

20 MAG 1266

Approved: \_\_\_\_\_

DINA MCLEOD

Assistant United States Attorney

Before: THE HONORABLE SARAH NETBURN  
United States Magistrate Judge  
Southern District of New York

----- X

UNITED STATES OF AMERICA

- v. -

TRISTAN ROWE,

a/k/a "Angus,"

Defendant.

----- X

**SEALED COMPLAINT**

Violations of  
18 U.S.C §§ 1030(a)(2),  
1030(c)(2)(B)(ii),  
2261A(2)(B), and 2.

COUNTY OF OFFENSE:  
THE BRONX

SOUTHERN DISTRICT OF NEW YORK, ss.:

ANTHONY SANTILLI, being duly sworn, deposes and says that he is a Detective with the New York City Police Department ("NYPD"), and charges as follows:

**COUNT ONE**  
**(Cyberstalking)**

1. From at least in or about 2015, up to and including 2019, in the Southern District of New York and elsewhere, TRISTAN ROWE, a/k/a "Angus," the defendant, with intent to injure, harass, and intimidate another person, used the mail, interactive computer services and electronic communication services and electronic communication systems of interstate commerce, and other facilities of interstate and foreign commerce, to engage in a course of conduct that caused, attempted to cause, and would be reasonably expected to cause substantial emotional distress to a person, to wit, ROWE engaged in a years-long pattern of harassing and threatening conduct against an individual ( "Victim-2") in the Bronx, New York, including sending harassing and threatening phone and text communications to Victim-2, compromising Victim-2's online accounts, harassing Victim-2's friends and family members, and

generating multiple false 911 calls to Victim-2's residence in the Bronx, New York.

(Title 18, United States Code, Sections 2261A(2)(B) and 2.)

**COUNT TWO**

**(Computer Fraud - Unauthorized Access)**

2. From at least in or about 2016, up to and including at least in or about 2019, in the Southern District of New York and elsewhere, TRISTAN ROWE, a/k/a "Angus," the defendant, willfully and intentionally accessed a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, and did so in furtherance of a criminal and tortious act in violation of the Constitution or laws of the United States and of any State, to wit, ROWE obtained unauthorized access to an online platform used by the high school attended by Victim-2 ("High School-1"), the online grading system of High School-1, and the online accounts of the individuals referred to herein as Victim-1, Victim-6, and Victim-7 in furtherance of the cyberstalking offense charged in Count One.

(Title 18, United States Code, Sections 1030(a)(2),  
1030(c)(2)(B)(ii) and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

3. I am a Detective with the NYPD and I have been personally involved in the investigation of this matter. I am assigned to the NYPD's Computer Crimes Squad. This affidavit is based upon my personal participation in the investigation of this matter, my conversations with law enforcement agents, witnesses, and others, as well as my examination of report and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

4. Since at least 2018, the NYPD has been investigating an online stalking and harassment campaign that targeted Victim-2, and involved the possession, sharing and exploitation of



personal identifying information of, and illegally accessing online accounts belonging to a father ("Victim-1") and daughter (Victim-2), as well as the ex-boyfriend of Victim-2 ("Victim-3") and Victim-3's sister ("Victim-4"). In addition, the NYPD has been investigating a number of computer intrusions which are associated with the stalking and harassment of Victim-2.

5. Based on an interview with Victim-1 and Victim-2, I have learned the following, in substance and in part:

a. Victim-1 and Victim-2 reside in the Bronx, New York.

b. An individual going by the name "Angus" (later identified as TRISTAN ROWE, a/k/a "Angus," the defendant) has been harassing and threatening Victim-1 and Victim-2 since in or about 2015.

c. Victim-2 reported that, beginning in or about 2015 and continuing into in or about 2019, she would receive repeated, persistent phone calls and text messages from "Angus"—some obsessive, some lewd, some threatening. Those communications were sent from what appeared to be many different phone numbers. Victim-2 also reported that her online accounts—including her personal email account and her Facebook account—were compromised by a person she believes to be "Angus." "Angus" would then send messages from those compromised accounts to friends of Victim-2—often with demands that those friends put him in touch with Victim-2.

6. In a voluntary interview with law enforcement, conducted at his residence, in the presence of his father, TRISTAN ROWE, a/k/a "Angus," the defendant, admitted, in sum and substance, that between in or about 2015 and in or about 2019, ROWE compromised and accessed multiple online accounts belonging to Victim-1 and Victim-2, including Victim-2's college email account, posted Victim-1 and -2's personal identifying information online, called multiple fake 911 calls to the home of Victim-1 and Victim-2 alleging that violent crimes were taking place at the residence, called false bomb threats to Victim-2's high school, and contacted Victim-1 and Victim-2 on an almost daily basis via phone and online communications.

7. Based on my review of the messages sent to Victim-2 and interviews with Victim-2 and with TRISTAN ROWE, a/k/a "Angus," the defendant, I have learned the following in substance and in part:

a. Certain of the messages sent by ROWE to Victim-2 contain threatening language and imagery. On or about January 9, 2019, Victim-2 received an iMessage which contained a photograph of a large kitchen knife. ROWE admitted to sending that photo to Victim-2.

b. As another example, on or about January 20, 2019, Victim-2 received a text message from ROWE which read, "Harmless when I get u im putting u in the back of the trunk bitch ass nigga ill cut u from fucking ear to ear and ill pull ur tongue through the slit Columbian style bitch" from phone number 954-459-3569 (the "3569 Phone Number"). ROWE admitted to sending that message to Victim-2.

c. On or about September 6, 2018, Victim-2 received a text message from an unattributed number which read, "[Victim-2] should I sign you up on an escorts website."

d. On or about September 7, 2018, Victim-2 received a text message from an unattributed number reading, "Angus(noun): [Victim-2]'s cyberstalker."

e. On or about February 26, 2018, Victim-2 received text messages from an unattributed number reading, "i'm bombing the school" and "im buying an ar15"—an apparent reference to the AR-15 semi-automatic rifle.

f. Victim-2 also reported receiving messages from "Angus", which are no longer present on Victim-2's phone, that stated, in sum and substance, "You don't deserve to live," as well as a message, which I have reviewed, which contained a map with a detailed route mapped out from Tennessee to Victim-2's home address in the Bronx, New York.

8. Based on interviews with Victim-1 and Victim-2, I have learned that Victim-1 and Victim-2 were subjected to multiple "swatting" incidents at their residence in the Bronx, New York. Based on my training and experience, and my participation in this investigation, I know that "swatting" refers to a harassment tactic of deceiving an emergency service into sending a police or emergency service response team to another person's address. This is typically triggered by false reporting of a serious law enforcement emergency, such as a bomb threat, murder, hostage situation, or a false report of a "mental health" emergency, such as a report that a person is allegedly suicidal or homicidal and may or may not be armed. Further, according to Victim-2:



a. On multiple occasions, police officers responded to her home in the Bronx, New York—often with guns drawn.

b. She was once awoken by police officers outside her bedroom door, and found the "swatting" incidents to be extremely frightening and upsetting.

9. Based on my review of text messages sent to Victim-1 from unattributed phone numbers, I have learned the following in substance and in part:

a. On or about January 1, 2018, Victim-1 and Victim-2 received text messages in a series, which read as follows, in sum and substance, "if you do not speak up you will be shot and killed by a swat team," "I do not play games with swatting," "next swatting victim will be courtesy of me," "or I will send armed swat cops," and "they killed a man in Witchita [sic] Kansas over some swatting."

b. On or about August 23, 2017, Victim-1 received text messages in a series, which read as follows, in sum and substance, "u wanna get swatted," "even better I'll swat the nypd," and "your choice u can wind up dead cause the armoured cops will come raid u," "or u can comply," and "this is ur final warning."

10. Based on an interview with the principal of a high school in the Bronx ("High School-1") attended by Victim-2, I have learned the following, in substance and in part that between at least in or about 2017 to at least in or about 2018, High School-1 received multiple threats, including a bomb threat and an active shooter threat, from an individual who identified himself as "Angus," and demanded to be put in contact with Victim-2.

11. Based on an interview with the technology director ("IT Director-1") of High School-1, I have learned the following in substance and in part:

a. On or about August 29, 2017, IT Director-1 reported to the NYPD that an unknown individual had compromised High School-1's grading system ("High School-1 Grading System") and portfolio system. IT Director-1 further reported that the perpetrator had been able to obtain personal identifying information for students, parents, and staff.

b. In or about August 2017, IT Director-1 discovered that an unknown individual had breached a Google platform

----- ("Google Platform-1") used by High School-1. In or about January and May 2018, IT Director-1 observed attempted breaches of Google Platform-1. -----

12. Based on interviews with Victim-3 and Victim-4 (the sister of Victim-3), I have learned the following in substance and in part:

a. Victim-2 dated Victim-3 for a period of time.

b. Beginning in or about December 2018, Victim-3's Google and Snapchat accounts were compromised. Based on my review of Google security alerts sent to Victim-3, and my review of the IP logs for Victim-3's Google account, I learned that an IP address geolocated in Smyrna, Tennessee had accessed Victim-3's Google account. Specifically, Google sent a notification to Victim-3's Google account stating that the password had been changed for the account and that there had been log-ins to the account from a particular IP address ("IP Address-1"). Google stated that the "approximate location" for IP Address-1 was in Smyrna, Tennessee. IP Address-1 falls within a block of IP addresses assigned to "James Rowe" at a particular address in Smyrna, Tennessee—as described in paragraph 18 of this Complaint.

c. Victim-4 stated she had received a text message on or about January 10, 2019 of an adult male penis from the 3569 Phone Number.

d. The father of Victim-3 and Victim-4 ("Victim-5") also reported that he had received multiple harassing phone calls and text messages, in which the sender or caller referred to Victim-2 as his "girlfriend" and sought help in contacting Victim-2. Victim-5 also reported that since in or about December 2018, his residence in the Bronx, New York had been the subject of multiple swatting incidents.

13. Based on my review of records maintained by the NYPD, I have learned that between on or about December 30, 2018 and on or about January 20, 2019, three phone calls were made to 911 from the phone number 212-417-1750. The caller in one of the calls identified himself as "Angus" and gave the 3569 Phone Number as the number to be used to contact him. In that call "Angus" claimed to be suicidal and stated he needed to speak to Victim-2. In the other two calls to 911, the caller falsely reported to police that ongoing emergencies or criminal activity were occurring at the residences of Victim-2 and/or Victim-3.



14. According to records obtained from a Voice over Internet Protocol<sup>1</sup> ("VoIP") provider, the 3569 Phone Number was accessed exclusively from the IP address 68.52.60.74 between on or about January 19, 2019 and January 21, 2019.

15. Based on my review of records obtained from a telecommunications company pursuant to subpoena, on January 20, 2019, IP address 68.52.60.74 was assigned to "James Rowe" at a particular address in Smyrna, Tennessee (the "Smyrna Residence").

16. Based on interviews with the boyfriend of Victim-2's mother ("Victim-6") and a relative of Victim-2 ("Victim-7"), in or about 2017, email accounts belonging to Victim-6 ("Email Account-1") and Victim-7 ("Email Account-2") were compromised. Between September and October 2018, multiple harassing emails were sent to individuals associated with Victim-2's college, including Victim-2's professors, from Email Account-1. In some of those emails, the sender offered to sell photographs of Victim-2 and nude photographs of Victim-6.

17. According to records obtained from a certain email service provider, between in or about July 2018 and January 2019, Email Account-1 and Email Account-2 were each accessed at least 15 times by an IP address within a particular range of IP addresses (the "2601 IP Address Block"). In addition, the Netflix account belonging to Victim-1 was accessed by an IP address in the 2601 IP Address Block on or about November 10, 2018.

18. According to records obtained from a certain telecommunications company, the 2601 IP Address Block is assigned to "James Rowe" at the Smyrna Residence.

19. Based on my review of messages sent on a certain VoIP platform ("VoIP Platform-1") obtained consensually from one of Victim-2's classmates, I have learned the following in substance and in part:

a. While using the Facebook Messenger application, classmates of Victim-2 were invited to participate in a group chat on VoIP Platform-1 by an unknown individual.

---

<sup>1</sup> VoIP allows an individual to conduct voice communications over the internet.

b. In that group chat on VoIP Platform-1, a user identifying himself as "Angus" posted a screenshot of a plotted route on Google Maps from Smyrna, Tennessee to Victim-2's residence in the Bronx, New York, with the note "that's about how far I am."

c. In a chat on VoIP Platform-1, an individual identifying himself as "Angus" told a classmate of Victim-2 that he had a particular birth date ("Birth Date-1").

20. Based on my review of records in an online database, I learned that an individual named "Tristan Rowe" was born on Birth Date-1.

21. Based on a review of Tennessee records conducted by law enforcement in Tennessee, I learned that an individual named "Tristan Rowe" resided at the Smyrna Residence.

22. On or about March 18, 2019, <sup>92 SM</sup> a Circuit Court judge in Rutherford County, Tennessee authorized a search of the Smyrna Residence for evidence including computers.

23. On or about March 19, 2019, that search warrant was executed at the Smyrna Residence. Pursuant to that warrant, multiple electronic devices, including a laptop, were seized, including a desktop computer ("Computer-1"). Those electronic devices were later searched pursuant to a search warrant authorized by a magistrate judge in the Southern District of New York.

24. On that same day, in the Smyrna Residence, and in the presence the father of TRISTAN ROWE, a/k/a "Angus," the defendant, I conducted a voluntary interview of ROWE. Based on that interview, I learned the following in substance and in part:

a. ROWE stated that he first interacted with Victim-2 online in or about February 2014 when they both participated in an online videogame. In or about October 2014, Victim-2 stopped playing that videogame online with ROWE and others. After Victim-2 stopped playing online, ROWE tried to contact Victim-2 but Victim-2 stated that she was not interested in further interaction.

b. ROWE admitted that he was the individual identified as "Angus" and that he was the individual who had



harassed and/or threatened Victim-1 through Victim-4 from in or about 2015 to in or about 2019.

c. ROWE also admitted to calling in false bomb threats to High School-1 and compromising multiple online accounts of Victim-2. He also admitted to making over 100 calls to New York City's 911 phone line falsely reporting emergencies, including falsely reporting emergencies at the homes of Victim-2 and Victim-3.

d. ROWE stated that about five other individuals also participated in the compromises of online accounts related to Victim-2, and others.

25. Based upon my review of Computer-1, conducted pursuant to a judicially-authorized search warrant, I have learned the following, in substance and in part:

a. Computer-1 contained a folder labeled "takeout," which contain files which appear to have been taken from Victim-2's account with Google Platform-1. For example, the folder contained school assignments bearing Victim-2's name.

b. Computer-1 also contained a file with a name referencing High School-1, which contained what appear to be hundreds of usernames and passwords associated with High School-1.

c. Computer-1 also contained a spreadsheet with the names of High School-1 students, the courses those students were enrolled in, and the grades received by those students in those courses.

d. IT Director-1 confirmed that the file referenced in Paragraph 26(c) appears to be genuine confidential information taken from the High School-1 Grading System.

26. In addition, in my review of Computer-1, I discovered evidence of other cyber intrusion activity related to the use of a SQL injection tool.

a. Based on my training and experience, I know that "SQL" is a computing language used to manage databases. A SQL injection is a type of computer compromise that supplies a malicious input to a database. If that database has a security vulnerability, that input can be processed as part of a command

or query, and can allow the perpetrator to obtain unauthorized access to the database.

b. Computer-1 contains a folder called ".SQLMap," which in turn, contains a folder called "output." The "output" folder shows multiple attempts to utilize SQL injection software (the "SQL Malware").

c. When an individual uses the SQL Malware, the SQL Malware automatically generates a folder for that particular target and generates a log file<sup>2</sup> detailing the execution of the SQL Malware.

d. Computer-1 contained log files generated by the SQL Malware—indicating attempts to breach a particular network—for the following entities, among others:

- i. An inmate tracking website used by federal and local law enforcement ("Inmate Tracking Website-1");
- ii. A website for a state Department of Motor Vehicles;
- iii. A website used by a major telecommunications company;
- iv. A reverse phone number lookup website<sup>3</sup> ("Phone Lookup Website-1").

e. Computer-1 also contains data which appears to have been exfiltrated from certain of those networks, including:

- i. Exfiltrated data from Phone Lookup Website-1, including credit card numbers, expiration dates for those credit card numbers, and card verification values (CVVs);
- ii. Exfiltrated data from Inmate Tracking Website-1.

27. In addition, Computer-1 contained evidence, which based on my training and experience, indicates that its user was

---

<sup>2</sup> A log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software.

<sup>3</sup> Reverse phone number lookup websites allow users to input a phone number and find out the user of that phone.



engaged in collecting information that would allow the user to conduct future computer compromises, including the following:

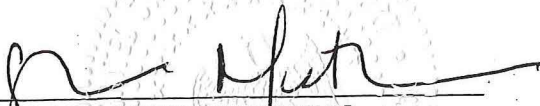
- a. A tool which allows the user to conduct brute force scanning of computer networks for vulnerabilities ("Reconnaissance Tool-1").
- b. Evidence that Reconnaissance Tool-1 was used against the following entities, among others:
  - i. A police department website;
  - ii. The website for a hospital in the Bronx, New York;
  - iii. A state law enforcement website.

WHEREFORE, I respectfully request that a warrant be issued for the arrest of TRISTAN ROWE, a/k/a "Angus," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.



ANTHONY SANTILLI  
Detective  
NYPD

Sworn to before me this  
4th day of February, 2020



THE HONORABLE SARAH NETBURN  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK