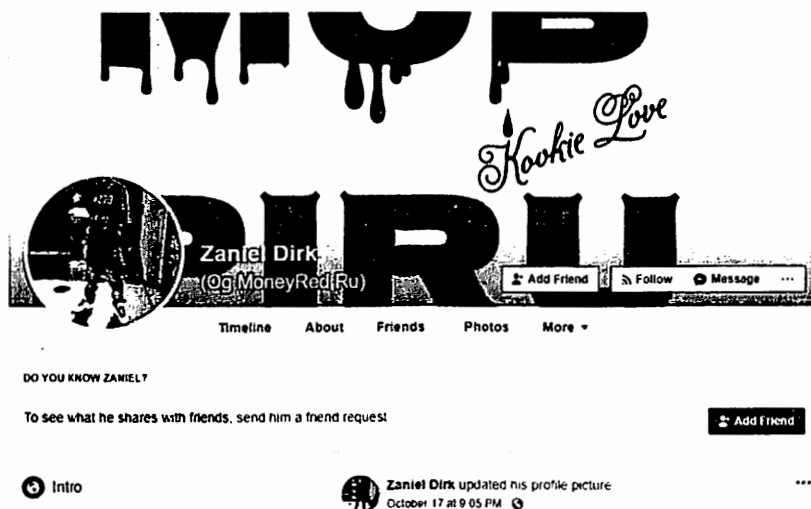
Moneyredd: It's a 2 hr drive

LEGG: Call the Orlando bus station and see if there's a bus going out today

Moneyredd: I ain't trynna slide n no bus but iight

Moneyredd: They ain't answer

73. Law enforcement officers searched Facebook and located the below Facebook profile for "Zaniel Dirk" with the subtitle "OG MoneyRed Ru." The current profile photograph of "Zaniel Dirk (Og MoneyRed Ru)" resembles ZIRK, and I was able to confirm that previous, public profile photos of Facebook user "Zaniel Dirk (Og MoneyRed Ru)" are photographs of ZIRK.

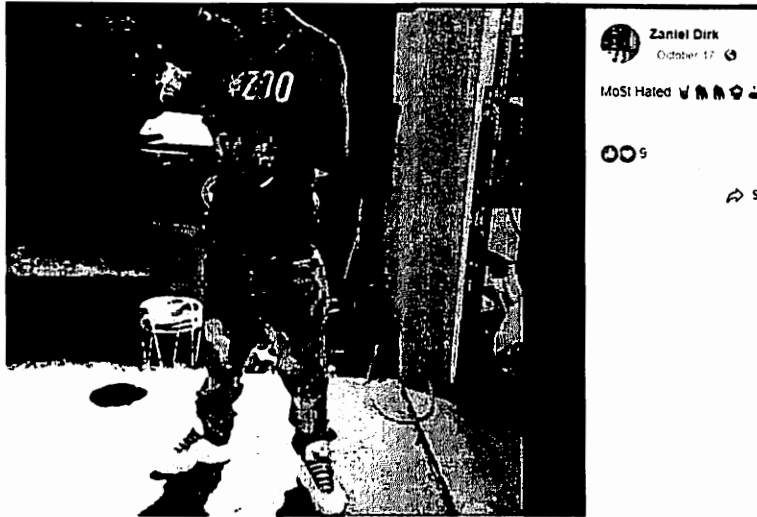


74. After reviewing a recent mugshot of DANIEL ZIRK taken in Hernando County on July 28, 2019, and comparing this with surveillance photographs and the photograph recovered from LEGG's phone, I was able to determine that ZIRK was the previously unknown subject seen in surveillance photographs with ARMSTRONG and LEGG prior to and shortly after the attempted bank robbery on September 25, 2019.

75. A second contact entry labeled "Moneyred" assigned to telephone number 816-463-1354 was also located in LEGG's telephone. This number ending in 1354 appeared to have been used by ZIRK prior to him obtaining the number ending in 0614, as between July 5, 2019 and September 8, 2019, there were several text message communications between LEGG and the number ending in 1354. On August 31, 2019, at approximately 4:34 p.m., "Moneyred" (from phone number 816-463-1354) sent an outgoing text to LEGG stating "I'm in hernando county right next door to Orlando," following which Moneyred sent LEGG a screen shot of the address 436 Hallcrest Ave., Spring Hill, FL 34608 (the PREMISES). A law enforcement database search for the number ending in 1354 showed that it belonged to ZIRK as of August 31, 2019. ZIRK then appears to have switched his number to the number ending in 0614 approximately one week prior to the PNC Bank robbery, as subscriber information shows that this phone number was activated on September 16, 2019, as further explained below.

76. On October 17, 2019, ZIRK updated his Facebook profile picture. In this profile picture, ZIRK can be seen standing in a driveway in front of a home.

The home in the photo is a unique red color and is consistent with the layout, color and texture of the PREMISES.



77. Investigators began surveillance on the PREMISES on October 22, 2019. On the evening of October 22, 2019, Investigators observed ZIRK exit the PREMISES via a back door. On October 24, 2019, at approximately 11:00 a.m., deputies with the Hernando County Sheriff's Office were conducting an unrelated investigation at the PREMISES. During their investigation the deputies spoke with all the residents of the PREMISES. At that time, ZIRK was identified as a resident of the PREMISES and his identity was confirmed on scene by deputies.

Cellular Analysis for ZIRK's Phone Ending in 0614 during the Carjacking and Robberies on September 25-26, 2019

78. On October 7, 2019, State investigators obtained via a State search warrant limited cell-site information, phone connection records, and subscriber information regarding the telephone number 352-631-0614 (SUBJECT PHONE 2), which has since been tied to ZIRK. (The United States is now seeking a more

comprehensive set of the cell site information SUBJECT PHONE 2). The records obtained by the State showed that SUBJECT PHONE 2 is a prepaid phone purchased on September 16, 2019 from Wal-Mart with cellular service through T-Mobile. SUBJECT PHONE 2 does not have any subscriber information.

79. Further analysis of the records obtained by State investigators for telephone number 352-631-0614 showed that on September 25, 2019, between the hours of midnight and 6:00 a.m., ZIRK was only in contact with the telephone number ending in 3888 belonging to LEGG and the telephone number ending in 2515 belonging to ARMSTRONG. The majority of these communications took place during the time period from just prior to the carjacking until the time that the stolen Camry and the black Lincoln arrived together in the area of the PNC Bank, or in other words during the time when the male who carjacked the Camry, ZIRK, was following the black Lincoln. Additional analysis showed that ZIRK's cellular telephone connected to a tower in the vicinity of 6750 Forest City Road (the location of the 4:30 a.m. carjacking) between 4:37 a.m. and 4:41 a.m. At 5:41 a.m. ZIRK's phone connected to a tower in the vicinity of 3725 Guinyard Way (the location where the stolen Camry was parked at that time). Between the hours of 6:02 a.m. and 11:09 a.m., ZIRK's phone did not have make or receive any calls until it connected to a tower near the 7-11 located at 5942 International Drive where ZIRK was seen on video surveillance with LEGG.

80. On September 26, 2019, ZIRK's cellular telephone number ending in 0614 was in contact with ARMSTRONG between 12:22 a.m. and 1:30 a.m., after

which ZIRK did not make or receive any calls or texts until 9:58 a.m.

(approximately two hours after the BB&T robbery), at which time ZIRK's phone connected to a tower in the area of 3725 Guinyard Way in Orlando, Florida.

81. On September 27, 2019, ZIRK's phone connected to a tower in the vicinity of the PREMISES approximately 40 times between 12:47 p.m. and 9:58 p.m.

82. On October 7, 2019 starting at approximately 3:08 p.m., telephone pings placed ZIRK's phone (SUBJECT PHONE 2) in the area of the PREMISES. This locational pinging had an accuracy level of 1400 meters or less. This locational pinging continued for approximately 21 hours, during which time the telephone stayed in the same area.

Cell-Site Data and Providers

83. Because users of cellular telephones generally tend to keep their phones with them, the requested historical cell-site information for SUBJECT PHONE 1 recovered from ARMSTRONG on August 30, 2019 is sought to assist in proving that ARMSTRONG was in the area of the 7-11 robbery on June 14, 2019, and the robbery of the bank of the Ozark on July 31, 2019. Additionally, cell-site information for ZIRK's number, SUBJECT PHONE 2, is sought to assist in proving that ZIRK was present with ARMSTRONG and LEGG during the carjacking and attempted bank robbery of PNC bank on September 25, 2019, as well as the robbery of the BB&T bank on September 26, 2019, and also to assist in

confirming that ZIRK was with ARMSTRONG and LEGG on September 22, 2019 and the days leading up to the carjacking.

84. I have learned that T-Mobile is a company, headquartered at 4 Sylvan Way, Parsippany, New Jersey, and AT&T is a company headquartered at 208 S. Akard St., Dallas, Texas, and that both of these companies provide cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as “tower/face information” or “cell tower/sector records.” Cell-site data identifies the “cell towers” (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data.

85. Based on my training and experience, I know that T-Mobile and AT&T can collect cell-site data about the phone numbers in question. I also know that wireless providers such as T-Mobile and AT&T typically collect and retain cell-site

data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

86. Based on my training and experience, I know that wireless providers such as T-Mobile and AT&T typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile and AT&T typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute fruits, evidence and instrumentalities of the crimes under investigation because the information can be used to identify the phones' user or users and may assist in the identification of co-conspirators.

Computers, Electronic Storage, and Forensic Analysis

87. As described in Attachment B, the application to search the PREMISES seeks permission to search for records that might be found in whatever form they are found. One form in which the records might be found is data stored on a cellular telephone or other electronic 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).

88. *Probable cause.* I submit that if a cellular telephone is found on the PREMISES, there is probable cause to believe those records will be stored on that cellular telephone, which functions like a computer with electronic storage capabilities, 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, 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 so 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 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.”

89. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cellular telephones 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 the PREMISES 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 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.

90. *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.

91. *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.

Technical Terms

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

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from

the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio,

using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is 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 computer must be assigned an IP address so that 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.
- f. Based on my training, experience, I know that the Device has the capabilities to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device. In my training and experience, examining data stored on devices of this

type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Electronic Storage and Forensic Analysis

93. Based on my knowledge, training and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

94. *Forensic evidence.* As further described in Attachment H, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device 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).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic 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.

95. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

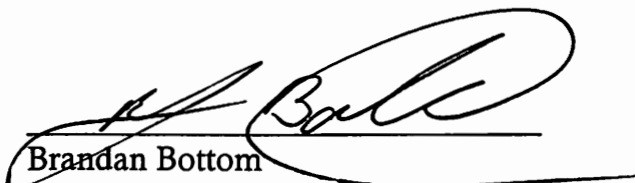
96. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I

submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

97. Based on the foregoing facts and evidence, I submit that probable cause exists to charge ZIRK with attempting to commit bank robbery, in violation of 18 U.S.C. § 2113(a), and using a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. § 924(c). I also submit that probable cause exists to search the premises at 436 Hallcrest Avenue, Spring Hill, Florida. I also believe that probable cause exists to search for records related to cellular use and connection information for SUBJECT PHONE 1 and SUBJECT PHONE 2, as well as to search ARMSTRONG's Device.

This concludes my affidavit.


Brandon Bottom
Task Force Officer, FBI

Sworn to and subscribed to this
29 day of October, 2019.


The Honorable Thomas B. Smith
United States Magistrate Judge

ATTACHMENT A

Property to be searched:

The property to be searched is 436 Hallcrest Avenue, Spring Hill, Florida 34608 (the "PREMISES"), which is a single-family style, one-story residence, with a red stucco exterior, located on the east side of Hallcrest Avenue, just north of Cameo St. The PREMISES has a concrete driveway leading from the roadway to the PREMISES' single-car garage.

ATTACHMENT B

Items to be seized from the PREMISES:

Evidence of violations of 18 U.S.C. §§ 2113(a) (bank robbery) or 2119 (carjacking) from September 25, 2019 through September 26, 2019, including, but not limited to:

1. Any and all items worn or used during the commission of the violations described above, including, but not limited to, masks, articles of clothing, bags, shoes, backpacks, jewelry, and firearms.
2. Any and all proceeds of the robberies, including cash as well as the personal property stolen from bank tellers, which includes purses, car keys, and phones.
3. Any and all documents or records related to the whereabouts of the proceeds of the violations described above, such as bank records and receipts.
4. Any and all documents or records related to the whereabouts of ZIRK, ARMSTRONG, or LEGG during the commission of the violations described above.
5. Cellular telephones used during or to effect the commission of the violations described above, and all information electronically stored therein related to the commission of the robberies, including stored email messages, text messages, photographs, and location information.

6. For any cellular telephone whose seizure is otherwise authorized by this warrant, and any 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 indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the COMPUTER user;
- c. evidence indicating the COMPUTER user's state of mind as it relates to the crimes 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 logs, 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; and**
- k. Contextual information necessary to understand the evidence described in this attachment.**

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage; 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).

ATTACHMENT C

Property to be Searched:

This warrant applies to records and information associated with the cellular telephone assigned call number (321) 230-6458 ("SUBJECT PHONE 1" or the "Account"), that are stored at premises controlled by AT&T ("the Provider"), headquartered at 208 S. Akard St., Dallas, TX 75202.

ATTACHMENT D

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment C is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time periods set forth below:

- a. For the time period from **June 1, 2019 through August 30, 2019**, the following information about the customers or subscribers of the

Account:

- i. Names (including subscriber names, user names, and screen names);
- ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
- iii. Local and long distance telephone connection records;
- iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
- v. Length of service (including start date) and types of service utilized;
- vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber

Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. For the time period from **June 13, 2019** through **August 1, 2019**, all records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

- i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
- ii. information regarding the cell towers through which the communications were sent and received, including:
 1. the identity and location of the cell tower;
 2. the sector or "face" of the cell tower receiving the signal;
 3. the "azimuth" or angle of the signal.
 4. All available NELOS records

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1951 or 2113(a) involving John Armstrong during the period of June 14, 2019 through July 31, 2019.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

ATTACHMENT E

Property to be Searched:

This warrant applies to records and information associated with the cellular telephone assigned call number (352) 631-0614 ("SUBJECT PHONE 2" or the "Account"), that are stored at premises controlled by T-Mobile ("the Provider"), headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

ATTACHMENT E

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment E is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time periods set forth below:

- a. For the time period from **September 16, 2019 through October 29, 2019**, the following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
 - v. Length of service (including start date) and types of service utilized;
 - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber

Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

- vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. For the time period from **September 21, 2019 through September 27, 2019**, all records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

- i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
- ii. information regarding the cell towers through which the communications were sent and received, including:
 - 1. the identity and location of the cell tower;
 - 2. the sector or "face" of the cell tower receiving the signal;
 - 3. the "azimuth" or angle of the signal;
 - 4. all available "timing advance" records.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. §§ 1951 or 2119 involving Daniel Zirk during the period of September 25, 2019 to September 26, 2019.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

ATTACHMENT G

Property to be searched:

The property to be searched is a Samsung Galaxy S10+ cellular telephone assigned call number (321) 230-6458 (the "Device"). On October 28, 2019, the Device was sent by the FBI, Fort Myers Resident Agency (RA) via overnight FED-EX delivery addressed to the FBI, Orlando RA, where it will be kept and searched. The Orlando RA of the FBI is located at 850 Trafalgar Square #400 Maitland, FL 32751.

ATTACHMENT H

The items to be seized are as follows:

1. All records and information on the Device described in Attachment G that relate to a violation of 18 U.S.C. §§ 1951 (Hobbs Act robbery), 2113(a) (bank robbery), or 924(c) (unlawful use of a firearm in the commission of a violent crime), and involve John ARMSTRONG, between June 13, 2019 and July 31, 2019, including:
 - a. Incoming and outgoing telephone numbers;
 - b. Stored contact/address information, voice messages, photographs and videos, text messages, emails, and other means of communications storing methods included as part of the phones features; and
 - c. Stored location and use information, or any data that would disclose the location or use of the device.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms “records” and “information” include evidence in whatever form and by whatever means it may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.