UNITED STATES DISTRICT COURT

DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA : ss: Hartford, Connecticut

COUNTY OF HARTFORD :

3:18MJ132 (DFM)

AFFIDAVIT

I, Molly Reale, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent employed by the United States Secret Service (U.S.S.S.), an agency within the Department of Homeland Security. I have been with the U.S.S.S. since January 30, 2017. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18 of the United States Code.

2. Since joining the U.S.S.S. I have been involved with investigations of, among other things, counterfeit currency, credit card fraud, bank fraud and wire fraud. I am currently assigned to the Connecticut Financial Crimes Task Force. The Task Force has the authority to investigate financial and cyber-related crimes having a nexus to the State of Connecticut. My current duties involve the investigation of cybercrimes and providing protection to leaders of the United States and foreign dignitaries. This is the first criminal affidavit for which I have served as an affiant.

3. I submit this affidavit to provide probable cause that **Alex Alberto Fajin-Diaz** and **Argenys Rodriguez** committed bank fraud in violation of 18 U.S.C. Sections 1344 and 2 by removing cash from a Citizen's Bank ATM located in Cromwell, Connecticut on January 27,

2018. I know that Citizen's Bank is a banking institution insured by the FDIC. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not set forth all of my knowledge about this matter.

Jackpotting: Thefts from ATMs Facilitated by Malware

4. In December of 2017 and January of 2018, I received multiple reports from law enforcement agencies in New York and Miami, FL as well as from ATM manufacturers, about malware attacks on ATM machines. These attacks targeted the cash dispensing functions of ATMs. This criminal activity is commonly referred to as "Jackpotting," since the malware is designed to cause the ATM to eject all of the U.S. currency contained in the machine without a legitimate ATM transaction.

5. In general, the scheme appears to involve two steps. First, individuals dressed as legitimate repair technicians approach the ATM and install the "jackpotting" malware. They are followed by two other individuals who then proceed to extract all of the cash from the ATM. Extracting the cash takes some time, since an ATM machine can contain tens of thousands of dollars.

6. On January 26, 2018, the U.S. Secret Service received information that individuals were planning in the next 10 days to activate cash-out teams to attack certain Diebold ATM machines using malware.

7. On January 26, 2018, I learned that Connecticut ATM locations were attacked with malware earlier in the week, specifically in Hamden, Connecticut and Guilford, Connecticut. Additionally, I learned there had been a malware attack on an ATM in Rhode Island.

Jackpotting Malware Attack in Providence, Rhode Island

8. I learned that on January 22, 2018, a Citizens Bank ATM located in Providence, RI was infected with ATM malware.

9. Video surveillance revealed that on January 22, 2018 two men appeared at the ATM dressed in what appeared to be Diebold technician uniforms and accessed the interior of the ATM machine. The subjects spent several minutes conducting activities inside the ATM consistent with protocols used to install malware in ATMs. The suspects then closed and secured the ATM before leaving.

10. Additional surveillance footage showed what appeared to be two other males approach the ATM and remain for a considerable amount of time, which I believe to be consistent with them obtaining cash that was being ejected from the ATM. Pictures of these suspects do not appear to match the physical description of **Fajin** and **Rodriguez**.

11. Video surveillance captured the suspects operating a 2-door white Honda Accord with possible MA registration plates beginning with the digits 411. As noted below, **Alex Alberto Fajin-Diaz** and **Argenys Rodriguez** were arrested by Connecticut authorities in a 2-door white Honda Accord, albeit with different license plates, during the January 27, 2018 ATM incident described below.

12. An initial investigation by Citizens Bank revealed that the ATM was found to be empty of currency. Citizen's Bank believes that more than $50,000 was taken.

Probable Cause to Arrest Alex Alberto Fajin-Diaz and **Argenys Rodriguez:**

Malware Attack in Cromwell, Connecticut

13. On January 27, 2018, Citizen Bank investigators monitoring their ATMs noticed an anomaly at a drive up ATM located in Cromwell, CT.

14. At that time, video surveillance revealed that two men were at the ATM and were accessing the interior of the ATM. They appeared to be dressed as ATM technicians. The video feed was then interrupted. Additional footage was later provided by Citizens Bank that showed a dark colored SUV and white 2-door Honda Accord at the ATM machine for an extended period of time.

15. Citizen Bank Investigators contacted the Cromwell Police Department and patrol units responded to the location. The dark SUV left the area prior to the arrival of law enforcement, but the white Honda Accord was on scene when police arrived.

16. Officer Brooks was first to arrive on scene and observed a white Honda Accord occupied by two Hispanic males, later learned to be **Alex Alberto Fajin-Diaz** and **Argenys Rodriguez**. The Honda Accord, driven by **Argenys Rodriguez,** was stopped by Officer Brooks approximately fifty feet north of the ATM kiosk. No other vehicles were observed in the immediate area at that time.

17. Officer DiMaio arrived on scene approximately thirty seconds after Officer Brooks arrived. Officer Brooks checked the Honda's license plate and attempted to obtain the driver's personal information. Officer DiMaio ordered the occupants of the car to place their hands on the dashboard. Officer DiMaio heard the drive-up ATM beeping. As Officer DiMaio approached the ATM, he heard it making sounds that an ATM makes when it is about to dispense money.

Officer DiMaio saw the ATM dispense a stack of twenty-dollar bills (later learned to be forty twenty-dollar bills). Officer DiMaio seized the twenty-dollar bills and secured them in his vehicle.

18. The Honda Accord had a CT registration plate (463UCX) affixed to the rear of the car. The police later learned that this Connecticut Registration plate was assigned to a red 2005 Lexus RX330 and was a misused plate. Officer DiMaio ordered Rodriguez to turn off the Honda Accord's engine and to hand him the key. Rodriguez complied.

19. Officer DiMaio asked Rodriguez what he was doing at the ATM. While they spoke, Officer DiMaio noticed a screwdriver within the area of the center lower dashboard that meets the center console. Rodriguez stated that he and Diaz pulled up to the ATM and noticed that there was a red light on at the side of the ATM. He said that he put his card into the ATM but nothing happened. He explained he tried it a couple of times but it did not work. Officer DiMaio asked Rodriguez about the screwdriver. He replied that it was "nothing," but did not offer any explanation when asked why he had it in the car. Officer DiMaio also noticed two Massachusetts license plates (2DC574) in the rear passenger compartment. Rodriguez was asked about the plates and he stated that they were old plates that he had to return.

20. Both occupants were then handcuffed behind their back and were seated the curb within the ATM lane. Rodriguez subsequently gave verbal consent to search his vehicle.

21. Law enforcement officers proceeded to search the vehicle. They found screwdrivers, pliers, and Allen wrenches strewn about the interior of the vehicle. Within a black nylon bag that was discovered in the front passenger compartment, officers found a large amount of twenty-dollar bills. A black electronic device that was approx. 3 1/2 inches by 3 1/2 inches square and

approx. 1 inch thick and resembled and Apple TV was also discovered. Along with that electronic device, officers also found cables and wires. Additionally, in the trunk of the vehicle, officers discovered a plastic bag with many cables and wires with various different connectors. Based on what I learned, these tools and electronic devices are consistent with the items needed to compromise an ATM machine to dispense its cash contents.

23. Both Diaz and Rodriguez were placed under arrest for state charges and searched. Diaz possessed a large fold of twenty-dollar bills in his jeans front right pocket. A count later revealed that there were sixty-five, twenty-dollar bills in his pocket. Rodriguez's brown Gucci wallet contained eighteen twenty-dollar bills.

24. The items found by officers during the search of the vehicle were left in the vehicle and the vehicle was towed to the Cromwell Police Department so a search warrant could be obtained.

25. Detective Mark Solomon from the Greenwich Police Department and a legitimate ATM technician responded to the scene and inspected the ATM machine. They concluded that the interior of the ATM machine had been accessed and that a cable, foreign to the interior of the ATM, was connected to the components of the ATM. Furthermore, the machine displayed a picture that was also foreign to the setup of the ATM. Additionally a deep insert ATM skimming device test sheet was found inside the ATM.

26. At the Cromwell Police Department, Rodriquez was advised of his rights both orally and in writing. Rodriguez denied being a part of the malware attack. He stated that the machine was ejecting money and that they put the cash within the vehicle. Rodriguez subsequently requested to contact an attorney. To the best of my knowledge, both defendants are still in state custody.

27. After obtaining a state search warrant for the car, officers discovered a wireless keyboard with a USB cord attached to it. Based on what I have learned in this case, I believe that once hooked to the ATM, this device would allow individuals to remotely contact a computer to facilitate the "jackpotting" scheme.

CONCLUSION

28. Based on the foregoing, there is probable cause to believe, and I do believe, that **Alex Alberto Fajin-Diaz** and **Argenys Rodriguez** participated in a scheme to obtain money under the control of, or owned by, Citizen's Bank by means of material false or fraudulent pretenses. Specifically, they participated in a scheme that provided electronic instructions directing a Citizen's Bank ATM to dispense United States currency in the absence of a legitimate ATM transaction, in violation of 18 U.S.C §§ 1344 and 2.

Molly Reale
Special Agent, USSS

Subscribed and sworn to before me this 31st day of January, 2018

/s/ DFM

[redacted]
THE HONORABLE DONNA F. MARTINEZ
UNITED STATES MAGISTRATE JUDGE