

**SEALED**

**UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

UNITED STATES OF AMERICA

v.

AUSTIN RYAN STEINBART.

CRIMINAL COMPLAINT

CASE NUMBER: 20-9119 MJ

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

On or about March 21, 2020, within the District of Arizona and elsewhere, the defendant RYAN AUSTIN STEINBART, with intent to extort money and other things of value from COMPANY B, transmitted in interstate and foreign commerce a communication containing a demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) 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: Raymond K. Woo, AUSA RW


SA Steven Garbett, FBI  
Name of Complainant

  
Signature of Complainant

Sworn and subscribed to me telephonically.  
3/26/2020 @ 2:40 pm  
Date

at Phoenix, Arizona  
City and State

HONORABLE EILEEN S. WILLETT  
United States Magistrate Judge  
Name & Title of Judicial Officer

  
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 11 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 10 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. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

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 for the requested warrant and does not set forth all of my knowledge about this matter.

3. On or about March 13, 2020, a YouTube user named Austin Steinbart ("STEINBART") posted a video to his YouTube profile. In the video, STEINBART stated he wanted to share a video clip he shot while visiting a medical clinic (COMPANY A) in Los Angeles, California. STEINBART stated he received medical services from

COMPANY A and that he hacked "famous peoples' medical records." In the clip, STEINBART could be seen sitting at a desk with a computer terminal that exhibited a date of January 20, 2020. STEINBART stated he found what appeared to be an entire archive of medical records. STEINBART then showed a directory on the computer terminal titled, "Patient Archive." STEINBART browsed the "Patient Archive" directory and clicked on patient names and record files for three separate patients. The first patient record showed the patient's name, age, health history notes, "Plan" prescribed by the doctor, and signed doctor's notes. The second patient record showed the patient's name, sex, date of birth, and details of the patient's brain scan procedure. The third patient record showed the patient's name, sex, date of birth, and details of the patient's brain scan procedure. While sitting at the terminal, STEINBART stated he was supposed to be taking a "boring test" on the computer but said, "I just couldn't help myself."

4. On March 18, 2020, COMPANY A representatives confirmed that STEINBART had posted patient information files onto YouTube that belonged to COMPANY A. COMPANY A stated STEINBART was a patient at COMPANY A and that he was supposed to be taking a computerized assessment on the computer terminal in the video. COMPANY A had been in contact with STEINBART since becoming aware of the leaked patient information. COMPANY A had asked STEINBART to take down the video and he refused.

5. On or about March 17, 2020, an attorney representing COMPANY A sent an email to STEINBART at email address [austinsteinbart@gmail.com](mailto:austinsteinbart@gmail.com). STEINBART's

parents were also included in the email. In the email, COMPANY A requested the YouTube video containing COMPANY A patient information be taken down immediately. STEINBART responded to the email with the following email message from [austinsteinbart@gmail.com](mailto:austinsteinbart@gmail.com):

My parents have NOTHING TO DO WITH THIS.

And you will DIRECT ALL FURTHER CORRESPONDENCE TO ME EXCLUSIVELY if you'd like things to remain CORDIAL between us.

Be advised: you have NO IDEA what patient data I possess, or what my next move is. All you know for certain is that I have thousands of highly engaged followers ready to propagate my leaks FAR AND WIDE across the global internet, at a moments notice. So it would be PRUDENT to heed this FIRST AND FINAL WARNING.

Respond immediately without my parents CC'd if you intend to comply.

6. On or about March 18, 2020, COMPANY A received a text message from STEINBART. The text message stated:

Unless you guys want NUCLEAR ARMAGEDDON to rain down on all of your heads, you will IMMEDIATELY APOLOGIZE to my parents, and your attorneys will DIRECT ALL FURTHER CORRESPONDENCE TO ME EXCLUSEIVELY.

7. A search of Arizona Motor Vehicle Division (MVD) records revealed an individual with the name of Austin Ryan STEINBART, driver's license number ending in 9191, date of birth of January 14, 1991, social security number ending in 1185, and an address of 1323 W Glenmere Dr, Chandler, AZ. The MVD photograph of STEINBART appeared to be the same individual in the YouTube video.

8. On March 19, 2020, FBI agents contacted STEINBART at his residence at 1323 West Glenmere Drive, Chandler, Arizona. When STEINBART answered the door, he held a Desert Eagle handgun in his right hand behind the door frame. After the agents identified themselves, STEINBART put the handgun away and advised the agents he was not threatening them with the weapon. STEINBART explained he "had a lot of psychos."

9. During the interview, STEINBART stated he took patient brain scans and medical records from COMPANY A and posted them on YouTube in a video. STEINBART stated, "I just sat down on one of their computers they were having me take a test at and just got right into their stuff." When asked about hacking into the computer, STEINBART stated, "It's actually not hard" and "almost anywhere I go like within 30 to 90 seconds I can get whatever I want."

10. STEINBART advised that he was doing "outrageous" things to demonstrate how stand-down orders work. STEINBART referred to himself as a spy and a Defense Intelligence Agency agent. STEINBART said he posted patient information on YouTube to, "Just show people that I won't get in trouble" and "the DIA will stand-down whoever I'm going to get in trouble with." STEINBART said he had told the doctor at COMPANY

A that they were "hacked by a very targeted intelligence operation." STEINBART stated he received his orders from messages that were sent from himself in the future. STEINBART said he received those messages through Neuralink brain implants that received signals from satellites.

11. STEINBART stated he had taken a video of himself accessing the patient records at COMPANY A. STEINBART also stated he recorded his YouTube videos inside his residence on Glenmere Drive. When asked by the FBI if he would take down the leaked information, STEINBART declined.

12. STEINBART also claimed he had illegally transported marijuana across the border from Mexico into the United States. On a YouTube video posted on March 21, 2020, STEINBART stated, "I have drugs, guns, and explosives in my house."

13. On March 21, 2020, STEINBART posted another video of himself on his YouTube profile. In the video, STEINBART stated COMPANY B removed a collection of digital files referred to as, "the amorphous archive" from his account. On a YouTube video posted February 8, 2020, STEINBART described his archive as containing "curated wikileaks." COMPANY B advised that some of the files in the archive were labeled, "CIA Documents." STEINBART called the removal of the archive by COMPANY B a "direct act of war against the American people" and stated it would not be tolerated. In the video, STEINBART stated:

"So, starting tonight we will be launching an economic blockade against COMPANY B until they decide to give us our amorphous archive back. How we

are going to do that is very simple, we are going to degrade and destroy their ability to support their customers by blowing up their tech support email. Every time we send an email to support@[COMPANY B].com, a ticket is automatically created in their system. So, by flooding that email with thousands of messages demanding our archive back, we can create tons of fake tickets and dramatically inhibit their ability to support their customers. **If they do not give us our archive back by Monday, we will start flooding their phone lines and their billing email system as well - choking off more and more their ability to operate their business every day until they either give us our files back or go out of business, their choice.**" (Emphasis added.)

14. Within the description of the YouTube video page, STEINBART posted the following text:

"Please COPY and SEND the message below to Support@[COMPANY B].com [and if that goes down, send to COMPANY B's other support email - support@[COMPANY B SUB COMPANY].com]

COMPANY B BE ADVISED:

YOU ARE IMPEDING A LIVE MILITARY INTELLIGENCE OPERATION BEING CONDUCTED BY THE DEFENSE INTELLIGENCE AGENCY.

REINSTATE AUSTIN STEINBART'S ACCESS TO THE AMORPHOUS ARCHIVE IMMEDIATELY, OR YOU WILL BE BRIGADED AND BLOCKADED UNTIL FURTHER NOTICE."

15. Representatives from COMPANY B explained they suspended STEINBART's account due to violations of their Terms of Service; which was related to a copyright claim submitted by a third party. COMPANY B stated STEINBART had not replied to messages from COMPANY B regarding the copyright claim.



16. After STEINBART posted the video on YouTube regarding the “blockade,” COMPANY B began receiving thousands of fictitious support emails over the next two days. Each fictitious support email caused COMPANY B’s computer system to create an electronic file that triggered a service response. That file, called a “ticket,” was routed through COMPANY B’s data computer system. Because of the influx of commands generated by the fictitious emails, COMPANY B’s system became overwhelmed. In response, COMPANY B deployed automatic filtering to help reduce the number of separate tickets and email communications reaching COMPANY B employees, but there were still hundreds of tickets that were auto-generated. COMPANY B also mobilized additional employees to help process the “false” emails and tickets.

17. On or about March 23, 2020, STEINBART posted a video to his YouTube profile. In the video, STEINBART made the following statements:

“We just began our first Q-Army economic blockade against a major corporation called COMPANY B...They have already crafted a successful defense against our flooding attack this weekend. How they did that was by programming a filter onto their mail servers that weeds out messages containing unique keywords from the pre-written message I had you send them...We are just going to make a slight adjustment and go right back at them...[Don't] use those blacklisted key words so that they can make it past those flood filters. So the next step in our economic blockade against COMPANY B is gonna be two fold. The first step is to make your own madlib out this template I made for you and send it in an email to these five email addresses: billing@[COMPANY B].com, sales@[COMPANY B].com, partners@[COMPANY B].com, legal@[COMPANY B].com, and support@[COMPANY B].com...The second step is to call support line I'm gonna list in the description below and dial 9 which will take you to their emergency after hours support. I would be super grateful for as much time as you could spare to volunteer to help me encumber their emergency tech support line. Ideally you could call and wait 'til someone picks up and tell them to give us our archive back when they do. But you if can't, any amount of time you could volunteer to help block up that phone line would really help. Blocking up that phone line will dramatically



inhibit their ability to support their highest paying customers and will dramatically raise the cost of their unconstitutional censorship. I'll write up the instructions for the second economic blockade and put them in the description below so you guys can have that for after the video.”

18. Within the description of the YouTube video page, STEINBART posted the following text:

COMPANY B TECH SUPPORT PHONE NUMBER: +1-833-832-4780 (then dial option 9 for emergency support)

NEW EMAIL TEMPLATE FOR COMPANY B BLOCKADE

-----  
Subject: NEED HELP WITH \_\_\_\_\_

I am writing from \_\_\_\_\_ Corporation. Having some MAJOR issues with the \_\_\_\_\_ that's connected into the \_\_\_\_\_.

THIS IS AN ABSOLUTE EMERGENCY SO PLEASE HELP ME FIX IT SOON AS POSSIBLE!!!

-----  
Send your CUSTOM MESSAGE in an EMAIL to:

support@[COMPANY B].com  
sales@[COMPANY B].com  
billing@[COMPANY B].com  
partners@[COMPANY B].com  
legal@[COMPANY B].com  
contact@[COMPANY B].com

19. In anticipation of the threat of a large quantity of incoming phone calls, COMPANY B increased the number of telephone channels with their telecom provider. The cost of adding telephone channels was estimated to be approximately \$10,800 per month. Despite these measures, COMPANY B still received complaints from customers that calls to COMPANY B would ring over three minutes with no answer, two days after STEINBART posted his video. COMPANY B reportedly received over 200 fraudulent phone calls after STEINBART's video post on March 21, 2020. COMPANY B employees reported some of the fraudulent calls lasted 10 to 15 minutes as the caller pretended to be a legitimate customer before eventually demanding that the amorphous archive be restored.


20. On or about March 14, 2020, STEINBART posted a video to his YouTube profile in which he described purchasing a Tokarev TT-33 handgun. In the video, STEINBART could be seen handling the weapon as well as a container of Tannerite, a binary explosive often used as a rifle target.

21. Based upon the aforementioned facts, your Affiant believes that probable cause exists that on or about March 21, 2020 and March 23, 2020 STEINBART, with intent to extort money and other things of value from COMPANY B, transmitted in interstate and foreign commerce a communication containing a demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of 18 U.S.C. §§ 1030(a)(7)(C) and (c)(3)(A).

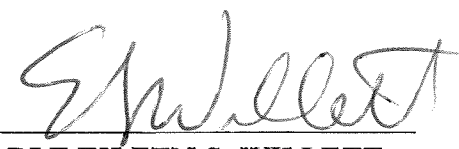
22. This affidavit was sworn telephonically before a United States Magistrate Judge legally authorized to administer an oath for this purpose. I have thoroughly reviewed the affidavit and any attachments, and I attest that there is sufficient evidence to establish probable cause that the defendant committed the offense listed above.

Respectfully submitted,

3/26/2020  
Executed on (Date)

  
\_\_\_\_\_  
STEVEN GARBETT  
Special Agent  
Federal Bureau of Investigation

X Sworn by Telephone

Date/Time: 3/26/2020 @ 2<sup>40</sup> pm   
\_\_\_\_\_  
HONORABLE EILEEN S. WILLETT  
United States Magistrate Judge