

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -x

UNITED STATES OF AMERICA :

SEALED
INDICTMENT

- v. - :

12 Cr. ()

RYAN ACKROYD, :

a/k/a "kayla," :

a/k/a "lol," :

a/k/a "lolspoon," :

JAKE DAVIS, :

a/k/a "topiary," :

a/k/a "atopiary" :

DARREN MARTYN, :

a/k/a "pwnsauce," :

a/k/a "raepsauce," :

a/k/a "networkkitten," and :

DONNCHA O'CEARRBHAIL, :

a/k/a "palladium," :

Defendants. :

- - - - -x

COUNT ONE

(CONSPIRACY TO COMMIT COMPUTER HACKING - INTERNET FEDS)

The Grand Jury charges:

BACKGROUND ON ANONYMOUS AND INTERNET FEDS

1. Since at least in or about 2008, up through and including on or about the date of this Indictment, "Anonymous" has been a loose confederation of computer hackers and others sharing, among other things, common interests, common slogans, and common identifying symbols. During that time period, certain members of Anonymous have 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 throughout the world.

2. Between in or about December 2010 and in or about May 2011, one group of individuals affiliated with Anonymous who engaged in such criminal conduct was composed of elite computer hackers who collectively referred to themselves as "Internet Feds." At various times relevant to this Indictment, members of Internet Feds carried out a series of cyber attacks against the websites and computer systems of certain business and government entities in the United States and around the world, including, among others, the following businesses and organizations:

a. Fine Gael, a political party in Ireland, which maintained the website "www.finegael2011.com;"

b. HBGary, Inc. and its affiliate, HBGary Federal, LLC (collectively referred to herein as "HBGary"), computer security firms based in the United States which provided computer security software and services, among other things, to their clients, and which maintained the website "www.HBGaryFederal.com;" and

c. Fox Broadcasting Company ("Fox"), a commercial broadcast television network in the United States, which maintained the website "www.fox.com."

3. These cyber attacks involved, among other things: (1) breaking into computer systems, deleting data, and stealing

confidential information, including encrypted and unencrypted sensitive personal information for thousands of individual victims; (2) de-encrypting confidential information stolen from victims' computer systems, including encrypted passwords; (3) publicly disclosing that stolen confidential information on the Internet by dumping it on certain websites; (4) hijacking victims' email and Twitter accounts; (5) defacing victims' Internet websites; and/or (6) "doxing," that is, publicly disclosing online a victim's personal identifying information, such as the victim's name, address, Social Security number, email account, and telephone number, with the object of, among other things, intimidating the victim and subjecting the victim to harassment.

4. At various times relevant to this Indictment, and as part of Anonymous, members of Internet Feds sought to publicize their Internet assaults and intimidate their victims by, among other things: (1) posting messages online in which they discussed their attacks and threatened additional attacks; (2) using particular logos and slogans when, for example, they posted messages online and defaced websites; and (3) discussing their attacks with members of the press.

5. At various times relevant to this Indictment, and much like other members of Anonymous, members of Internet Feds, despite their efforts to publicize their illegal conduct,

typically attempted to hide their true identities by, for example, using aliases when they communicated with the public or with each other.

6. At various times relevant to this Indictment, members of Internet Feds, much like other members of Anonymous, communicated using, among other means, Internet Relay Chat ("IRC") channels -- that is, real-time, text-based online forums. Some of these channels were open to the public. Others, particularly channels in which members of Anonymous and members of Internet Feds planned and organized criminal activity, including cyber attacks, were not. Instead, those channels were generally password-restricted and available by invitation only, usually to trusted individuals who had proven themselves through past criminal hacking. Specifically, members of Internet Feds and their co-conspirators planned and coordinated their cyber attacks using password-restricted, invitation-only IRC channels such as "#InternetFeds," "#Hackers," and "#hq," among others.

7. At various times relevant to this Indictment, the members of Internet Feds included, among others, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, as well as

other individuals, including, but not limited to, individuals who used the online aliases "SABU," "TFLOW," and "AVUNIT."

THE DEFENDANTS

8. At all times relevant to this Indictment, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," and JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendants, were computer hackers who resided in the United Kingdom.

9. The role of RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, in each of the conspiracies charged in this Indictment included, among other things, identifying and exploiting vulnerabilities in victims' computer systems for the purpose of gaining unauthorized access to those systems.

10. The role of JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, in each of the conspiracies charged in this Indictment included, among other things, acting as a spokesman for the groups charged in Counts One and Two of this Indictment, for example by engaging in interviews with the media and publicizing those groups' hacking activities; and organizing and storing confidential information stolen in connection with the computer hacking described in Counts One and Two of this Indictment.

11. At all times relevant to this Indictment, DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a

"networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, were computer hackers who resided in Ireland.

CYBER ATTACKS BY INTERNET FEDS

12. From in or about December 2010, up to and including in or about May 2011, members of Internet Feds, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, and their co-conspirators, including, among others, SABU, TFLOW and AVUNIT, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others:

Hack of Fine Gael

a. In or about January 2011, MARTYN and O'CEARRBHAIL participated in a cyber attack on Fine Gael's website, www.finegael2011.com. Among other things, MARTYN and O'CEARRBHAIL accessed without authorization computer servers in Arizona used by Fine Gael to maintain its website, and uploaded code that defaced the website.

Hack of HBGary

b. In or about February 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and

AVUNIT, participated in a cyber attack on the website and computer systems of HBGary.

c. Among other things, ACKROYD, DAVIS, MARTYN, and their co-conspirators accessed without authorization computer servers used by HBGary in California and Colorado and stole confidential information from those servers, including approximately 60,000 emails from email accounts used by HBGary employees and a senior executive of HBGary Federal, LLC (the "HBGary Federal Executive"), which ACKROYD, DAVIS, and MARTYN, and their co-conspirators publicly disclosed via the www.thepiratebay.org website (an anonymous file sharing website that permits users to post stolen content), among other means.

d. ACKROYD, DAVIS, MARTYN, and their co-conspirators used information gained from those stolen emails to access, without authorization, and steal the contents of an email account belonging to a senior executive of HBGary, Inc. (the "HBGary, Inc. Executive"); gain unauthorized access to the servers for the website www.rootkit.com, an online forum on computer hacking maintained by the HBGary, Inc. Executive, and steal confidential data, including usernames and encrypted passwords for approximately 80,000 user accounts; access without authorization and deface the Twitter account of the HBGary Federal Executive; and dox the HBGary Federal Executive by, among other things, posting his Social Security number and home

address on his Twitter account without his authorization or approval.

e. ACKROYD, DAVIS, MARTYN, and their co-conspirators de-encrypted tens of thousands of the encrypted www.rootkit.com users' passwords that they had stolen, and publicly disclosed those de-encrypted passwords, the rootkit.com usernames they had stolen, and the contents of the email account belonging to the HBGary, Inc. Executive, by dumping them on certain Internet websites.

Hack of Fox

f. In or about April 2011, ACKROYD, DAVIS, MARTYN, O'CEARRBHAIL, and their co-conspirators, including SABU, TFLOW and AVUNIT, participated in a cyber attack on the website and computer systems of Fox.

g. Among other things, ACKROYD, DAVIS, MARTYN, O'CEARRBHAIL, and their co-conspirators accessed without authorization computer servers in California used by Fox and stole and publicly disclosed confidential information, including a database of the names, dates of birth, telephone numbers, email addresses, and residences, among other information, for more than 70,000 potential contestants on "X-Factor," a Fox television show.

STATUTORY ALLEGATIONS

13. From at least in or about December 2010, up to and including in or about May 2011, in the Southern District of New York and elsewhere, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, 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).

14. It was a part and an object of the conspiracy that RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, 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

15. 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:

a. On or about January 9, 2011, DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendant, sent an electronic communication to DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendant, containing computer code to be used to deface the www.finegael2011.com website.

b. In or about February 2011, SABU used a computer located in New York, New York to access without authorization computer servers used by HBGary and steal tens of thousands of emails belonging to employees of HBGary and the HBGary Federal Executive.

c. In or about February 2011, JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, accessed without authorization the Twitter account of the HBGary Federal Executive and posted one or more fraudulent tweets.

d. In or about February 2011, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, accessed without authorization an email account belonging to the HBGary, Inc. Executive and sent one or more fraudulent emails from that account to an administrator for the www.rootkit.com website requesting administrative access to that website.

e. On or about February 7, 2011, TFLOW uploaded links to tens of thousands of stolen emails belonging to employees of HBGary and the HBGary Federal Executive as well as a copy of certain text that had been used to deface the www.HBGaryFederal.com website, to an account on the website www.thepiratebay.org in the name "HBGary leaked emails."

f. On or about February 8, 2011, DAVIS, using the IRC channel #hq, discussed how Twitter had locked the Twitter account of the HBGary Federal Executive and stated, "That works in our favour. His Twitter still has all our tweets. Including his SSN."

g. On or about February 9, 2011, ACKROYD, using the IRC channel #hq, asked TFLOW whether he had received a copy of emails belonging to the HBGary, Inc. Executive, to which TFLOW responded affirmatively and stated that he would add them to an "online viewer."

h. On or about February 12, 2011, SABU, using the IRC channel #hq, stated that he had deleted data on a server used by HBGary.

i. On or about February 13, 2011, DAVIS, using the IRC channel #hq, told AVUNIT "I'm happy to talk to press on IRC/Skype, have done [so] for months," and told TFLOW that he had "talked to maybe 150 journalists."

j. In or about May 2011, SABU used a computer in New York, New York to access without authorization a computer server used by Fox and download a database containing personal information relating to potential contestants on the X-Factor television show.

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

COUNT TWO

(CONSPIRACY TO COMMIT COMPUTER HACKING - LULZSEC)

The Grand Jury further charges:

16. The allegations in paragraphs 1 through 12 and 15 this Indictment are repeated and realleged as though fully set forth herein.

BACKGROUND ON LULZSEC

17. In or about May 2011, following the publicity that they had generated as a result of their hacking of Fine Gael and HBGary, among other victims, members of Internet Feds, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a

"lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, as well as SABU, TFLOW, and AVUNIT, formed and became the principal members of a new hacking group, "Lulz Security" or "LulzSec."

18. Like Internet Feds, LulzSec undertook a campaign of malicious cyber assaults on the websites and computer systems of various business and government entities in the United States and throughout the world. Although the members of LulzSec and their co-conspirators claimed to have engaged in these attacks for humorous purposes ("lulz" is Internet slang which can be interpreted as "laughs," "humor," or "amusement"), LulzSec's criminal acts included, among other things, the theft of confidential information, including sensitive personal information for thousands of individuals, from their victims' computer systems; the public disclosure of that confidential information on the Internet; the defacement of Internet websites; and overwhelming victims' computers with bogus requests for information (known as "denial of service" or "DoS" attacks).

19. Also like Internet Feds, LulzSec sought to gain notoriety for their hacks by varied and repeated efforts to broadcast their acts of online destruction and criminality. As a means of publicizing their cyber assaults, members of LulzSec

and their co-conspirators maintained a website, "www.LulzSecurity.com;" an account in the name "LulzSec" at www.thepiratebay.org; and a Twitter account, "@LulzSec;" all of which they used to, among other things, announce their hacks and issue written "press releases" about them; mock their victims; solicit donations; and publicly disclose confidential information they had stolen through their cyber attacks.

20. Similar to Internet Feds, as a means of publicizing their online assaults, as well as intimidating their victims, members of LulzSec and their co-conspirators used particular logos and slogans in, for example, their "press releases," their website defacements, and on the www.LulzSecurity.com website and the @LulzSec Twitter account.

21. Despite going to great lengths to seek attention for their illegal conduct, the members of LulzSec and their co-conspirators - like Internet Feds - attempted to hide their true identities. Among other things, they referred to themselves by aliases, attempted to promote false personas, and used technical means, including proxy servers, in an effort to conceal themselves online.

22. At various times relevant to this Indictment, members of LulzSec, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a

"raepsauce," a/k/a "networkkitten," the defendants, as well as SABU, TFLOW, and AVUNIT, and their co-conspirators, launched cyber attacks on the websites and computer systems of the following victims, among others:

a. Sony Pictures Entertainment ("Sony Pictures"), a division of Sony, a global electronics and media company, which produced and distributed television shows and movies and maintained the website "www.sonypictures.com;"

b. The Public Broadcasting Service ("PBS"), a non-profit public television broadcasting service in the United States, which maintained the website "www.pbs.org;"

c. The Atlanta, Georgia chapter of the Infragard Members Alliance ("Infragard-Atlanta"), an information sharing partnership between the Federal Bureau of Investigation ("FBI") and private industry concerned with protecting critical infrastructure in the United States, which maintained the website "www.infraguardatlanta.org;" and

d. Bethesda Softworks, a video game company based in Maryland, which owned the videogame "Brink" and maintained the website "www.brinkthegame.com."

23. At various times relevant to this Indictment, and in addition to identifying and exploiting vulnerabilities in their victims' computer systems on their own, the members of LulzSec also received from other computer hackers information

regarding vulnerabilities in the computer systems of a variety of business and government entities. LulzSec members used this information to launch cyber attacks on those entities or stored it in anticipation of future attacks.

24. At various times relevant to this Indictment, members of LulzSec and their co-conspirators communicated with each other and planned and coordinated their cyber attacks using password-restricted, invitation-only IRC channels, including, among others, "#upperdeck" and "#hq".

CYBER ATTACKS BY LULZSEC

25. From in or about May 2011, up to and including at least in or about June 2011, members of LulzSec, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, and their co-conspirators, including, among others, SABU, TFLOW, and AVUNIT, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others:

Hack of PBS

a. In or about May 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and AVUNIT, in retaliation for what they perceived to be unfavorable news coverage in an episode of the PBS news program Frontline,

undertook a cyber attack on the website and computer systems of PBS.

b. ACKROYD, DAVIS, MARTYN, and their co-conspirators, accessed without authorization computer servers in Virginia used by PBS, stole confidential information from those servers, including, among other things, databases containing names, email addresses, usernames and passwords of more than approximately 2,000 PBS employees and other individuals and entities associated with PBS; publicly disclosed that information on certain websites, including the www.LulzSecurity.com website; and defaced the PBS website, including by inserting a bogus news article.

Hack of Sony Pictures

c. In or about May 2011, ACKROYD, DAVIS, and their co-conspirators, including SABU, TFLOW and AVUNIT, participated in a cyber attack on computer systems used by Sony Pictures. This attack included accessing without authorization Sony Pictures' computer servers in California, and stealing and publicly disclosing on certain websites, including the www.LulzSecurity.com website, confidential information for at least approximately 100,000 users of the www.sonypictures.com website, including the users' passwords, email addresses, home addresses, and dates of birth.

Hack of Infragard-Atlanta

d. In or about June 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and AVUNIT, launched cyber attacks on the website and computer systems of Infragard-Atlanta. These attacks included stealing the login credentials, encrypted passwords, and other confidential information for approximately 180 users of the Infragard-Atlanta website, www.atlantainfraguard.org; defacing that website; de-encrypting the stolen passwords; and publicly disclosing the stolen confidential user information, including the de-encrypted passwords, on certain websites, including the www.LulzSecurity.com website.

Hack of Bethesda Softworks

e. In or about June 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including TFLOW, participated in a cyber attack on the computer systems used by Bethesda Softworks, stealing confidential information, including authorization keys, as well as usernames, passwords, and email accounts for approximately 200,000 users of Bethesda Softworks' website, "www.brinkthegame.com." ACKROYD, DAVIS, MARTIN, and their co-conspirators, publicly disclosed some of that stolen data on certain websites, including the www.LulzSecurity.com website.

STATUTORY ALLEGATIONS

26. From at least in or about May 2011, up to and including at least in or about June 2011, in the Southern District of New York and elsewhere, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, 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).

27. It was a part and an object of the conspiracy that RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, 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, and which would and did cause damage

affecting a computer used by and for an entity of the United States Government, to wit the FBI, in furtherance of the administration of justice, national defense and national security, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I) and (V).

OVERT ACTS

28. 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:

a. On or about May 6, 2011, JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, established a Twitter account in the name "@LulzSec."

b. In or about May 2011, SABU used a computer located in New York, New York, to gain unauthorized access to computer systems used by PBS and install one or more surreptitious means ("backdoors") by which SABU and others could secretly re-access those systems without authorization.

c. In or about May 2011, DAVIS wrote a bogus news article, which was used to deface the www.pbs.org website.

d. In or about May 2011, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, and SABU accessed without authorization computer servers used by PBS and downloaded confidential information.

e. In or about May 2011, SABU used a computer located in New York, New York, to gain unauthorized access to servers used by Sony Pictures.

f. In or about June 2011, SABU used a computer located in New York, New York to gain unauthorized access to, and install one or more backdoors in, computer systems used by Infragard-Atlanta.

g. In or about June 2011, ACKROYD accessed without authorization servers used by Infraguard-Atlanta and downloaded confidential information.

h. In or about June 2011, a co-conspirator not named as a defendant herein provided information concerning a vulnerability in computer systems used by Bethesda Softworks to ACKROYD and other members of LulzSec.

i. On or about June 12, 2011, ACKROYD used the foregoing vulnerability to gain unauthorized access to computer systems used by Bethesda Softworks, install one or more backdoors, which he provided to other members of LulzSec, and download confidential information.

j. In or about June 2011, DAVIS used a backdoor provided by ACKROYD to access without authorization computer systems used by Bethesda Softworks and download confidential information, which DAVIS then organized.

k. On or about June 12, 2011, MARTYN posted the following message in the IRC channel #upperdeck: "Ok, who are we raping, brink?" to which ACKROYD responded affirmatively.

l. On or about June 12, 2011, DAVIS posted the following message in the IRC channel #upperdeck: "so everyone knows, Brink leakage is 100% organized on my end; just waiting on the 200K DB."

m. On or about June 21, 2011, a co-conspirator not named as a defendant herein provided SABU with confidential files relating to a computer network at the "madison ave hq in nyc" of Sony Music Entertainment, a division of Sony.

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

FORFEITURE ALLEGATION AS TO COUNTS ONE AND TWO

29. As a result of committing one or both of the offenses alleged in Counts One and Two of this Indictment, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, shall forfeit to the United States, pursuant to 18 U.S.C.

§ 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of one or both of the said offenses, including but not limited to a sum of

money representing the amount of proceeds obtained as a result of one or both of the said offenses.

SUBSTITUTE ASSETS PROVISION

30. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value;
or

e. has been commingled with other property which cannot be subdivided without difficulty;

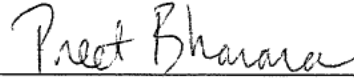
it is the intent of the United States, pursuant to 18 U.S.C.

§ 982(b)(1) and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982(a)(2)(B) and (b)(1), and Title 21, United States Code, Section 853(p).)



FOREPERSON



PREET BHARARA
United States Attorney

ORIGINAL

Approved: Thomas Brown/Rosemary Nidiry
THOMAS BROWN/ROSEMARY NIDIRY
Assistant United States Attorneys

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

- - - - - x

UNITED STATES OF AMERICA :

SEALED COMPLAINT

- v. - :

Violation of 18 U.S.C. §§ 1029,
1030 and 2.

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,"

COUNTY OF OFFENSE:
New York

Defendant.

- - - - - x

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 chats 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 CVV¹ 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 gigabytes² 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 "antisecc 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 "antisecc teaser 12/26" was posted to a file sharing website. Like the document titled "antisecc 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 "antisecc 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," "#antisecc," "#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 antisecc [an IRC channel]," indicating that he used the alias "crediblethreat" when chatting on the antisecc 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://ibhg35kgdvn7jvw.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 servers 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 #lulzxmash 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 #antisecc 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 shopping
* * *
<@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 #lulzxcmas 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> HAHAAHAHA
<@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 #antisecc 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 htms 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 #lulzmas 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 #antisecc 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 lulzmas
<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 #antisecc 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 #lulzmas 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

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - -x

UNITED STATES OF AMERICA : INFORMATION

- v. - : 11 Cr.

HECTOR XAVIER MONSEGUR, :

a/k/a "Sabu," :

a/k/a "Xavier DeLeon," :

a/k/a "Leon," :

Defendant.

- - - - -x

11 Cr. 11 Cr. 11 Cr.

COUNT ONE

(Conspiracy to Engage in Computer Hacking -- Anonymous)

The United States Attorney charges:

THE DEFENDANT

1. At all times relevant to this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, was an experienced computer hacker who resided in New York, New York. At various times relevant to this Information, MONSEGUR was an influential member of three hacker organizations -- Anonymous, Internet Feds, and Lulz Security (also known as "LulzSec") -- that were responsible for multiple cyber attacks on the computer systems of various businesses and governments in the United States and throughout the world.

2. At all times relevant to this Information, MONSEGUR's primary area of expertise and role in hacker

organizations was to act as a "rooter," that is, a computer hacker who identified vulnerabilities in the computer systems of potential victims to be exploited for the purpose of gaining unauthorized access to the systems. Upon discovering these vulnerabilities, MONSEGUR either passed information regarding them to other hackers, who sought to exploit them, or MONSEGUR exploited the vulnerabilities himself. MONSEGUR also provided infrastructure support to members of hacker organizations, that is, unauthorized access to computer servers and routers that others could use to launch cyber attacks on victims.

BACKGROUND ON ANONYMOUS

3. At all times relevant to this Information, "Anonymous" was a collective of computer hackers and other individuals located in the United States and elsewhere that undertook "operations" -- that is, coordinated efforts that included cyber attacks -- against individuals and entities that were perceived to be hostile to Anonymous and its members' interests. These attacks included, among other things, the theft and later dissemination of confidential information from computer systems and the defacement of Internet websites. These attacks also included attacks against websites, known as "denial of service" or "DoS" attacks, which involved the use of a large number of computers to bombard a victim's website with bogus

requests for information, causing the website to temporarily cease functioning.

4. At all times relevant to this Information, the members of Anonymous, through their cyber attacks, sought to support, among other causes, Wikileaks, an international non-profit organization that published otherwise unavailable documents from anonymous sources; and Julian Assange, who was the founder of Wikileaks.

THE DEFENDANT'S COMPUTER HACKING AS PART OF ANONYMOUS

5. From in or about December 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks as part of Anonymous, including the following, among others:

DoS Attacks on Visa, MasterCard and PayPal

a. In or about December 2010, MONSEGUR briefly participated in "Operation Payback," in which members of Anonymous launched DoS attacks against the websites of the credit card companies Visa and MasterCard and the online payment service PayPal, with the intent to disrupt the operation of those companies' websites. The members of Anonymous intended Operation Payback to serve as retaliation for the refusal of Visa, MasterCard, and PayPal to process donations to Wikileaks.

Hack and DoS Attack on Tunisian Government Computers

b. In or about January 2011, MONSEGUR participated in "Operation Tunisia," in which members of Anonymous launched cyber attacks against computer systems used by the government of Tunisia. Among other things, MONSEGUR hacked into and defaced the website of the Prime Minister of Tunisia. MONSEGUR and others also participated in a DoS attack against other websites used by the Tunisian government.

DoS Attack on Algerian Government Computers

c. In or about early 2011, MONSEGUR participated in "Operation Algeria," in which members of Anonymous launched cyber attacks against computer systems used by the government of the People's Democratic Republic of Algeria. Among other things, MONSEGUR participated in a DoS attack against websites belonging to the Algerian government.

Hack of Yemeni Government Computers

d. In or about early 2011, MONSEGUR participated in "Operation Yemen," in which members of Anonymous launched cyber attacks against computer systems used by the government of the Republic of Yemen. Among other things, MONSEGUR identified security weaknesses in these computer systems. MONSEGUR tested the security weaknesses by accessing without authorization Yemeni government computer systems and

downloading certain information. MONSEGUR shared the security weaknesses with other computer hackers in Anonymous.

Hack of Zimbabwean Government Computers

e. In or about early 2011, MONSEGUR participated in "Operation Zimbabwe," in which members of Anonymous launched cyber attacks against computer systems used by the government of Zimbabwe. Among other things, MONSEGUR identified security weaknesses in those computer systems. MONSEGUR tested the security weaknesses by accessing without authorization Zimbabwean government computer systems and downloading certain information. MONSEGUR shared the security weaknesses with other computer hackers in Anonymous and attempted to steal information from a Zimbabwean government email server.

STATUTORY ALLEGATIONS

6. From at least in or about December 2010, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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).

7. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

OVERT ACTS

8. In furtherance of the conspiracy and to effect the illegal object thereof, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. In or about December 2010, while using a computer located in New York, New York, MONSEGUR participated in a DoS attack that was being organized by the members of Anonymous against the computer systems of PayPal, MasterCard, and Visa.

b. In or about early 2011, while using a computer located in New York, New York, MONSEGUR participated in

DoS attacks against the computer systems used by the governments of Tunisia and Algeria.

c. In or about early 2011, while using a computer located in New York, New York, MONSEGUR attempted to obtain information, without authorization, from an e-mail server used by the government of Zimbabwe.

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

COUNT TWO

(Conspiracy to Engage in Computer Hacking -- Internet Feds)

The United States Attorney further charges:

9. The allegations in paragraphs 1 through 5 and 8 of this Information are repeated and realleged as though fully set forth herein.

BACKGROUND ON INTERNET FEDS

10. In or about December 2010, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, was invited by a co-conspirator not named as a defendant herein to participate in "Internet Feds," a group of elite computer hackers affiliated with Anonymous that undertook cyber attacks on the computer systems of various business and government entities in the United States and throughout the world. These attacks included, among other things, the theft of confidential information from victims' computer systems, the

defacement of victims' Internet websites, and DoS attacks. At various times relevant to this Information, members of Internet Feds, including MONSEGUR, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others: HBGary, Inc. and HBGary Federal, LLC (HBGary Federal, LLC is owned in part by HBGary, Inc.; both are collectively referred to herein as "HBGary"), a private cyber security firm; Fox Broadcasting Company ("Fox"), a commercial broadcast television network; and the Tribune Company, a media company which owns various television and radio stations and publishes the Chicago Tribune and the Los Angeles Times, among other newspapers. In addition, during the time period relevant to this Information, members of Internet Feds other than MONSEGUR launched computer attacks on computer servers used by ACS Law, a law firm in Australia and the Sony PlayStation Network, an online multiplayer gaming and digital media delivery service.

THE DEFENDANT'S COMPUTER HACKING AS PART OF INTERNET FEDS

11. From in or about December 2010, up to and including in or about March 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks and unauthorized intrusions as part of Internet Feds, including the following, among others:

Hack of HBGary

a. In or about early 2011, MONSEGUR participated in a cyber attack on the computer systems of HBGary. Among other things, MONSEGUR and his co-conspirators accessed without authorization computer servers belonging to HBGary in Sacramento, California and Colorado Springs, Colorado, and stole confidential information from those servers. In addition, MONSEGUR and his co-conspirators used information gained from this hack to, among other things, access without authorization and download emails from the email accounts of the CEO of HBGary and the owner of HBGary; access without authorization and steal confidential information from the servers for the website rootkit.com, an online forum on computer hacking maintained by the owner of HBGary; and access without authorization and deface the Twitter account of the CEO of HBGary.

Unauthorized Access to the Tribune Company's Computer Systems

b. In or about early 2011, MONSEGUR and his co-conspirators misappropriated login credentials to access the Tribune Company's computer systems without authorization.

Hack of Fox

c. In or about early 2011, MONSEGUR participated in a cyber attack on the computer systems of Fox. Among other things, MONSEGUR and his co-conspirators accessed

without authorization computer servers in Los Angeles, California, belonging to Fox and stole confidential information, including information relating to contestants on "X-Factor," a Fox television show.

Statutory Allegations

12. From at least in or about December 2010, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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).

13. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

Overt Acts

14. In furtherance of the conspiracy and to effect the illegal object thereof, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. In or about early 2011, while using a computer in New York, New York, MONSEGUR participated in a cyber attack on computer systems used by HBGary.

b. In our about early 2011, while using a computer in New York, New York, MONSEGUR participated in a cyber attack on computer systems used by Fox.

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

COUNT THREE

(Conspiracy to Engage in Computer Hacking -- LulzSec)

The United States Attorney further charges:

15. The allegations in paragraphs 1 through 5, 8, 10, 11 and 14 of this Information are repeated and realleged as though fully set forth herein.

BACKGROUND ON LULZSEC

16. From in or about May 2011, up to and including in or about June 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, formed "Lulz Security," or "LulzSec," with other elite hackers, including

individuals who used the online nicknames "Kayla," "Topiary," "Tflow," "Pwnsauce," and "AVUnit." "Lulz" is Internet slang which can be interpreted as "laughs," "humor," or "amusement." The members of LulzSec undertook cyber attacks on the computer systems of various business and government entities in the United States and throughout the world. These attacks included, among other things, the theft of confidential information from victims' computer systems, the defacement of victims' Internet websites, and attacks against victims' websites which rendered the websites temporarily unavailable to the public. In addition to attacking the computer systems of their victims, the members of LulzSec also received from other computer hackers information regarding vulnerabilities in the computer security systems of a variety of business and government entities. LulzSec members used this information to launch cyber attacks on those entities or stored it in anticipation of future attacks.

17. At various times relevant to this Information, members of LulzSec launched cyber attacks on the computers systems and websites of the following victims, among others:

a. Various divisions of Sony, a global electronics and media company, including Sony Pictures Entertainment ("Sony Pictures"), which produces and distributes television shows and movies; and Sony Music Entertainment ("Sony Music"), which produces and distributes audio recordings;

b. The Public Broadcasting Service ("PBS"), a non-profit public television broadcasting service in the United States;

c. Nintendo, a video game company based in Japan;

d. The Atlanta, Georgia chapter of the Infragard Members Alliance ("Infragard-Atlanta"), an information sharing partnership between the Federal Bureau of Investigation and private industry concerned with protecting critical infrastructure in the United States;

e. Unveillance, a cyber security firm headquartered in Delaware;

f. The United States Senate; and

g. Bethesda Softworks, a video game company based in Maryland.

THE DEFENDANT'S COMPUTER HACKING AS PART OF LULZSEC

18. From in or about May 2011, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, participated in several cyber attacks as part of LulzSec, including the following, among others:

Hack of PBS

a. In or about May 2011, MONSEGUR and other members of LulzSec, in retaliation for what they perceived to be

unfavorable news coverage of Wikileaks in an episode of the PBS news program Frontline, undertook a cyber attack on computer systems used by PBS. MONSEGUR and others accessed without authorization computer servers in Alexandria, Virginia used by PBS, stole confidential information from those servers, and defaced the website for the PBS news program The News Hour, including by inserting a bogus news article that the deceased rapper Tupac Shakur was alive and living in New Zealand.

Hack of Sony Pictures

b. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR participated in a cyber attack on computer systems used by Sony Pictures. This attack included accessing without authorization and stealing confidential information from Sony Pictures' computer servers in El Segundo, California.

Hack of Sony Music

c. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR received information from another individual on a security vulnerability in Sony Music's computer systems in Belgium, the Netherlands, and Russia. MONSEGUR used that vulnerability to steal information, including the release dates of music records, from computer servers in Belgium and the Netherlands used by Sony Music. MONSEGUR also passed to other members of LulzSec the

details of the security vulnerability in Sony Music's computer system in Russia.

Hacks of Infragard-Atlanta and Unveillance

d. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR and other members of LulzSec launched cyber attacks on computer systems used by Infragard-Atlanta and Unveillance. These attacks included the theft of login credentials, passwords, and other confidential information from Infragard-Atlanta and the defacement of Infragard-Atlanta's website. In addition, MONSEGUR and his co-conspirators used information gained from this hack to access without authorization, and to download, emails from the email accounts of the CEO of Unveillance.

Hack of the U.S. Senate

e. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR received from another hacker and shared with the members of LulzSec a security vulnerability in computer systems used by the United States Senate. MONSEGUR and other LulzSec members used that vulnerability to access without authorization those computer systems and to download confidential information.

Hack of Bethesda Softworks

f. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR and other members

of LulzSec participated in a cyber attack on the computer systems used by Bethesda Softworks, stealing confidential information, including usernames, passwords, and email accounts.

Statutory Allegations

19. From at least in or about May 2011, up to and including on or about June 7, 2011, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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).

20. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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, did intentionally cause damage without authorization, to a protected computer, and the loss caused by such behavior was at least \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

Overt Acts

21. In furtherance of the conspiracy and to effect the illegal object thereof, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. In or about May 2011, MONSEGUR, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by PBS that resulted in the theft of confidential information and the defacement of the website for the PBS news program The News Hour.

b. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by Sony Pictures that resulted in the theft of confidential information.

c. From in or about late May 2011, up to and including on or about June 7, 2011, MONSEGUR, while using a computer located in New York, New York, participated in a cyber attack on computer systems used by Infragard-Atlanta that resulted in the theft of confidential information from Infragard-Atlanta and the defacement of Infragard-Atlanta's website. In addition, MONSEGUR and his co-conspirators used information gained from this hack to access without

authorization, and to download, emails from the email accounts of the CEO of Unveillance.

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

COUNT FOUR

(Computer Hacking In Furtherance of Fraud)

The United States Attorney further charges:

22. In or about 2010, in the Southern District of New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willingly and knowingly, and with intent to defraud, accessed a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained a thing of value, to wit, MONSEGUR, using a computer located in New York, New York, accessed without authorization the computer systems of a company that sells automobile parts, and fraudulently caused four automobile motors with a value of approximately \$3,450 to be shipped to himself in New York, New York.

(Title 18, United States Code, Sections 1030(a)(4),
1030(c)(3)(A) and 2.)

COUNT FIVE

(Conspiracy to Commit Access Device Fraud)

The United States Attorney further charges:

23. From at least in or about 2010, up to and including on or about June 7, 2011, in the Southern District of

New York and elsewhere, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," 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 under Title 18, United States Code, Section 1029(a).

24. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly, and with intent to defraud, would and did effect transactions, with one and more access devices issued to other persons, to receive payment and other things of value during a one-year period the aggregate value of which was equal to and greater than \$1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

Overt Acts

25. In furtherance of the conspiracy and to effect the illegal object thereof, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, using a computer located in New York, New York, obtained dozens of credit card

numbers of other individuals that he knew to be obtained without the authorization of the cardholders. MONSEGUR obtained some of these credit card numbers by hacking into the computer systems of at least two companies. MONSEGUR obtained other credit card numbers from an online forum known for providing stolen credit card numbers.

b. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, while in New York, New York, used the credit card numbers of other individuals, without the authorization of those individuals, to pay his own bills and, by such conduct, made and attempted to make payments in excess of \$1,000 during a one-year period.

c. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR provided, in exchange for a fee, credit card numbers of other individuals to co-conspirators not identified herein, knowing that those co-conspirators planned to use the credit card numbers to make more than \$1,000 in fraudulent charges for, among other things, bills that they owed.

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

COUNT SIX

(Conspiracy to Commit Bank Fraud)

The United States Attorney further charges:

26. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate and agree together and with each other to commit offenses under Title 18, United States Code, Section 1344.

27. It was a part and an object of the conspiracy that HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, and others known and unknown, willfully and knowingly would and did execute a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institution by means of false and fraudulent pretenses, representations and promises, in violation of Title 18, United States Code, Section 1344.

Overt Acts

28. In furtherance of the conspiracy and to effect the illegal object thereof, HECTOR XAVIER MONSEGUR, a/k/a

"Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, committed the following overt acts, among others, in the Southern District of New York and elsewhere:

a. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, using a computer located in New York, New York, obtained the routing and account numbers for more than a dozen accounts, together with personal identification information including, among other things, names, Social Security numbers and addresses of individuals associated with those accounts.

b. From at least in or about 2010, up to and including on or about June 7, 2011, MONSEGUR, using a computer located in New York, New York, transmitted to a co-conspirator not identified herein the aforementioned routing and account numbers, together with certain personal identification information of others, knowing that the co-conspirator would use that information to try to obtain monies to which the co-conspirator was not entitled.

(Title 18, United States Code, Section 1349.)

COUNT SEVEN

(Aggravated Identity Theft)

The United States Attorney further charges:

29. From at least in or about 2010, up to and including on or about June 7, 2011, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, willfully and knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, MONSEGUR transferred, possessed, and used, among other things, the names, Social Security numbers, account numbers, and credit card account numbers of other persons in connection with his participation in a conspiracy to commit access device fraud, as charged in Count Five of this Information, and in connection with his participation in a conspiracy to commit bank fraud, as charged in Count Six of this Information.

(Title 18, United States Code, Sections 1028A and 2.)

FORFEITURE ALLEGATION AS TO COUNTS ONE THROUGH FOUR

30. As a result of committing one or more of the offenses alleged in Counts One through Four of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting,

or derived from, proceeds obtained directly or indirectly as a result of one or more of the offenses, including but not limited to a sum of money representing the amount of proceeds obtained as a result of one or more of the said offenses.

FORFEITURE ALLEGATION AS TO COUNT FIVE

31. As a result of committing the offense alleged in Count Five of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States:

a. pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, including but not limited to a sum of money representing the amount of proceeds obtained as a result of the said offense; and

b. pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the said offense.

FORFEITURE ALLEGATION AS TO COUNT SIX

32. As a result of committing the offense alleged in Count Six of this Information, HECTOR XAVIER MONSEGUR, a/k/a "Sabu," a/k/a "Xavier DeLeon," a/k/a "Leon," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(2)(A), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the

offense, including but not limited to, a sum of money representing the amount of proceeds obtained as a result of the said offense.

Substitute Assets Provision

33. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value;

or

e. has been commingled with other property which cannot be subdivided without difficulty; it is the intent of the United States, pursuant to 18 U.S.C. § 982 and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982(a)(2)(A), 982(a)(2)(B), and 1029(c)(1)(C), and Title 21, United States Code, Section 853(p).)

Preet Bharara
PREET BHARARA
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

HECTOR XAVIER MONSEGUR,
a/k/a "Sabu,"
a/k/a "Xavier DeLeon,"
a/k/a "Leon,"

Defendant.

INFORMATION

11 Cr.

(18 U.S.C. §§ 1030(b), 1030(a)(4),
1029(b)(2), 1349, 1028A and 2)

PREET BHARARA
United States Attorney.

12 MAG 609

Approved: Thm Bm
THOMAS BROWN
Assistant United States Attorney

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

- - - - -x
UNITED STATES OF AMERICA : AMENDED COMPLAINT

-v.- : Violation of
18 U.S.C. §§ 2511 & 2

DONNCHA O'CEARRBHAIL, :
a/k/a "palladium," : COUNTY OF OFFENSE:
a/k/a "polonium," : NEW YORK
a/k/a "anonsacco," :
Defendant. :
- - - - -x

SOUTHERN DISTRICT OF NEW YORK, ss.:

GEORGE J. SCHULTZEL, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges:

COUNT ONE

1. From in or about January 2012, up to and including in or about February 2012, in the Southern District of New York and elsewhere, DONNCHA O'CEARRBHAIL, a/k/a "palladium," a/k/a "polonium," a/k/a "anonsacco," the defendant, willfully and knowingly, intentionally disclosed, and endeavored to disclose, to any other person the contents of any wire, oral, and electronic communication, knowing and having reason to know that the information was obtained through the interception of a wire, oral and electronic communication in violation of Title 18, United States Code, Section 2511(1), to wit, the defendant, while in Ireland, unlawfully and intentionally recorded a telephone conference call between law enforcement officers in the United States and law enforcement officers in the United Kingdom and then provided copies of that recording to individuals in New York, New York and elsewhere.

(Title 18, United States Code, Sections 2511(1)(c) & 2.)

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

2. I have been a Special Agent with the FBI for approximately two years and have been involved in the investigation of this matter. 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, and my conversations with 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 the 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.

BACKGROUND ON ANONYMOUS, LULZSEC AND ANTISEC

3. Since in or about 2010, the FBI has been involved in the investigation of a loose confederation of computer hackers and others known as "Anonymous," and its affiliated groups. Since at least in or about 2008, certain members of Anonymous have 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 throughout the world. Between in or about December 2010 and in or about May 2011, one group of individuals affiliated with Anonymous who engaged in such criminal conduct was composed of elite computer hackers who collectively referred to themselves as "Internet Feds." In or about May 2011, certain members of Internet Feds formed and became the principal members of a new hacking group, "Lulz Security" or "LulzSec." Then, in or about June 2012, certain individuals who were affiliated with Anonymous, Internet Feds, and/or LulzSec, joined with other computer hackers 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, among other things, the intrusion into, and subsequent release of data stolen from, computer systems used by more than 50 police departments in the United States and an intrusion into the computer systems of the North Atlantic Treaty Organization ("NATO").

THE INVESTIGATION

4. Based on my participation in this investigation, I know that a computer hacker who was, at various times, affiliated with Anonymous and other computer hacking organizations (the "CW"), was arrested by the FBI, and agreed to cooperate with the Government's investigation in the hope of receiving a reduced sentence. The CW has pleaded guilty to various charges, including charges relating to computer hacking, pursuant to a cooperation agreement with the Government. The information provided by the CW has been shown to be accurate and reliable and is corroborated by other information developed in this investigation. While acting under the direction of the FBI, the CW has communicated with other computer hackers and received information from those hackers regarding their hacking activities.

5. Based in part on information provided to the FBI by An Garda Síochána, the National Police Service of Ireland (the "Garda"), I know that in or about December 2011/January 2012, the personal Gmail webmail accounts of two Garda officers (the "Garda Officers") were compromised by a computer hacker (the "Compromised Gmail Accounts"). I also know that one of the Garda Officers whose accounts were compromised routinely sent email messages from an official Garda email account to one of the Compromised Gmail Accounts.

6. Based on information provided by the CW, and based on records from the FBI's email system, I know that in or about January 2012, email messages were circulated among various FBI agents and foreign law enforcement officers, including law enforcement officers in Ireland, for the purpose of scheduling a conference call on January 17, 2012 to discuss law enforcement investigations of Anonymous and other hacking groups. These email messages contained a telephone number and passcode that was to be used to access the conference call. Based upon information provided by the Garda to the FBI, I know that one of the Garda Officers forwarded these emails to one of the Compromised Gmail Accounts.

7. Based on information provided by the CW, and based on a transcript of Internet chats recorded by the FBI, I know that on or about January 14, 2012, an individual using the online nickname "anonsacco" and the CW exchanged Internet chat

messages in a private Internet chatroom.¹ According to the transcript of that chat, anonsacco stated, "Hi mate. Could I ask you for help? I need to intercept a conference call which would be a very good leak. I have acquired info about the time, phone number, and pin number for the conference call. I just don't have a good VOIP^[2] setup for actually calling in to record it." Anonsacco then stated, "If you could help me, I am happy to leak the call to you solely. I guarantee it will be of interest!!" Anonsacco further stated that the call was on "Tuesday" [which would be January 17, 2012], and that "I want to test everything out before hand. I don't want to miss this call!!" and "This will be epic!"

8. Based on a recording to which I have listened, and based on my conversations with an FBI agent who spoke with several participants in the call, I know that the January 17, 2012 law enforcement conference call ("the Conference Call") in fact occurred. During the Conference Call, several FBI agents, some of whom were in the United States at the time of the call, and foreign law enforcement agents, who were in the United Kingdom at the time of the call, engaged in discussion of various matters related to the investigation of Anonymous and affiliated computer hacking groups. Among other things that were discussed was the investigation being conducted by the FBI in New York.

9. Based on information provided by the CW, and based on a transcript of Internet chats recorded by the FBI, I know that on or about January 28, 2012, anonsacco exchanged Internet chat messages with the CW in a private Internet chatroom. According to the transcript of that chat, anonsacco stated, "Hey mate. Would you like a recording of a call between SOCA^[3] and the FBI regarding anonymous and lulzsec?" Anonsacco

¹ All the Internet chats involving the CW that are detailed in this Complaint were recorded by the FBI with the CW's consent.

² Based on my training, experience, and familiarity with this investigation, I know that "VOIP" stands for "Voice Over Internet Protocol," a popular means by which individuals may place telephone calls over the Internet. Skype is a popular provider of VOIP services.

³ Based on my training, experience, and familiarity with the investigation, I know that SOCA is an acronym for the Serious

further stated, "I think we need to hype it up. Let the feds think we have been recording their calls. They will be paranoid that none of their communications methods are safe or secure from Anon [Anonymous]" and "It will hopefully cause lots of issues and affect the feds ability to communicate and cooperate around the world." Anonsacco then provided to the CW, through a file sharing service on the Internet, a copy of the recording of the Conference Call. I have spoken with an FBI agent who has listened to this recording and who has spoken with several participants in the January 17, 2012 Conference Call, and that agent informs me that the recording is in fact of the Conference Call. At the times the CW chatted with anonsacco, as detailed above, and at the time that anonsacco provided the recording of the Conference Call to the CW, the CW was in New York, New York.

10. Based on my review of YouTube.com, a popular Internet video sharing website, I know that, on or about February 3, 2012, an individual using the online nickname "TheDigitalfolklore" posted an audio file of the Conference Call to the YouTube website. The video image associated with the recording bore a symbol associated with AntiSec, as well as the word "AntiSec." The recording on YouTube is available to the general public.

IDENTIFICATION OF THE DEFENDANT

11. As detailed below, I know that anonsacco is DONNCHA O'CEARRBHAIL, a/k/a "palladium," a/k/a "polonium," a/k/a "anonsacco," the defendant, a resident of Ireland, for the following reasons:

a. Based on my conversations with other FBI agents and my review of documents related to the investigation, I know that in early January 2011, a computer network that hosted the website of Fine Gael, an Irish political party, was hacked and Fine Gael's website was defaced with an Anonymous-related symbol and, among other things, the words "<owned [hacked] by Raepsauce and Palladium>." I have spoken with another agent who has reviewed the contents, obtained pursuant to a search warrant obtained in the Southern District of New York, of a Facebook account held by a co-conspirator not named as a defendant herein. Based on my conversation with that agent, I have learned that on

Organized Crime Agency, a law enforcement agency in the United Kingdom.

or about January 9, 2011 (around the time the Fine Gael website was defaced), the user of the Facebook account received an electronic message from another Facebook user with the name "Donncha Carroll" ["Carroll" is an English equivalent of the Gaelic "O'Cearrbhail"]. The message from "Donncha Carroll" contained computer code which produces the same defacement as appeared on the Fine Gael website when it was defaced.

b. Based on information provided by the CW, and based on a transcript of Internet chats recorded by the FBI, I know that on or about August 4, 2011, the CW and an individual using the online nickname "palladium" exchanged private chat messages over the Internet. During the chat, the CW and palladium discussed the theft of palladium's online identity by another individual. Palladium inquired what he could do to prove his identity to the CW and stated, "I can post some info I have from really old opps," meaning prior computer hacking activity. Palladium continued, "I can explain something about the sun" and "I can give you some info I still have from the first fox LFI [hack]."⁴ Later in the chat, the CW asked if a certain IP address⁵ (the "Palladium IP Address") was used by palladium, to

⁴ Based on my conversations with other FBI agents and my review of documents related to the investigation, I know that (1) in or about April 2011, individuals affiliated with Internet Feds, including an individual using the online alias "palladium," participated in a cyber attack on the website and computer network of Fox Broadcasting Company ("Fox"), in which those individuals gained unauthorized access to Fox's computer network and stole and publicly disclosed confidential information; and (2) in or about July 2011, individuals affiliated with LulzSec and AntiSec, including an individual using the online alias "palladium," participated in a cyber attack on the website and computer network of The Sun, a British newspaper. Among other things, The Sun's website was defaced with a fake news article that referenced the word "palladium."

⁵ 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.

which palladium responded that the "ip [address] looks like a wifi I connect from." The CW also asked whether palladium uses "Perfect Privacy," a virtual private network^[6] service located in Germany, to which palladium responded, "yes I use that vpn."

c. Based on information provided to the FBI by the Garda, I know that on or about September 1, 2011, Garda officers arrested DONNCHA O'CEARRBHAIL in Ireland⁷ for his alleged participation, using the online nickname "palladium," in connection with the Anonymous-related hack and defacement of the Fine Gael website in around January 2011. Prior to O'CEARRBHAIL's arrest, the FBI had provided to the Garda certain chat logs obtained by the CW of communications in two online chat forums called "#sunnydays" and "#babytech."⁸ Garda officers then showed certain of these chat logs to O'CEARRBHAIL during his post-arrest interview, in which O'CEARRBHAIL admitted participating in the Fine Gael hack described above. O'CEARRBHAIL was released following his arrest pending consideration of charges against him.

d. Based on information provided by the CW, and based on a transcript of Internet chats recorded by the FBI, I know that on or about November 12, 2011, the CW and an individual using the online nickname "polonium" exchanged private chat messages over the Internet. During the chat, polonium stated "I know for a fact the FBI has a large amount of log files" from a server associated with Anonymous, and that "I was v&[⁹]", to

⁶ Based on my training, experience, and familiarity with the investigation, I know that a "virtual private network" or "VPN" service can be used by individuals to securely and anonymously access the Internet.

⁷ Based on information provided by the Garda, I know that O'CEARRBHAIL is an Irish citizen who resides in Ireland.

⁸ Based on my training, experience, and familiarity with this investigation, I know that "#sunnydays" and "#babytech" were chat channels used by individuals associated with Anonymous and affiliated hacking groups. #sunnydays was a restricted channel which required a password to enter.

⁹ Based on my training, experience, and familiarity with this investigation, I know that "v&" or "vand" or "vanned" is Internet slang for being arrested, as in to be taken away in a police van.

which the CW responded, "no way. what makes you think that?," to which polonium replied, "I was shown them during my interrogation." The CW then asked, "like did you see raw logs or from channels?", to which polonium responded, "#sunnydays and #babytech at least." Later in the conversation, the CW asked, "who is this?" to which polonium responded, "this is palladium."

e. Based on information provided by the CW, and based on a transcript of Internet chats recorded by the FBI, I know that on or about January 9, 2012, the CW and anonsacco exchanged Internet chat messages . During the chat, anonsacco stated, "I just got into the iCloud for the head of a national police cybercrime unit. I have all his contacts and can track his location 24/7."¹⁰ Anonsacco then referenced "sunnydays", after which the CW inquired, "so who were you? if you know about !sunnydays," and "the channel name was leaked to feds. so clearly im interested in who you were," to which anonsacco responded, "I understand it was leaked. That caused me a lot of hassle. Could you understand that I don't want to align myself with a compromised screenname?" The CW then asked, "hassle how? you got raided? or people doxed¹¹ you?" Later, the CW asked, "so if you were raided, did they ask you about me?", to which anonsacco responded, "No. Not you personally."

f. Pursuant to a court order, the FBI obtained information from Google regarding the Compromised Gmail Accounts. According to the records obtained from Google, and based on information provided by the Garda and the Garda Officers, it appears that in or about January 2012 there were a total of 146 instances in which an individual using the VPN service Perfect Privacy obtained unauthorized access to the Compromised Gmail Accounts. In addition, during this same time, there was at least one instance of unauthorized access to one of the Compromised Gmail Accounts by the Palladium IP Address, and several instances of unauthorized access by IP addresses allocated to the same

¹⁰ Based on information provided by the Garda to the FBI, I know that one of the Garda Officers was the supervisor of the Garda's cybercrime unit.

¹¹ Based on my training, experience, and familiarity with this investigation, I know that "raided" is Internet slang for being arrested and that "dox" or "doxed" is Internet slang for having one's true identity being revealed on the Internet.

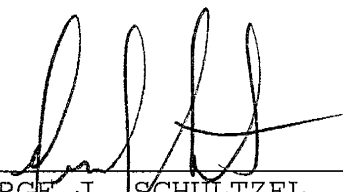
Internet service provider in Ireland as the Palladium IP Address.¹²

g. Based on my training, experience, and familiarity with the investigation, I know that individuals engaged in certain forms of Internet chat, such as some of those detailed in this Complaint, may seek to cloak their true identities, including their true IP addresses, when engaged in online chat sessions.¹³ Individual users may do this by using a "cloak key" that is unique to each computer network that hosts chat forum(s) in which the user participates. A cloak key employs an algorithm which uses, among other things, the user's IP address to generate a new, "cloaked" loginID. Accordingly, if a user with the same IP address logs into the same chat hosting computer network, the user's cloaked loginID should tend to be the same, regardless of whatever other aliases the user employs in chats. Based on the FBI's analysis of the chat sessions detailed above, it appears that the online nicknames palladium, polonium, and anonsacco shared one or more times the same cloaked loginID. Accordingly, it appears that these nicknames had been accessed from the same IP address and thus the same computer. In addition, on several other occasions since in or about June 2011 up to the present, the nicknames palladium and polonium shared loginIDs which had "Donncha" -- the defendant's first name -- as the associated username.

¹² Based on my training, experience, and familiarity with the investigation, I know that "Internet Service Providers" or "ISPs" are assigned sequential blocks of IP address which they assign to their customers.

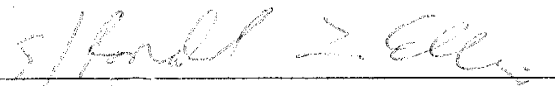
¹³ When users log in to particular kinds of online chats, including chats discussed in this Complaint, they are often identified by information -- separate from any aliases by which the user may later identify themselves in chats -- in the form [username]@[loginID]. The loginID is a string of information, which may include the user's IP address. The username is designated by the user.

WHEREFORE, deponent prays that a warrant issue for the arrest of DONNCHA O'CEARRBHAIL, a/k/a "palladium," a/k/a "polonium," a/k/a "anonsacco," the defendant, and that he be imprisoned or bailed as the case may be.



GEORGE J. SCHULTZEL
Special Agent
Federal Bureau of Investigation

Sworn to before me this
6th day of March, 2012



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