UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA	)	Case No. 12 CR 146
v.	)	Magistrate Judge Sheila Finnegan
JEREMY HAMMOND also known as ""Anarchaos," also known as "sup_g," also known as "burn," also known as "yohoho," also known as "POW," also known as "tylerknowsthis," also known as "crediblethreat"	)	

AFFIDAVIT IN REMOVAL PROCEEDING

I, ERIC BRELSFORD, personally appearing before United States Magistrate Judge SHEILA FINNEGAN and being duly sworn on oath, state that as a federal law enforcement officer I have been informed that JEREMY HAMMOND, also known as ""Anarchaos," also known as "sup_g," also known as "burn," also known as "yohoho," also known as "POW," also known as "tylerknowsthis," also known as "crediblethreat", (hereinafter "Hammond") has been charged by Complaint in the Southern District of New York with the following criminal offenses: conspiracy to commit computer hacking, in violation of Title 18, United States Code, Section 1030; computer hacking, in violation of Title 18, United States Code, Section 1030; and conspiracy to commit access device fraud, in violation of Title 18, United States Code, 1029.

A copy of the Complaint is attached. A copy of the arrest warrant also is attached.

ERIC BRELSFORD
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 6th day of March, 2012.

SHEILA FINNEGAN
United States Magistrate Judge

CR 12 (Rev. 5/03) ORIGINAL

WARRANT FOR ARREST

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA V. JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat"	DOCKET NO. / MAGISTRATE'S CASE NO. NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED: JEREMY HAMMOND
WARRANT ISSUED ON THE BASIS OF: ☐ Order of Court ☐ Indictment ☐ Information X Complaint	DISTRICT OF ARREST: Southern District of New York
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER	CITY

YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.

DESCRIPTION OF CHARGES

Computer hacking, Access device fraud

IN VIOLATION OF	UNITED STATES CODE TITLE: 18	SECTION: §§ 1029, 1030, 2

BAIL	OTHER CONDITIONS OF RELEASE	
ORDERED BY: RONALD L. ELLIS United States Magistrate Judge	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE): Ronald L. Ellis	DATE ORDERED: MAR 05 2012
CLERK OF COURT: Southern District of New York	(BY) DEPUTY CLERK	DATE ISSUED

RETURN

This warrant was received and executed with the arrest of the above-named person.

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE EXECUTED		

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

ORIGINAL

Approved: _____
THOMAS BROWN/ROSEMARY NIDIRY
Assistant United States Attorneys

Before: THE HONORABLE RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA - v. - JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," Defendant.	**SEALED COMPLAINT** Violation of 18 U.S.C. §§ 1029, 1030 and 2 COUNTY OF OFFENSE: New York

SOUTHERN DISTRICT OF NEW YORK, ss.:

MILAN PATEL, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Hacking)

1. From at least in or about December 2011, up to in or about March 2012, in the Southern District of New York and elsewhere, JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

2. It was a part and an object of the conspiracy that JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I).

Overt Acts

3. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere, by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others:

a. In or about December 2011, HAMMOND, using an online alias, provided credit card information stolen from the computer network of Strategic Forecasting, Inc. ("Stratfor"), a company based in Austin, Texas, as part of several text-based online "chat" messages that were received by a computer located in the Southern District of New York.

b. On or about December 14, 2011, HAMMOND, using an online alias, exchanged online chat messages with a co-conspirator not named herein ("CC-2"), in which HAMMOND stated that he had hacked into Stratfor's computer network.

c. On or about December 19, 2011, a co-conspirator not named herein ("CC-1") uploaded data stolen from a Stratfor email database to a server located in the Southern District of New York.

(Title 18, United States Code, Section 1030(b).)

COUNT TWO
(Computer Hacking)

4. From at least in or about December 2011, up to in or about March 2012, in the Southern District of New York and elsewhere, JEREMY

HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, willfully and knowingly caused the transmission of a program, information, code and command, and, as a result of such conduct, intentionally caused and attempted to cause damage without authorization, to a protected computer, which caused and attempted to cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 to one and more persons during any one year period, to wit, HAMMOND and others gained unauthorized access to computer systems used by Stratfor, a company which provides information analysis services for its clients, and, among other things, defaced Stratfor's website; stole confidential data from Stratfor's computer network, including Stratfor employees' emails, as well as personally identifying information and credit card data for Stratfor's clients; publicly disclosed at least some that data by dumping it on certain Internet websites; and deleted data on Stratfor's computer network.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b), 1030(c)(4)(B)(i), and 2).

COUNT THREE
(Conspiracy to Commit Access Device Fraud)

5. From at least in or about December 2011, up to in or about March 2012, in the Southern District of New York and elsewhere JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3), and 1029(a)(5).

6. It was a part and an object of the conspiracy that JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did traffic in and use one and more unauthorized access devices during a one year period, and by such conduct would and did obtain a thing of value aggregating $1,000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

7. It was further a part and an object of the conspiracy that JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did possess fifteen and more devices which were unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

8. It was further a part and an object of the conspiracy that JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others known and unknown, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did effect transactions, with one and more access devices issued to another person and persons, to receive payment and another thing of value during a one-year period the aggregate value of which was equal to or greater than $1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

Overt Act

9. In furtherance of the conspiracy and to effect the unlawful objects thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others:

a. In or about December 2011, HAMMOND, using an online alias, provided credit card information stolen from the computer network of Stratfor as part of several text-based "chat" messages that were received by a computer located in the Southern District of New York.

(Title 18, United States Code, Section 1029(b)(2).)

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

10. I have been a Special Agent with the FBI for the last eight years. I am currently assigned to the Computer Intrusion Squad of the New York Division of the FBI, and have received training in computer

technology, computer fraud, access device fraud, identity theft, and other white collar crimes. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my examination of reports and records, interviews I have conducted, and conversations with other law enforcement officers and other individuals. 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, unless noted otherwise.

OVERVIEW

11. As detailed below, the FBI's investigation to date has revealed that, from at least in or about December 2011, up to in or about March 2012, JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, has participated in sophisticated computer hacking activities, including a hack of Strategic Forecasting, Inc., a private, subscription-based provider of information analysis services with offices in Austin, Texas ("Stratfor" and "Stratfor Hack").

12. In particular, at least in or about early December 2011, JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and his co-conspirators, among other things: (1) obtained unauthorized access to computer systems used by Stratfor, (2) stole confidential information from those computer systems, including Stratfor employees' emails, as well as account information for approximately 860,000 Stratfor subscribers or clients; (3) publicly disclosed at least some of the stolen confidential information on certain websites; and (4) stole information for approximately 60,000 credit card users; and (5) used some of the stolen credit card data to make at least $700,000 worth of unauthorized charges without the knowledge or consent of the credit card account holders.

TECHNICAL BACKGROUND

13. Based on my training and experience, I am aware of the following:

a. **IP addresses.** Internet Protocol ("IP") addresses are unique numeric addresses used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be routed properly from its source to its destination.

b. **MAC addresses.** Media Access Control ("MAC") addresses are unique identifiers often assigned by manufacturers to devices attached to computer networks, including, among other devices, computers and wireless routers. MAC addresses often include specific numbers that identify the particular manufacturer of the device.

c. **Computer servers.** A computer server is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email or Internet web pages, or accesses files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "Web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

d. **Instant messaging, IRC and Jabber.** Instant messaging (IM) is a collection of technologies that permit users to engage in real-time communication, or "chats" over the Internet. Internet Relay Chat ("IRC") is a form of IM that can allow groups of individuals to have live, text-based chats. IRC users chat over so-called "channels," which may be open to the public or may be restricted, invitation-only channels which are password protected. IRC channels are typically identified by the naming convention "#[channel name]". IRC users are identified by usernames of their choice, which are often

aliases. "Jabber" refers to another form of IM. So-called "Jabber servers" are computer servers that use specialized software to host one or more user accounts, from which users can communicate in real time with other users on the same or different Jabber servers via text or other methods of exchange. A Jabber server is identified by a domain name, e.g., "example.com." User accounts are identified by the naming convention "[username]@[example.com]. Chats via Jabber, unlike some other forms of IM, can be encrypted. Jabber users also often employ aliases as usernames. Transcripts of Jabber and IRC chants are often referred to as "logs."

e. **TOR.** The Onion Router ("TOR") is a system designed to enable users to access the Internet anonymously. Users employ software that automatically and randomly routes their Internet communications through a network of so-called TOR servers, which obscure a user's own IP address as well as the IP addresses of other computers on the Internet which they access.

f. **Domain names.** A domain name is a simple, easy-to-remember name that identifies a particular computer or site on the Internet. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." Each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain. For example, the domain name "www.example.com" means that the computer assigned that name is in the ".com" top-level domain and the "example" second-level domain, and is a web server (denoted by the "www").

g. **.onion.** ".onion" is a naming convention similar to traditional domain names (described above), but designed to hide computer servers on the Internet as well as the individuals accessing those computers. In particular, .onion is a so-called pseudo top-level domain name that designates computers which are accessible via TOR using particular software, but which are otherwise not easily found on the Internet. Designating a computer using the .onion pseudo top-level domain name, among other things, not only makes it more difficult for others to locate and identify a particular .onion computer, but also tends to hide the individuals accessing that computer.

BACKGROUND ON ANONYMOUS, LULZSEC, AND ANTISEC

14. Based on my training and experience, I know that "Anonymous" is a loose confederation of computer hackers and other individuals

located in the United States and elsewhere. Certain members of Anonymous have, since at least in or about 2008, waged a deliberate campaign of online destruction, intimidation, and criminality, as part of which they have carried out cyber attacks against businesses and government entities in the United States and around the world. These attacks have included, among other things, unauthorized access to, and the theft and later dissemination of confidential information from, victims' computer systems, as well as the defacement of victims' Internet websites. These attacks have also included attacks against websites, known as "denial of service" or "DoS" attacks, which involved the use of computers to bombard a victim's website with bogus requests for information, causing the website to temporarily cease functioning.

15. Based on my participation in this investigation, I know that, in or about May 2011, certain individuals affiliated with Anonymous formed a group that they called "Lulz Security," or "LulzSec." The members of LulzSec undertook cyber attacks against the computer systems of various business and government entities in the United States and throughout the world. Among other things, LulzSec has claimed responsibility for cyber attacks on the websites and computer systems of victims that include, among others, Sony Pictures Entertainment, a division of Sony, a global electronics and media company; the Public Broadcasting Service, a non-profit public television broadcasting service; the Atlanta, Georgia chapter of Infragard, an information sharing partnership between the FBI and private industry concerned with protecting critical infrastructure in the United States; and Bethesda Softworks, a video game company based in Maryland.

16. Based on my participation in this investigation, I know that one of the members of LulzSec ("CW-1") was arrested by law enforcement, and agreed to cooperate with the Government in the hope of receiving a reduced sentence. CW-1 has pleaded guilty to various charges, including charges relating to computer hacking, pursuant to a cooperation agreement with the Government. I have found that the information provided by CW-1 has been accurate and reliable, and corroborated by other information developed in this investigation.

17. Based on my participation in this investigation, including information provided by CW-1, I have learned that in or about June 2011, several members of LulzSec joined with other individuals who were affiliated with Anonymous to create a new hacking group called "Operation Anti-Security," or "AntiSec." AntiSec has, among other things, publicly encouraged cyber attacks on government-related entities. In addition, AntiSec has publicly claimed responsibility

for: (1) the intrusion into, and subsequent release of data stolen from, computer systems used by more than 50 police departments in the United States; (2) an intrusion into the computer systems of the North Atlantic Treaty Organization ("NATO"); and (3) the Stratfor Hack.

THE INVESTIGATION

A. The Stratfor Hack

18. Based on my participation in the investigation, including conversations I have had with another FBI agent who has spoken to representatives of Stratfor; my conversations with CW-1; my review of transcripts of online chats between CW-1, an individual later identified to be JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and others (discussed in detail below); and publicly available information, including confidential data from Stratfor that was publicly disseminated on various websites following the Stratfor hack, I know the following:

a. Stratfor maintained a website, www.stratfor.com, through which it provided subscription-based information analysis services to its clients. Stratfor's clients included private individuals and entities, various United States Government agencies, including law enforcement agencies and their employees, as well as foreign law enforcement organizations and their employees. Stratfor's clients could register for online accounts that were identified by individual usernames and were password protected. As part of the registration process, Stratfor collected and stored on its computer systems in Austin, Texas information from each of its clients. This information included one or more of the following: the client's name, address, affiliated organization or agency, email address, credit card number, and associated CVV[1] and credit card expiration date. Stratfor stored its clients' passwords in an encrypted form called an "MD5 hash," but stored other client information, including credit card numbers and associated data, in clear text.

[1] A card verification value ("CVV") is generally a three-digit code that typically appears on the reverse side of credit cards. An anti-fraud measure, CVVs are often used for online transactions to verify that the credit card user is in possession of a valid credit card at the time of the transaction.

b. As discussed in detail below, starting in or about December 2011, HAMMOND and his co-conspirators obtained unauthorized access to Stratfor's computer systems. Between at least in or about early December 2011, up to and including on or about December 24, 2011, HAMMOND and his co-conspirators stole multiple gigabytes[2] of confidential data from Stratfor's computer systems, including, among other things: (1) approximately 60,000 credit card numbers and associated data, including CVVs and expiration dates, belonging to Stratfor clients; (2) records for approximately 860,000 Stratfor clients or subscribers; (3) Stratfor employees' emails; and (4) internal Stratfor corporate documents, including company financial data.

c. On or about December 24, 2011, HAMMOND and his co-conspirators briefly defaced Stratfor's website, www.stratfor.com, before executing one or more commands to delete data stored on Stratfor's computer servers, including the server that stored Stratfor employees' emails and the server that hosted Stratfor's website. As a result, among other things, Stratfor's website was rendered inoperable and remained offline for approximately the following six weeks,[3] and data stored on Stratfor's computer servers, including Stratfor's employees' stored emails and historical archives of Stratfor's analysis products, was deleted.

d. On or about December 25, 2011, a document titled "antisec teaser 12/25" was posted on a file sharing website. The document included several links to what appear to be files of stolen Stratfor data, as discussed below, as well as the following text, among other things:

> How is everybody enjoying Lulzxmas so far? Did you enjoy the epic defacement and destruction of Stratfor's websites? . . . Attached are ~4000 credit cards, md5 passwords, and home addresses to just a few of Stratfor's "private client list".

e. On or about December 25, 2011, a document titled

---

[2] A gigabyte is a measure of data storage equivalent to approximately 675,000 pages of text.

[3] As of the date of this Complaint, Stratfor's website is still not fully operational. For example, Stratfor's web-based paid subscription service has not yet been repaired.

"Anonymous Lulzxmas rooting your proud" was posted on a file sharing website. The document, which references "Merry LulzXmas" and "#AntiSec," includes text that appears to demonstrate unauthorized access to Stratfor's computer systems. The document also included what appears to be a link to a file of stolen Stratfor data, as discussed below.

f. On or about December 26, 2011, a document titled "antisec teaser 12/26" was posted to a file sharing website. Like the document titled "antisec teaser 12/25," this document contained similar references to "Merry LulzXmas" and "AntiSec." In addition, the document stated, among other things, that "over $500,000 [is] being expropriated from the bigshot clients of Stratfor," as well as the following:

> Accordingly, we'll start the day after Christmas off right by dropping a third of the damn alphabet. How does a drop of 30,000 additional names, credit cards, addresses, phone numbers, and md5 hashed passwords sound? Sounds like financial calamity to us.

The document also referred to "private mail spools [email databases] that we'll be dropping later," and included what appear to be several links to stolen Stratfor data, as discussed below.

g. On or about December 29, 2011, a document titled "antisec teaser 12/29 (legit)" was posted on a file sharing website. This document contained the same references to "Merry LulzXmas" and "#AntiSec" as the prior two documents, as well as the following text, among other things:

> It's time to dump the full 75,000 names, addresses, CCs and md5 hashed passwords to every customer that has ever paid Stratfor.
>
> But that's not all: we're also dumping ~860,000 usernames, email addresses, and md5 hashed passwords for everyone who's ever registered on Stratfor's site.
>
> * * *
>
> We call upon all allied battleships, all armies from darkness, to use and abuse these password lists and credit card information to wreak unholy havoc upon the systems and personal email accounts of these rich and powerful oppressors.

The document also included what appear to be links to files containing stolen Stratfor data, as discussed below.

h. I have reviewed files found on a .onion server using one of the links attached to one or more of the documents discussed above. Based on my review, I learned that: (1) those files' names are the same as file names contained in one or more links attached to each of the above-discussed documents; and (2) at least two of the files contain what appears to be information regarding over 860,000 Stratfor clients, including individual user IDs, usernames, encrypted passwords, and email addresses, among other data; and what appears to be names, physical addresses, and credit card numbers and associated CVVs and expiration dates, among other data, for nearly 60,000 Stratfor clients.

i. On or about January 6, 2012, an email purporting to be from a Stratfor executive was sent to email accounts belonging to Stratfor customers whose account files had been compromised during the Stratfor Hack. Attached to the email was a document titled "Official Emergency Communique Straight from the Anonymous Hacker Underground" and which referred to "Merry LulzXmas" and the IRC channels "#anonymous," "#antisec," "#lulzxmas," among others. The document cited the Stratfor Hack, as well as cyber attacks on, and data thefts from, computer systems associated with the websites www.nychiefs.org, which is the website of the New York State Association of Chiefs of Police, www.cslea.com, which is the website of the California Statewide Law Enforcement Association, and www.specialforces.com, a website that sells military and police equipment. Regarding the Stratfor Hack, the document included the following statement:

> The sheer amount of destruction we wreaked on Stratfor's servers is the digital equivalent of a nuclear bomb: leveling their systems in such a way that they will never be able to recover. We rooted box after box on their intranet: dumping their mysql databases, stealing their private ssh keys, and copying hundreds of employee mail spools. For weeks, we used and abused their customer credit card information (which was all stored in cleartext in their mysql databases), eventually dumping [stealing] all 75,000 credit cards and 860,000 md5-hashed passwords of their "private client list". And if dumping everything on their employees and clients wasn't enough to guarantee their bankruptcy, we laid waste to their webserver, their mail server, their development server, their clearspace and srm intranet portal and backup archives in such a way that

ensures they won't be coming back online anytime soon.

In addition, the document included a claim that more than $500,000 in unauthorized charges had been made to credit cards stolen through hacking activity, including unauthorized charges to make "donations to dozens of charities and revolutionary organizations."

j. As discussed in more detail below, at or around the time the Stratfor Hack took place, CW-1, at the direction of the FBI, provided to HAMMOND and his co-conspirators a computer server in New York, New York, which could be used to store data, and to which HAMMOND and his co-conspirators in fact transferred data.[4] I have spoken to an employee of the FBI who reviewed the transferred data, and learned that it was similar in content and format to the data found in the files found on the .onion server discussed above.

k. From on or about December 6, 2011, up through early February 2012, at least approximately $700,000 worth of unauthorized charges were made to credit card accounts that were among those stolen during the Stratfor Hack.[5]

l. As a result of the Stratfor Hack, Stratfor has incurred more than $1 million in costs and damages associated with, among other things, responding to the hack, conducting a damage assessment, and restoring or attempting to restore its computer systems and the data stored on them to their condition before the hack. Stratfor also estimates that it has lost more than $1 million in revenue due to the Stratfor Hack, including because of the inoperability of its website.

---

[4] Based on my experience with the investigation, including my review of chats described herein, I believe that HAMMOND and his co-conspirators used multiple servers to store stolen data, including credit card data stolen during the Stratfor Hack. CW-1 did not further disseminate any data that HAMMOND or his co-conspirators stored on the New York Server.

[5] This figure does not reflect any of the charges that may have been incurred on cards associated with the Stratfor Hack for which records have not yet been reviewed.

B. **Evidence of the Defendant's Involvement in the Stratfor Hack**

19. Evidence collected during this investigation, including online chats obtained by CW-1, documents posted to a file sharing website shortly after the Stratfor Hack occurred, and stolen Stratfor data that was transferred to a computer server operated by CW-1, as discussed in detail below, shows that JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, was a principal participant in a criminal scheme to gain unauthorized access to Stratfor's computer network, steal confidential information from that network, and exploit and publicly disclose these sensitive data.

20. During the course of the investigation, CW-1 has obtained certain chats between and among various individuals who - based on, among other things, the contents of the chats and information provided by CW-1 - were members of Anonymous, LulzSec, and/or AntiSec.[6] Based on my experience investigating computer crimes, I know that individuals involved in computer-related criminal activity often use multiple accounts and usernames, including IRC and Jabber usernames, to mask their identities. Also based on that experience, I know that it is possible, based on how online chats are logged by certain IM applications such as IRC and Jabber, as well as how individuals communicate with each other over the Internet, to associate an individual with two or more online aliases. For example, if during the course of an IM chat there is a question about the identity of an individual, others in the chat will often seek to verify the individual's identity by, among other things, asking questions about previous online interactions. In addition, if an IM user knows an individual by multiple aliases, the user may refer to that individual using different aliases during the same chat. At times, chat logs, including IRC and Jabber chat logs, will also identify that a user who previously logged in with a different alias is now logging in with a new name. Through these various methods, in the course of this investigation, I have identified a number of different online aliases that the defendant used to communicate with CW-1 and others, including the following: "anarchaos,"[7] "yohoho,"[8] "sup_g,"[9] "burn,"[10]

---

[6] CW-1 participated in the various chats set forth in this Complaint under the supervision of the FBI. CW-1 was in New York, New York when he participated in the chats.

[7] This is the alias that the defendant used primarily to communicate with CW-1 and others in June and July 2011.

"ghost_,"[11] "tylerknowsthis,"[12] "POW,"[13] and "crediblethreat"[14].

---

[8] The defendant used the alias "yohoho" to communicate with CW-1 over Jabber.

[9] For example, in a chat with the defendant on or about December 26, 2011, discussed in greater detail below, CW-1 referred to the defendant as both "sup_g" and "anarchaos." The defendant responded to both aliases. In a chat with CW-1 over Jabber on or about November 6, 2011, the defendant, using the alias "yohoho," told CW-1 "k im sup_g," that is, identifying himself as both "yohoho" and "sup_g."

[10] Chat logs collected by CW-1 reflected that when "sup_g" logged in, he was sometimes referred to as "burn" by others involved in the chat. In a chat on or about November 8, 2011, "sup_g" and others discussed the fact that "sup_g" also had used the alias "burn." Similarly, "yohoho," the Jabber alias that the defendant would use to communicate with CW-1, discussed in a chat with CW-1 on or about November 7, 2011 that another individual had suspected "yohoho" was "burn." Specifically, "yohoho" said: "I never answered though . . . I think he picked up some language similarities I've worked with [another individual] on other ops [operations] in the past."

[11] For example, a chat log dated on or about November 13, 2011 reflected that "ghost_ is now known as sup_g" when joining the chat.

[12] For example, a chat log dated on or about March 1, 2011 reflected that "ghost_ is now known as tylerknowsthis" when joining the chat.

[13] CW-1 reported that the individual using the nickname "anarchaos" also used "POW." In a chat on July 21, 2011, POW was asked "who is POW?" and responded "old school new name"; when asked "POW: your old nick ?" POW responded: "something anarchist related maybe."

[14] For example, in a chat on or about January 20, 2012, the defendant, using the alias "yohoho," told CW-1: "btw [by the way] 'crediblethreat' is me on antisec [an IRC channel]," indicating that he used the alias "crediblethreat" when chatting on the antisec IRC channel.

The December 6, 2011 IRC Chat

21. I have reviewed a copy of a private online chat that occurred on or about December 6, 2011 between an individual using the alias "sup_g," later identified as the defendant, and CW-1. During this chat, the defendant describes how he was attacking Stratfor's computer systems: [15]

<sup_g> yo
<sup_g> you round?
<sup_g> working on this new target
* * *
<CW-1> yo
<CW-1> im here
<sup_g> =)
<sup_g> we real good here
<sup_g>
http://ibhg35kgdvnb7jvw.onion/inc0ming/stratfor.jpg
<-their admin panel
* * *
<sup_g> basicly this site [www.stratfor.com] is a paid membership where they gain access to articles
<sup_g> it stores billing info as well - cards
<sup_g> it's encrypted though
<sup_g> I think I can reverse it though but the encryption keys are store on their server (which we can use mysql to read)
<sup_g> when I get the key I can write a script ti [to] export the data en mass

[15] The text of the chats is reproduced in this Complaint as it appears in the chat logs I have reviewed; errors in spelling and punctuation have not been corrected. Each participant or "speaker" in a chat is identified by an alias. For example, <sup_g> indicates a statement from an individual using the alias "sup_g." Where statements from individuals other than the defendant are reproduced herein, those individuals' aliases have been redacted and replaced with <CC-1>, <CC-2>, <CW-1>, etc., as appropriate. Based on my training and experience, my participation in the investigation, and my familiarity with language used on the Internet, I have included certain interpretations of the overall content of selected chats. I have also included, in brackets, interpretations of certain terms, phrases, and abbreviations contained in the chats.

Later in the chat, the defendant describes how he had stolen data from the www.nychiefs.org website and planned to exploit it:

<CW-1> whats latest with that nychiefs ownage? You done with it or?
<sup_g> I tried every login/password that was cracked
<CW-1> mmm
<sup_g> dumped [stole] em all and can upload in a few days
<sup_g> so we can have people parse them and shit
<CW-1> sounds good
<sup_g> find juicy bits
<sup_g> if we can crack more hashes, we'll get more emails

The December 14, 2011 IRC Chat

22. I have reviewed a copy of a chat that occurred on or about December 14, 2011 over the #lulzxmas IRC channel between an individual using the alias "sup_g," later identified as the defendant, and CC-2. During this chat, the following exchange took place, in which the defendant bragged of having hacked into Stratfor's computer network and boasted of the damage that he and his co-conspirators would cause to Stratfor as a result of the hack:

<@sup_g> =)
<@sup_g> we in business baby
<CC-2> w00t?
<@sup_g> oh yes
<@sup_g> time to feast upon their spools [email databases]
<CC-2> stratfor?
<@sup_g> oh yes.
<@sup_g> after yall left yesterday I spent another eight hours
<@sup_g> and rooted [hacked] that mofo
<CC-2> They're so done now...
<@sup_g> Yeah it's over with.
<@sup_g> In their emails they were complaining of a few minute downtime as interrupting their business.
<@sup_g> I think they'll just give up after this goes down

The December 19, 2011 IRC Chat

23. I have reviewed a copy of a chat that took place on or about December 19, 2011 over the #lulzxmas IRC channel between an individual using the alias "sup_g," later identified as the defendant, and a

co-conspirator not named as a defendant herein ("CC-3") (the "December 19 Chat").

a. During the December 19 Chat, the following exchange took place:

<@sup_g> also do yall know if the mail was copied successfully?
* * *
<@sup_g> [CC-1] said he got it going, copying them all in it's entirety
* * *
<@sup_g> not sure if it finished though: and don't want to hop on the box now because it is biz hours for them
<CC-3> i m ftp'ing like 30gb of something [CC-1] asked
<@sup_g> clearspace? or the other thing
<CC-3> yep that
<@sup_g> ok clearspace is good but the mail is probably more relevant
<CC-3> the other thing is kinda 200gb
<CC-3> i dunno how we ll do that
<@sup_g> oh yah that must be mail =(

In the excerpt set forth above, the defendant was inquiring as to whether CC-1 had successfully copied an e-mail database that the defendant and his co-conspirators had stolen from Stratfor's computer network. The term "clearspace" refers to a web-based application that is used to support the operation of websites, among other things. In the above excerpt, the defendant and CC-3 discussed whether it was more useful to exploit the stolen Stratfor email database or Stratfor's clearspace platform, and the defendant preferred to exploit the stolen email database.

b. Later in the December 19 Chat, the defendant had the following exchange with a co-conspirator:

<@sup_g> I was thinking we order some servesr with them stolen CCs [credit card numbers].
<@sup_g> lots of servers with big hard drives.
<@sup_g> and make four or five mirror .onions with them
<@sup_g> a few will go down right away, a few might now.
<@sup_g> not.
<CC-3> [referring to CC-2]: can u get an offshore server with one of those verified CCs?
<CC-3> i ll try it too
<@sup_g> since web/onion is really the most practical way to

browse these mails and clearspace
<@sup_g> torrent is damn impractical, no one will download
<@sup_g> we might want to offer it anyway but even so, focus on web viewing

In the above exchange, the defendant proposed to use credit card data stolen during the Stratfor Hack to purchase .onion servers, which he and his co-conspirators could use to store surreptitiously and review anonymously data that they had stolen from Stratfor.

c. The December 19 Chat continued:

<CC-3> hm i was thinking about
<CC-3> getting servers with CCs
<CC-3> they ll die soon if discovered ofc [of course]
<CC-3> and give address to media outlets
<CC-3> so they take the emails to analyse themselves
<@sup_g> it may be till the end of the mnth before the cc owner recognizes the bad charges

In this exchange, the defendant and CC-3 discussed how to publicly distribute stolen Stratfor emails. They were also concerned about when the account holders of the stolen credit cards would notice unauthorized charges, and the defendant concluded that he and his co-conspirators would have until the end of the month to make unauthorized charges to the cards.

The First December 26, 2011 IRC Chat

24. I have reviewed a copy of a chat that took place on or about December 26, 2011 over the #lulzxmas IRC channel between an individual using the alias "sup_g," later identified as the defendant, and a co-conspirator not named as a defendant herein ("CC-4"). During that chat, the following exchange took place:

<@sup_g> hmm we need to repair and render these mails
<@sup_g> .tar file has issues
<@sup_g> we need more deployment servers as well that have enough space
<@sup_g> touching up press release and uploading this morning's card dump to multiple sites now, then I'll try extracting the attachments from their sql db
<@sup_g> sorry not as fun as owning shit
<CC-4> kk
<CC-4> can u upload that tar file into a server of mine ?

<CC-4> what protocol do u prefer, sftp ?
<@sup_g> either, i'll copy via screen
<@sup_g> but hmm wait
<@sup_g> might want to check with [CW-1] first, as it's his box [computer server], and ip info must be guarded
<@sup_g> this is just our first base of operations till we can move it elsewhere
<@sup_g> which we need to despareately

In the above exchange, the defendant and CC-4 discussed various tasks they were doing in connection with the Stratfor Hack, including drafting a "press release" announcing the hack and the steps required to make the stolen emails and credit cards available for exploitation. As part of the discussion, the defendant directed CC-4 to check with the CW-1 before uploading stolen data onto a server located in New York, New York, that CW-1, under the supervision of the FBI, had made available to the defendants and his co-conspirators (the "New York Server").

The Second December 26, 2011 IRC Chat

25. I have reviewed a copy of a second chat that took place on or about December 26, 2011 over the #antisec IRC channel between an individual using the alias "sup_g," later identified as the defendant, CC-4, and another co-conspirator not named as a defendant herein ("CC-5") (the "Second December 26 Chat").

a. During the Second December 26 Chat, the following exchange took place:

<@sup_g> I logged into clearspace.stratfor.com from a sysadmin account for a few.
<CC-4> 6.x remote pwnage
<@sup_g> Within 5-10 minutes, I saw NYPD SHIELD reports
<@sup_g> It's almost all PDF attachments.
* * *
<CC-5> DO we still have any of the 90k cc's ? wouldent mind going on some shoping
* * *
<@sup_g> [CC-5]: dropped a 30k already this morn
<@sup_g> but the rest is available.
<CC-4> prolly [probably] their internal IM system
<@sup_g> I have all of that locally.
<CC-4> [CC-5]: what would u shop ?
<@sup_g> Also another db 'rt' but I have to see what's in it.

<@sup_g> Clearspace is gon be the goods, besides the mail, and user accounts
* * *
<@sup_g> FYI: we have a private password list of the 860,000 users, grepped [filtered] for .mil and .gov and having an initial set of md5s run against it, for everyone here.
<@sup_g> 50k users, 4.5k users cracked

In the above chat, the defendant, CC-4 and CC-5 were discussed details about the data that they had stolen during the Stratfor Hack. Among other things, the defendant referred to the domain name for Stratfor's clearspace database, on which he stated that he found "NYPD SHIELD reports." I know, based on my training and experience, that NYPD SHIELD refers to a New York City Police Department ("NYPD") umbrella program encompassing a number of public/private security-related initiatives. The defendant and his co-conspirators also discussed stolen credit card numbers, with CC-5 inquiring whether 90,000 stolen credit cards were still available. In addition, the defendant and his co-conspirators also discussed passwords - including for government and military email accounts - that they had stolen. The defendant specifically pointed out that they had "cracked" (de-encrypted) the passwords of "4.5k" (or 4.5 thousand) of 50,000 users.

b. Later in the Second December 26 Chat, the defendant and his co-conspirators discussed how to exploit the stolen credit card data:

<@sup_g> we do have CCs in human readable format available, ones that haven't been released yet
<CC-4> i dont have reputation anymore in bitcoin-otc
<CC-5> is it full cc's with ccv and shit?
<CC-4> yy
<CC-4> and cvv+address
<@sup_g> if people want to go to town, however, all their clients have been notified, and it's possible their identift theft people are working on their DB
<CC-5> we need to act fast
<CC-4> yeah but non-US clients will be on vacation and shit
<CC-4> ive used some .de cards today
<CC-4> without a problem :P

The Third December 26, 2011 IRC Chat

26. I have reviewed a copy of a third chat that took place on or about December 26, 2011 over the #lulzxmas IRC channel between an

individual using the alias "sup_g," later identified as the defendant, and CW-1, during which the following exchange occurred:

<CW-1> yo yo
<@sup_g> hey homeboii
<@sup_g> its' all real good =)
<CW-1> :)(just woke up
<CW-1> took a na
<CW-1> na
<@sup_g> [CC-1] hooking it up with custom script to parse them things as we speak
<CW-1> hows the news looking?
<@sup_g> I been going hard all night
<CW-1> I heard we're all over the news papers
<CW-1> you mother fuckers are going to get me raied ["raided," i.e., arrested]
<CW-1> HAHAHAAHA
<@sup_g> we put out 30k cards, the it.stratfor.com dump, and another statement
<@sup_g> dude it's big..
<CW-1> raided
<CW-1> if I get raided anarchaos your job is to cause havok in my honor
<CW-1> <3
<CW-1> sup_g:
<@sup_g> it shall be so

In the foregoing excerpt, the defendant and CW-1 discussed the media's reaction to the Stratfor Hack (the Stratfor Hack was first publicized in the media on or about December 24, 2011). Notably, CW-1 referred to the defendant by two different aliases - "sup_g" and "anarchaos" - and the defendant responded to both. The defendant also informed CW-1 about the status of the defendant's and his co-conspirators' exploitation of stolen Stratfor data. In particular, the defendant explained that CC-1 was "parsing" the database, that is, processing it into a format that could be easily reviewed and transferred to the New York Server that CW-1 had made available to the defendant and his co-conspirators. According to the defendant, the data that had been uploaded to the New York Server included "30k cards" - that is, information from 30,000 stolen credit cards. With the assistance of an FBI computer scientist, I have reviewed contents of the New York Server shortly after the forgoing data was uploaded to it and have confirmed that the New York Server contained, among other things, account information for approximately 60,000 credit cards. As

discussed above, the content and format of this information matched data which appears to have been stolen during the Stratfor Hack.

The Fourth December 26, 2011 IRC Chat

27. I have reviewed a copy of a chat that took place on or about December 26, 2011 over the #antisec IRC channel between an individual using the alias "sup_g," later identified as the defendant, CW-1, and two co-conspirators not named as defendants herein ("CC-6" and "CC-7"), during which the following exchange took place:

<@sup_g> also confirmed: mails are on the way
<CW-1> weeee
<CC-6> lol
<CW-1> you already extracted and making htmls of the mails?
<CC-7> !!!
<CC-6> ur not high again ru?
<CC-7> are they searchable?
<@sup_g> [CW-1] no but I just checked on [CC-1]'s script and it is exporting correctly.

In the foregoing excerpt, the defendant followed up on CC-1's work to process stolen Stratfor emails and confirmed that the emails were being transferred to the New York Server provided by CW-1.

The December 31, 2011 IRC Chat

31. I have reviewed a copy of a chat that took place on or about December 31, 2011 over the #lulzxmas IRC channel between an individual using the alias "sup_g," later identified as the defendant, and CC-3 (the "December 31 Chat").

a. During the December 31 Chat, the following exchange took place:

<@sup_g> we can still deface cslea with their CC info
<@sup_g> and drop the CA/NY emails
<CC-3> yep great
<@sup_g> omfg
<CC-3> thats pretty muchs something cool on eve

Based on my participation in the investigation, I know that "cslea" refers to the California Statewide Law Enforcement Association ("CSLEA"). According to publicly available information, on or about December 31, 2011, one or more individuals associated with Anonymous

claimed to have gained unauthorized access to computer servers associated with the CSLEA website and posted on the Internet data that had been stolen from the CSLEA's computer network. The FBI has confirmed that the CSLEA website was hacked. Publicly available information also indicates that, in or about early January 2012, one or more individuals associated with AntiSec claimed to have gained unauthorized access to computer servers used by various New York State police chiefs and to have stolen emails from those computer servers. Based on my training and experience, as well as my participation in the investigation, I believe that the above chat excerpt refers to these computer hacking activities.

b. Later in the December 31 Chat, the defendant and CC-3 discussed the contents of a stolen Stratfor database in the following exchange:

<@sup_g> this stratfor list had [former U.S. Government official]
<CC-3> hahah probably
<@sup_g> former cia director
<@sup_g> [another former U.S. Government official]
<@sup_g> and former vice president [name]
<@sup_g> I can't think of many people higher on the food chain
<CC-3> great
<CC-3> u should pick up also
<CC-3> some of them
<@sup_g> [first name] motherfucking [last name]
< CC-3> to post
<@sup_g> well we already posted em

The January 2, 2012 IRC Chat

32. I have reviewed a copy of a chat that took place on or about January 2, 2012 over the #antisec IRC channel between an individual using the alias "sup_g," later identified as the defendant, CC-2, and CC-3, during which the following exchange took place:

<CC-3> but this stratfor shit was bigger shit than
<CC-3> old shits
<CC-3> at least it deserves no critics
<@sup_g> oh yes
<@sup_g> notice no one is throwing around script kiddie comments
* * *
<CC-2> [CC-3]: Yeah, but this time it's massive.
* * *

<CC-3> this time was classy
<CC-3> and thats perfect
<CC-3> we produced a cool video
* * *
<CC-3> we announced lulzxmas
<CC-3> we hacked big shit
<CC-3> we donated by 1000000
* * *
<CC-3> and we destroyed a big serious intel corp
<CC-3> actually just a lil bunch of ppl thinks shit on this
<CC-3> like 3
<CC-3> lol
<@sup_g> they are just mad because of the sheer amount of high profile people in this

In the foregoing excerpt, the defendant, CC-2, and CC-3 congratulated themselves on the Stratfor Hack, complained about critical press coverage, and boasted of the harm they had caused Stratfor as a result of the hack ("we destroyed a big serious intel corp"). They also congratulated themselves on having "donated," i.e., made unauthorized charges, worth one million dollars using credit card data stolen during the Stratfor Hack.

The January 5, 2012 IRC Chat

33. I have reviewed a copy of a chat that occurred on or about January 5, 2012 over the #antisec IRC channel. During this chat, an individual using the alias "sup_g," later identified as the defendant, quoted a media report which referred to an estimate of the cost of the Stratfor Hack: "'the cost of the breach is 200 million' re: stratfor."

The January 11, 2012 IRC Chat

34. I have reviewed a copy of a chat that occurred on or about January 11, 2012 over the #lulzxmas IRC channel between an individual using the alias "sup_g," later identified as the defendant, CW-1, and CC-3, during which the following exchange took place:

<CW-1> sup_g: wanna release that list of 92% cracked stratfor hashes?
<@sup_g> hrm
<@sup_g> your call..
<@sup_g> i'd err on the side of no, so that way we can more fully exploit
<@sup_g> but then again we got even more targets to work on now

<@sup_g> so
<CC-3> what about release it couple of days before mails go online
<@sup_g> which btw I started unpacking on [CW-1's] new server
<@sup_g> and is copying over to new server
<@sup_g> as we speak

In the foregoing excerpt, CW-1 asked the defendant whether he wanted to release the list of cracked Stratfor "hashes" (encrypted passwords) for the email accounts that the defendant and his co-conspirators had stolen from Stratfor's servers, and the defendant suggested that they should wait in order to fully exploit that stolen data. The defendant also reported that he was in the process of "unpacking" or "copying over" the stolen Stratfor database onto CW-1's "new server," i.e., the New York Server that CW-1, at the FBI's direction, made available to the defendant and his co-conspirators.

C. Identification of the Defendant as JEREMY HAMMOND

1. Personal Information Provided by the Defendant (Using Aliases) Linking Him to JEREMY HAMMOND

35. In the course of communications with CW-1 both before and after CW-1's arrest, the defendant, using a number of different aliases, provided various pieces of personal information to the CW-1 in chats. Based on a review of this information and subsequent investigation, there is probable cause to believe that an individual named JEREMY HAMMOND, of Chicago, Illinois, was the person using the aliases "Anarchaos," "sup_g," "burn," "yohoho," "POW," "tylerknowsthis," and "crediblethreat," in the communications described above, based in part on the following:

a. On or about August 29, 2011, at approximately 8:37 a.m., in a chat on an open IRC channel, an individual using the alias "burn," later identified as the defendant, said "some comrades of mine were arrested in st louis a few weeks ago . . . for midwestrising tar sands work." I know based on my investigation that "Midwest Rising" refers to a protest in St. Louis, Missouri, on August 15, 2011, in which 15 people were arrested. I have also learned that Chicago FBI agents have confirmed that Midwest Rising was attended by, among others, HAMMOND's twin brother and that an associate of HAMMOND (the "Associate") was one of the leaders of this protest. St. Louis police reports do not indicate, however, that either individual was among those arrested.

b. Before CW-1 was arrested, a person using the alias

"Anarchaos," later identified as the defendant, communicated to CW-1 that he had been arrested in 2004 during the Republican National Convention (RNC) in New York City. After CW-1 was arrested, in a chat via Jabber on or about June 10, 2011, at approximately 10:12 p.m., an individual using the alias "yohoho," later identified as the defendant, told CW-1: "I haven't been there [referring to New York City] since the RNC." FBI obtained from New York City authorities a list of all individuals who had been arrested or detained at the 2004 Republic National Convention. This information indicated that JEREMY HAMMOND, the defendant, was one of the individuals detained at the RNC in New York in 2004, although there is no record of his arrest. An FBI database check confirmed that an FBI agent interviewed HAMMOND in New York City at the time of the RNC.

c. In a number of chats with CW-1, the person using the aliases "sup_g" and "burn," later identified as the defendant, discussed having spent time in prison, including federal prison. In one chat, for example, on or about August 15, 2011, at approximately 7:21 p.m., an individual using the alias "burn," said: "I did time at a USP." In a chat on or about August 29, 2011, at approximately 3:39 a.m., an individual using the alias "burn," said to another individual: "bro I did prison time, how did you magically get off your federal case?" In another chat, an individual using the alias "sup_g", on or about December 6, 2011, at approximately 22:54, referred to "a federal USP" and stated "United States Penitentiary general refers to a maximum security federal prison in the US . . . USP = max." Based on my involvement in this investigation, I believe that the individual using the aliases "burn" and "sup_g" was referring to time that the individual had spent in a federal prison. In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

(i) Based on federal criminal records, HAMMOND was arrested on a number of occasions, including a federal arrest in March 2005 by the FBI in Chicago ("HAMMOND's 2005 Case"). HAMMOND was convicted upon a plea of guilty to computer intrusion in violation of 18 U.S.C. § 1030, in connection with his involvement in hacking into a politically conservative website and stealing its computer database including credit card information. In December 2006, he was sentenced to 24 months in federal custody to be followed by 3 years supervised release.

(ii) During the course of the investigation which led to HAMMOND's March 2005 arrest, the FBI learned from another source that HAMMOND had discussed with others that he intended to use the

stolen credit cards to make donations to liberal organizations, although he did not ultimately do so. HAMMOND himself stated in an interview with the FBI that he intended to use hacking to fight for social justice.

d. In a chat with CW-1 on or about July 21, 2011, an individual using the alias "Anarchaos," later identified as the defendant, told CW-1 that he had been "arrested for weed and did two weeks in county jail." Later in that same chat that individual said: "Don't tell anybody cause it could compromise my identity but I am on probation . . . I've done time before though it's all cool." In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

(i) According to published reports, HAMMOND was sentenced to 18 months' probation in November 2010 for involvement in a violent protest against the Olympics coming to Chicago. Although I have not seen public records showing HAMMOND was arrested for marijuana possession in July 2011, a criminal history check does show that he had marijuana arrests in December 2010, while he was on probation, and November 2004.

e. An individual using the alias "sup_g," later identified as the defendant, told CW-1 in chats that he was involved in and sympathetic with militant left-leaning activities and anarchist groups. For example, in a chat on or about January 25, 2012, at approximately 10:05 p.m., an individual using the alias "sup_g," described himself as "an anarchist communist." He also discussed his support for an anarchist movement. In prior chats, before CW-1 was arrested, according to CW-1, an individual using the alias "Anarchaos," later identified as the defendant told CW-1 about sympathy with and involvement in militant anti-racist groups. In the course of my investigation, I have learned the following about JEREMY HAMMOND, the defendant:

(i) I have learned from my conversations with Chicago law enforcement agents involved in JEREMY HAMMOND's 2005 Case, as well as a review of related records, including a report prepared by U.S. Probation, that one of the conditions of HAMMOND's federal supervised release included prohibition from involvement or contact with the Chicago Anarchist Network or related civil disobedience organizations.

(ii) According to public reports, HAMMOND and the Associate (described above) were arrested together in a protest

against the Olympics in Chicago in 2010 in which they were alleged to have thrown a banner into a flame. HAMMOND was sentenced to 18 months' probation in November 2010 for the anti-Olympics protest.

(iii) According to a U.S. Probation report, HAMMOND was arrested in November 2009 for violently protesting a speech by a Holocaust denier.

(iv) The FBI in Chicago obtained information in the course of a separate investigation that HAMMOND may have been involved in hacks into the website of a white supremacist organization. According to that investigation, various IP addresses used to access the reported hacked accounts were connected to HAMMOND.

(v) During a routine Cook County probation check of HAMMOND's residence - the location described as the CHICAGO RESIDENCE below - flyers were found for an organization called the South-Side Chicago Anti-Racist Action (SSCARA) promoting militant confrontation with local white supremacists.

f. In a chat on or about July 31, 2011, at approximately 3:30 a.m., an individual using the alias "POW," later identified as the defendant, stated that "dumpster diving is all good i'm a freegan goddess." I know based on my investigation that "freegans" are individuals who practice eating and reclaiming food that has been discarded as part of an anti-consumerist movement. According to Chicago law enforcement authorities whom I have spoken to who have conducted surveillance of JEREMY HAMMOND, the defendant, in the course of their investigations of HAMMOND since 2005, HAMMOND is a "freegan." In conducting surveillance, agents have seen HAMMOND going into dumpsters to get food.

2. Physical and Electronic Surveillance of JEREMY HAMMOND

36. FBI agents in Chicago provided an address for JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, in Chicago (the "CHICAGO RESIDENCE"). Beginning on or about February 28, 2012, law enforcement agents began conducting continuous physical surveillance of the CHICAGO RESIDENCE. The CHICAGO RESIDENCE is a two-apartment house on a residential block. HAMMOND was observed leaving the location on or about February 29, 2012, and returning to it subsequently, and continuing to stay and leave in a manner indicating that he resided there as set forth below. HAMMOND only used the side entrance to the

building. Based on information from Chicago agents, the front entrance of the building accesses a front apartment, while the side and rear entrances access a rear apartment, which is completely partitioned from the front apartment.

37. During the course of the physical surveillance, FBI agents detected public signals broadcast from a wireless router (the "ROUTER") which, based on measurements of signal strength and the use of directional antennas, they determined was located inside and towards the rear of the CHICAGO RESIDENCE. Based on the investigation, including information provided by JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, to CW-1, the defendant has in the past used wi-fi, that is, a wireless connection, to access the Internet. Through other public signals, agents were able to identify the "MAC addresses" assigned to computers that were connecting to that ROUTER. (As explained above, a MAC address is a unique identifier often assigned by manufacturers to devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

38. Law enforcement agents obtained a court order authorizing the FBI to use a pen register and trap and trace device (the "Pen/Trap") to collect dialing, routing, addressing and signaling information for all electronic communications to or from the ROUTER at the CHICAGO RESIDENCE. The wireless router monitoring device captures and records non-content dialing, routing, addressing and signaling information for all electronic communications to or from the ROUTER pursuant to the Pen/Trap Order. The transmitting device then transmits that data over the air to FBI agents. The Pen/Trap was installed on or about March 1, 2012.

39. Based on information obtained from the Pen/Trap, law enforcement agents have learned the following, in substance and in part, about electronic communications emanating from the CHICAGO RESIDENCE:

a. The Pen/Trap data indicated that there were multiple MAC addresses being used at the CHICAGO RESIDENCE. These MAC addresses were connecting to various IP addresses, including the IP addresses identified as belonging to Facebook, Twitter, and Google. The Apple MAC Address in particular was also connecting to known TOR network IP addresses. As explained above, the TOR network is a system designed to enable users to access the Internet anonymously. Although the system permits the masking of IP addresses, it is possible to identify which specific IP addresses are linked to the TOR network.

b. An FBI TOR network expert analyzed the data from the Pen/Trap and was able to determine that a significant portion of the traffic from the CHICAGO RESIDENCE to the Internet was TOR-related traffic. The Apple MAC Address was the only MAC address at the CHICAGO RESIDENCE that was connecting to known TOR network IP addresses. The defendant, using the alias "yohoho," has discussed with CW-1 that he used the TOR network. For example in a chat over a jabber service on or about February 2, 2012, at approximately 5:22 a.m., "yohoho" said that he could not play youtube videos because "it won't play over tor." On February 6, 2012, at approximately 4:31 p.m., "yohoho" complained that "tor's always up and down."

40. As noted above, physical surveillance has continued at the CHICAGO RESIDENCE since on or about February 28, 2012. The below analysis compares the following information from between February 29, 2012, when physical surveillance first located JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, through the morning of March 5, 2012: (i) the times at which physical surveillance in Chicago indicated that HAMMOND had entered, was inside, or had left, the CHICAGO RESIDENCE; (ii) the data from the Pen/Trap indicating Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE; and (iii) information obtained from CW-1, in Manhattan, about online communications between CW-1 and the defendant. Based on this analysis, as set forth below, Internet activity by the Apple MAC Address and TOR network activity from the CHICAGO RESIDENCE occurred during the time periods that HAMMOND is present inside the CHICAGO RESIDENCE, as confirmed by physical surveillance, and ceased, or at least continued but diminished, after HAMMOND was seen leaving the CHICAGO RESIDENCE. Similarly, information obtained from CW-1 about online activity by the defendant corresponded to the time periods that HAMMOND was confirmed to be inside the CHICAGO RESIDENCE as set forth below.

a. For example, on February 29, 2012 at approximately 2:45

p.m. Central Standard Time (CST), HAMMOND was seen leaving the CHICAGO RESIDENCE. While HAMMOND was outside of the residence and offline, CW-1, who was in New York, was also offline, so CW-1 was not in communication with the defendant. HAMMOND returned to the residence at approximately 3:40 p.m. CST. (As noted above, the Pen/Trap was installed on March 1, 2012.)

b. On March 1, 2012, at approximately 5:03 p.m. CST, HAMMOND was seen leaving the CHICAGO RESIDENCE. Almost immediately after, CW-1 (in New York) contacted me to report that the defendant was offline. Pen/Trap data also reflected that TOR network activity and Internet activity from the CHICAGO RESIDENCE stopped at approximately the same time.

c. Later, also on March 1, 2012, at approximately 6:23 p.m. CST, HAMMOND was observed returning to the CHICAGO RESIDENCE. TOR network traffic resumed from the CHICAGO RESIDENCE approximately a minute or so later. Moreover, CW-1 reported to me that the defendant, using the online alias "yohoho," was back online at approximately the same time as physical surveillance in Chicago showed HAMMOND had returned to the CHICAGO RESIDENCE. New York FBI, through a program that remotely monitors the Internet activity of the buddy list on CW-1's jabber program, including when a "buddy" signs on and off, corroborated CW-1's report that the defendant, using "yohoho," was back online. Pen/Trap data reflected extensive TOR-related activity through the night.

d. On March 2, 2012, at approximately 1:52 p.m. CST, HAMMOND was observed leaving the CHICAGO RESIDENCE by agents conducting physical surveillance. After he left, diminished TOR and Internet activity was detected from the Pen/Trap data in comparison to when he was at the residence and actively on the Internet earlier that day. At approximately 2:04 p.m. CST, HAMMOND returned. Based on my training and experience, I believe that both the TOR and Internet activity did not cease because HAMMOND had only left for a brief period so had kept his Internet connections open, but it diminished because he was not actively using the Internet connections during that time.

e. On March 3, 2012, at approximately 2:17 p.m. CST, HAMMOND was observed leaving the CHICAGO RESIDENCE, and he returned at approximately 3:26 p.m. CST. During the time that he was not at the residence, no TOR activity or Internet activity was detected at the residence.

f. On March 3, 2012, at approximately 6:20 p.m. CST, I

confirmed with agents conducting surveillance that HAMMOND had still not left the CHICAGO RESIDENCE. Pen/Trap data indicated that the Apple computer was online and TOR activity was detected at the residence. At that time, I confirmed through remotely accessing CW-1's jabber program buddy list that "yohoho" was online.

g. On March 3, 2012, at approximately 8:07 p.m. CST, agents observed HAMMOND leaving the CHICAGO RESIDENCE. According to the Pen/Trap data, the Apple MAC address Internet activity stopped at approximately 7:40 p.m. CST. At approximately 8:13 p.m. CST, CW-1, in New York, reported to me that "yohoho" was offline.

h. On March 4, 2012, at approximately 3:18 a.m. CST, agents observed HAMMOND returning to the CHICAGO RESIDENCE. According to the Pen/Trap data, at approximately 3:37 a.m. CST, the Apple computer at that location was back online, and both Internet and TOR activity started again. At approximately the same time, CW-1 contacted me in New York and reported that "yohoho" was back online.

i. Later on March 4, 2012, at approximately 4:02 p.m., while HAMMOND was still at the residence according to surveillance, Pen/Trap data indicated that the Apple Mac Address was active online, and confirmed TOR activity. At that time, CW-1, in New York, reported to me that "yohoho" was chatting online. Surveillance did not see HAMMOND leave the residence until approximately 10:15 p.m. CST. He was observed returning to the residence at approximately 10:35 p.m. CST. During this period that HAMMOND was not at the residence, diminished TOR and Internet activity was detected from there. As of the morning of March 5, 2012, he had not left the residence again. As

of the morning of March 5, 2012, CW-1's last online contact with the defendant was at approximately 7:00 p.m. CST on March 4, 2012.

WHEREFORE, deponent prays that a warrant be issued for the arrest of JEREMY HAMMOND, a/k/a "Anarchaos," a/k/a "sup_g," a/k/a "burn," a/k/a "yohoho," a/k/a "POW," a/k/a "tylerknowsthis," a/k/a "crediblethreat," the defendant, and that he be imprisoned or bailed, as the case may be.

MILAN PATEL
Special Agent
Federal Bureau of Investigation

Sworn to before me this
5th day of March 2012

HON. RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK