

DOA  
8-4-17

**UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

UNITED STATES OF AMERICA

v.

ROBERT JEREMY MILLER.

CRIMINAL COMPLAINT

CASE NUMBER: 17-8369AMJ

I, the undersigned complainant, being duly sworn, state that the following is true and correct to the best of my knowledge and belief:

Between on or about July 23, 2017, and August 4, 2017, in the County of Maricopa, in the District of Arizona, the defendant violated 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A) an offense described as follows:

Between on or about July 23, 2017, and August 4, 2017, in the District of Arizona, the defendant ROBERT JEREMY MILLER did knowingly and with intent to defraud access a protected computer of "Victim Company," a company headquartered in New Jersey, without authorization and exceeding any prior authorized access, and by means of such conduct furthered the intended fraud and obtained something of value, specifically, temporary login codes for, and location-tracking information available from, Victim Company's proprietary satellite-tracking system, in violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A).

I further state that I am a Special Agent from the Federal Bureau of Investigation (FBI) and that this complaint is based on the following facts:

**See Attached Statement of Probable Cause Incorporated By Reference Herein.**

Continued on the attached sheet and made a part hereof:  Yes  No

AUTHORIZED BY: James Knapp, AUSA

*(IMA FOR AUSA Jim Knapp)*

SA Steven Garbett, FBI

Name of Complainant

*(Signature)*

Signature of Complainant

Sworn to ~~before me and subscribed in my presence~~ *telephonically*

*8-5-17*

Date

at Phoenix, Arizona  
City and State

HONORABLE JOHN Z. BOYLE  
United States Magistrate Judge

Name & Title of Judicial Officer

*(Signature)*

Signature of Judicial Officer

**STATEMENT OF PROBABLE CAUSE**

I, Steven Garbett, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed for eight years. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer crimes, including criminal computer intrusions. I have gained experience through training at the FBI Academy, including training pertaining to cyber investigations. I have a bachelor's degree in Computer Information Systems and over ten years of experience working in Information Technology. I have received training in the area of computer intrusions and have had the opportunity to observe and review numerous cases and methods used by cyber criminals.

2. The facts in this Statement of Probable Cause come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause that Robert Jeremy MILLER (hereafter, "MILLER") committed a criminal offense in violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A), and does not set forth all of my knowledge about this matter.

3. On February 22, 2017, MILLER was terminated from his position at a large technology company headquartered in New Jersey, but with offices across the United States, including in Arizona (hereafter, the "Victim Company"). MILLER's job title at the time of his termination was Senior Project Management Specialist.

4. As a Senior Project Management Specialist, MILLER's duties primarily consisted of administering the Victim Company's proprietary satellite tracking system

(hereafter, the “STS”). The STS was designed to track the location and movements of aircraft and marine craft. Clients of the Victim Company, including commercial organizations as well as government and military agencies, would pay the Victim Company for access to an online system that would allow clients to log in and monitor the location and movements of the clients’ aircraft and/or marine craft. The Victim Company considered MILLER to be the Victim Company’s leading subject-matter expert on the STS. As an administrator of the STS, MILLER had the ability to access the STS remotely and create login IDs for the system; however, after February 22, 2017, the Victim Company removed MILLER’s access to the company computer network when his employment was terminated and deleted all known login IDs that MILLER had for the STS at that time.

5. On July 23, 2017, the Victim Company received a phone call from an individual calling himself “John Patriot.” “Patriot” was later identified as Brandon HARRIS (hereafter, “HARRIS”). HARRIS communicated with the Victim Company using telephone number (317) 220-3777. HARRIS stated that he had become aware of a man who planned to sell login IDs to access the Victim Company’s “satellites” on the black market. HARRIS explained that the man to whom he referred claimed to have a level one security and the ability to use temporary login IDs or create permanent IDs to access the Victim Company’s satellite system. Additionally, HARRIS claimed that the man was looking to sell the login IDs to allow a buyer access to the information and was hoping to obtain five million dollars. According to HARRIS, the man told HARRIS that

he had worked at the Victim Company and was “pissed that he didn’t get a raise and wanted to screw over the company.”

6. Investigators from the Victim Company followed up with a telephone call to HARRIS later that day. HARRIS initially did not give the real name of the individual who sought to sell the STS login IDs. However, after the investigator continued to ask for the individual’s real name, HARRIS stated that the individual’s name was “Robert Miller.” The investigator asked if the individual’s middle initial was “J,” and HARRIS confirmed. HARRIS stated that HARRIS “was not looking to get rich,” but wanted some compensation for bringing the matter to the Victim Company’s attention.

7. HARRIS provided the Victim Company with screen shots via text message of what HARRIS claimed to be the STS to show that he had unauthorized access to the computer network. Engineers from the Victim Company confirmed that the screen shots were from the Victim Company’s STS and depicted a visual of location data as to one of the Victim Company’s client’s aircraft and/or marine craft on July 26, 2017. Specifically, one of the screen shots displayed tracking information for one of the Victim Company’s client’s aircraft on July 26, 2017. HARRIS advised that he could facilitate a demonstration with MILLER of real-time access to the STS.

8. On July 26, 2017, the Victim Company received multiple telephone calls and text messages from HARRIS. During the phone and text message conversations, HARRIS advised that he would report that the Victim Company had a leak to the STS system to the media and the Victim Company’s customers if not compensated. When the

Victim Company asked what HARRIS was talking about in regards to payment, HARRIS responded that he believed the information would be worth “at least 5 figures.”

9. On July 27, 2017, HARRIS advised the Victim Company that he had become aware that his “contact” who had the STS access—that is, MILLER—had sold one of the login IDs. HARRIS stated that he did not know to whom or for how much the login ID was sold. HARRIS stated that he was aware of one more login ID that MILLER had for sale.

10. On July 31, 2017, FBI agents located and interviewed HARRIS. During the interview, HARRIS said that he had spoken with MILLER about the STS, that MILLER believed he could make money by selling access to the STS on the black market, and that HARRIS had told MILLER he could assist him in locating a potential buyer for the STS. HARRIS advised the FBI that he and MILLER had discussed trying to sell access to the STS to the Mexican cartel.

11. During the interview, HARRIS told the FBI agents that he had been communicating with MILLER via HARRIS’s cellular telephone, (317) 220-3777. At the time of his interview, HARRIS had in his possession the telephone utilizing phone number (317) 220-3777. HARRIS opened the telephone and showed the agents text messages he had exchanged with MILLER. HARRIS stated that MILLER only knew HARRIS by the name of “HR.” The text messages that HARRIS said he received from MILLER were from telephone number (801) 661-8953.

12. One of the text messages from MILLER to HARRIS, dated July 23, 2017, included the internet address of the Victim Company’s STS access page, and another text

message, dated July 23, 2017, included a temporary login ID and password for the STS. After discussing the STS with the Victim Company, your Affiant knows that a temporary login ID for the STS can only be created by accessing Victim Company's system.

13. Additionally, there were text messages between MILLER and HARRIS between July 23, 2017, and July 26, 2017, in which HARRIS and MILLER discussed how much a potential buyer would pay for access to the STS. During the text-message conversation, MILLER, using (801) 661-8953 asked HARRIS, "What price you think?" And, after HARRIS advised MILLER that he had "an offer for \$500k," MILLER wrote to HARRIS, "Think we should take an offer below 5mill and make em pay a hefty monthly?"

14. An additional text message sent from MILLER to HARRIS, dated July 26, 2017, included a screen shot of the STS. The screen shot was the same as the one previously provided to the Victim Company by HARRIS that displayed tracking information for an aircraft on July 26, 2017.

15. After speaking with FBI agents, HARRIS agreed to introduce an FBI agent to MILLER as a potential buyer of access to the STS. On July 31, 2017, HARRIS contacted MILLER. HARRIS stated that he had met with members of the Mexican cartel and had seen the money they were willing to pay for access to the STS. HARRIS told MILLER that he believed that the Mexican cartel would pay two million dollars for access to the STS. HARRIS informed MILLER that MILLER would be contacted directly by members of the Mexican cartel.

16. On August 1, 2017, an undercover FBI agent, posing as a member of the Mexican cartel, made a phone call to phone number (801) 661-8953. During the phone call, the agent stated that he had been in contact with "HR" and was interested in "buying." The agent told MILLER that he would like to see the STS and how it worked. MILLER and the undercover agent arranged a meeting for August 4, 2017.

17. On August 4, 2017, the same undercover agent made a phone call to phone number (801) 661-8953. The agent asked to meet in a public location and asked MILLER to be prepared to provide a live demonstration of his access to the STS.

18. On August 4, 2017, two undercover FBI agents, posing as members of the Mexican cartel, met with MILLER at a public location. At some point during the meeting, the agents and MILLER moved to a private room where MILLER used his own laptop to access the STS. During the meeting, MILLER stated that he had created a separate login ID and password to the STS while he was employed at the Victim Company. MILLER stated that he had created the separate login account to maintain access to the STS in the event that he was fired. In front of the agents, MILLER used the login account to log into the STS. While logged into the STS, MILLER accessed location data and demonstrated to the agents how to locate different aircraft and other vehicles.

19. At the end of the meeting, the FBI arrested MILLER. After being advised of his *Miranda* rights, MILLER consented to an interview. During the interview, MILLER admitted to accessing the STS. MILLER stated that he used a "tech support" login account that was shared by multiple technicians at the Victim Company. MILLER

stated that he knew he was not supposed to use the tech support account after his employment ended at the Victim Company. MILLER claimed that his intention in meeting with individuals whom he thought represented the Mexican cartel was to gather and share information with law enforcement. MILLER stated that he had researched how to become a DEA informant and was planning to talk to a DEA agent friend of MILLER's brother.

20. At the time of MILLER's arrest, FBI seized two cellular telephones from MILLER, one of which FBI has confirmed was associated with telephone number (801) 661-8953.

21. On August 4, 2017, after arresting MILLER, FBI agents executed a search warrant (17-7458MB) on MILLER's residence located at 620 N. 4th Avenue, Apartment 7, Phoenix, Arizona. During the course of the search, FBI seized multiple computers and hard drives. MILLER identified one hard drive as containing information from the Victim Company. However, MILLER claimed that he took the information from Victim Company inadvertently when he attempted to back up personal files from his work computer after his employment with Victim Company was terminated.

///

///

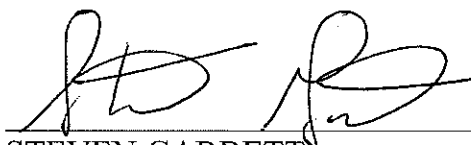
///

///

///



22. Based upon the aforementioned facts, your Affiant believes that probable cause exists that, between on or about July 23, 2017, and on or about August 4, 2017, MILLER committed the crime of computer fraud, namely the unauthorized access of a protected computer to defraud and obtain something of value, in violation of 18 U.S.C. §§ 1030(a)(4) and (c)(3)(A).



STEVEN GARBETT  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to <sup>telephonically</sup> before me on this 5 day of August, 2017.



HONORABLE JOHN Z. BOYLE  
United States Magistrate Judge