UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	HON. STEVEN C. MANNION
	:	
v.	:	Mag. No. 19-6175
	:	
TIMOTHY YOUNG	:	**CRIMINAL COMPLAINT**

I, Schiller Salomon, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

In violation of Title 18, United States Code, Section 1343.

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached page and made a part hereof.

Schiller Salomon, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

May 16, 2019 at Newark, New Jersey

HONORABLE STEVEN C. MANNION
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

From in or about March 3, 2019, through in or about May 2019, in the District of New Jersey and elsewhere, defendant

TIMOTHY YOUNG

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud the Victim Company, as defined below, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, including a wire communication from Young to an undercover law enforcement officer in New Jersey, in violation of Title 18, United States Code, Section 1343.

ATTACHMENT B

I, Schiller Salomon, am a Special Agent with the Federal Bureau of Investigation. I am familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and other evidence. Because this Complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where statements of others are related herein, they are related in substance and in part unless otherwise indicated. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

1. At all times relevant to this Complaint:

a. Defendant TIMOTHY YOUNG ("Young") was a resident of Nebraska and an employee with the Victim Company.

b. The "Victim Company" is data analytics and risk assessment firm based on New Jersey. The Victim Company serves customers worldwide, including entities providing insurance and financial services as well as government entities. The Victim Company maintains a network that houses, among other things, significant amounts of personally identifiable information.

2. On or about March 3, 2019, an individual ("the Individual"), using alias, posted a message on an online forum. The message was titled "[Victim Company] Access for SALE."

3. The message stated, in part:

> I am looking for a person or group who would be interested in buying network login information for a large corporation. It is a Fortune 500 company with annual profits of $2.5B. They are global in nature, but based in the US . . . . Types of databases include all property and casualty insurance claims including personal information . . . complete details of millions of individual buildings, medical claims. Details to every municipal water system in the US, every emergency communications center in the US, and every fire department in the US. . . .

4. The message further stated that the Individual was asking for $2,500,000 in cryptocurrency for this information, and that the money could be put in escrow during the period of the sale.

5. In another post on the same forum later that day, the Individual stated that he worked for the Victim Company.

6. On or about March 7, 2019, a confidential informant ("CI"), who has been reliable in the past, contacted the Individual at law enforcement's request.

7. The CI and the Individual then communicated over the internet. Among other things, the Individual told the CI that the Individual would sell his/her current username and password, and provide both future usernames and passwords as well as any needed assistance the buyer required to access the Victim Company.

8. On or about March 8, 2019, the Individual sent the CI a video ("the Video"). At the beginning of the Video, a sign-in screen is displayed. The username is obscured and the Video shows a password being entered (although the password itself is obscured). Once the password is entered, the Victim Company's internal website is displayed. The Video then displays the Victim Company's Human Resource Management System. As the Video continues, a username and password are entered and a "Sign In" button is clicked. The Video then displays an employee self-service page. This page provides links, to among other information, the employee's paycheck, tax information, and benefits summary – all of which would include personal identification information.

9. Beginning on or about March 7, 2019, an undercover law enforcement officer in New Jersey also communicated with the Individual. The UC offered $1,750,000 in cryptocurrency for the credentials and assistance. On or about March 7, 2019, the Individual sent the UC a screenshot of a spreadsheet ("the Spreadsheet"). The Spreadsheet included columns titled "CHIEF'S NAME," "LOGON NAME" and "PASSWORD." The Spreadsheet included, among other things, telephone numbers, names, logon names, and passwords. According to the Victim Company, the Spreadsheet contained accurate information for some of the Victim Company's clients, and appeared to be data taken from the Victim Company's internal, non-public computer systems.

10. On or about March 8, 2019, the Individual sent the Video to the UC, who received, opened, and watched the video while the UC was in New Jersey. Following these communications, the Individual and the UC largely ceased communicating until in or about May 2019, as discussed below.

11. The CI and the Individual agreed that the Individual would sell access (the username and password, and assistance accessing the Victim Company) for $100,000 upon initial verification and $50,000 a month thereafter until the buyer no longer wanted the access.

12. On or about March 17, 2019, the Individual asked the CI to transfer one bitcoin to him as a showing of good faith, and specifically, to help assure the Individual that the CI is not working with law enforcement. On or about March 19, 2019, in accordance with the Individual's request, law enforcement transferred approximately 1 bitcoin to the Individual via an escrow website, that is a website that would hold bitcoin and thus show the CI possessed the bitcoin, but not release bitcoin until authorized by the CI after completion of the transaction.

13. Later that day, the Individual sent the CI an encrypted email that allegedly contained user credentials for accessing the Victim Company' systems. The email was encrypted, and the CI was unable to access the contents of the mail.

14. Between on or about March 19, 2019 and on or about May 3, 2019, the Individual repeatedly told the CI that the Individual still intended to go through with the sale, but because the Victim Company brought in a private security firm to investigate the matter the Individual wanted to delay going through with the sale. The Victim Company has stated, in substance and in part, that it did bring in a private security firm to investigate the matter.

15. On or about May 3, 2019, the Individual provided a username and password (the "Credentials") to CI. Law enforcement contacted a representative of the Victim Company who stated, in substance and in part, that; (a) the username was associated with a former employee who retired in or about August 2018; and (b) the Victim Company had deactivated the Credentials in connection with the retirement. Law enforcement attempted to log into the Victim Company's system with the Credentials, but was unable to do so.

16. Later that day, May 3, 2019, CI told the Individual, in substance and in part, that the Credentials were not valid. The Individual claimed that he believed the Credentials would work. Shortly after this conversation, the Victim Company's records reflect that someone attempted to gain access to the Victim Company's system using the Credentials. Since on or about that time, the Individual has largely ceased communicating with CI.

17. On or about May 8, 2019, and May 9, 2019, the Individual attempted to contact the UC. The UC responded on or about May 10, 2019. In response, the Individual asked if the UC, in substance and in part, if the UC was still

interested in buying the database shown in the Spreadsheet. The UC and the Individual then entered into and consummated an agreement through which the Individual would sell the database for .5 bitcoin.

18. After the UC paid for received the database, it was reviewed by the FBI and the Victim Company. The database contains thousands of records customers of the Victim, including personal information such as names, addresses, email accounts, and other identifying information. The Victim Company confirmed that this was accurate information taken from their internal, non-public systems.

19. The Individual subsequently offered, in substance and in part, to sell the UC login credentials (username and password) for the Victim Company for .5 bitcoin. The UC, in substance and in part, expressed interest, but demanded proof that the credentials would work.

20. In response, the Individual provided a video demonstrating the credentials worked (the "Second Video"), and demanded 1 bitcoin for the credentials.

21. The Second Video, like the Video, purported to show the credentials being used to successfully access the Victim Company's internal systems. Unlike the earlier Video, the Second Video appeared to show a specific employee ID being used as the username (although the password was obscured). Upon a review of the Second Video, law enforcement observed that the Second Video had been edited to make it appear that the credentials worked when in fact Young was using other credentials to access the Victim Company's network. Specifically, a frame-by-frame analysis revealed that the username employed to access the Victim Company's system was different from the username that Young made it appear was able to access the Victim Company's system.

22. Law enforcement provided the true username used to access the Victim Company's system to the Victim Company. A representative of the Victim Company stated, in substance and in part, that that username is associated with Young and that Young was a current employee of the Victim Company.

23. The Second Video displayed the time and date that Young accessed the Victim Company's systems. The Victim Company's records confirm that at the time the Second Video was made, Young's credentials were used to access the Victim Company's. The Victim Company's and Young's internet service provider's records further demonstrate that the access occurred from an IP address assigned to Young's residence. In addition, the Victim Company's

records show that as part of that access, the Victim Company sent a two-factor authorization code to the Victim Company cellular telephone assigned to Young.

24. Law enforcement interviewed Young on or about May 16, 2019. During the interview, Young stated, in substance and in part, that he: (1) was an employee of the Victim Company; (2) met an individual online and agreed to provide that individual (the "Broker") his access credentials and data stolen from the Victim Company with the understanding that the information would be sold to criminals; (3) expected to be paid once the Broker sold the information; (4) took the database from the Victim Company's internal systems and provided it to the Broker, from which Young expected to receive money; (5) made and edited the Video and the Second Video and provided them to the Broker; (6) initially intended to sell his username and password to access the Victim Company's system, but later decided not to provided his real username and password; (7) provided the username of another employee of the Victim Company to the individual he met online along with a made up password; and (8) provided the database to a second individual he met online.