

NO. 13-1816

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

ANDREW AUERNHEIMER,

DEFENDANT-APPELLANT.

On Appeal From The United States District Court
For The District of New Jersey
Case No. 2:11-cr-00470-SDW-1
Honorable Susan D. Wigenton, District Judge

APPENDIX VOLUME I
pp. 1-36

Tor B. Ekeland
Mark H. Jaffe
TOR EKELAND, P.C.
155 Water Street
Brooklyn, NY 11201
Tel.: (718) 285-9343
Email: tor@torekeland.com

Orin S. Kerr
2000 H Street, N.W.
Washington, DC 20052
Tel.: (202) 994-4775
Email: okerr@law.gwu.edu

Marcia C. Hofmann
LAW OFFICE OF MARCIA C. HOFMANN
25 Taylor Street
San Francisco, CA 94102
Tel.: (415) 830-6664
Email: marcia@marciahofmann.com

Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Email: hanni@eff.org

*Attorneys for Defendant-
Appellant Andrew Auernheimer*

TABLE OF CONTENTS

	<u>Appendix Page</u>
Notice of Defendant’s Appeal.....	1
Superseding Indictment.....	2
Opinion Denying Auernheimer’s Motion to Dismiss	18
Judgment in a Criminal Case	30

Dated this 1st day of July, 2013

Respectfully submitted,

/s/ Hanni M. Fakhoury
Hanni M. Fakhoury
ELECTRONIC
FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: hanni@eff.org

*Attorney for Defendant-
Appellant Andrew Auernheimer*

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system on July 1, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 1, 2013

By: /s/ Hanni M. Fakhoury
Hanni M. Fakhoury
ELECTRONIC
FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 436-9993
Email: hanni@eff.org

*Attorney for Defendant-
Appellant Andrew Auernheimer*

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

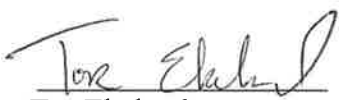
X	X
UNITED STATES OF AMERICA,	
Plaintiff,	
v.	
ANDREW AUERNHEIMER,	
Defendant.	
X	X

11-CR-470 (SDW)

**NOTICE OF DEFENDANT'S
APPEAL**

Defendant Andrew Auernheimer, through his attorneys, hereby gives notice that he appeals to the United States Court of Appeals for the Third Circuit from the entirety of the final judgment of this Court entered on March 20, 2013, as well as this Court's denial of Defendant's Motion for Judgment of Acquittal Under Federal Rule of Criminal Procedure 29, as announced by this Court on March 18, 2013.

Respectfully submitted,

By: 
Tor Ekeland
Dated: March 21, 2013

Mark H. Jaffe
Tor Ekeland, P.C.
155 Water Street
Brooklyn, NY 11201
Tel: 718.285.9343
Fax: 718.504.5417
Email: tor@torekeland.com

Nace Naumoski
Paris Ackerman & Schmierer LLP
618 Newark Avenue
Elizabeth, NJ 07208
Tel: 908.349.8462
Email: nace@palawfirm.com
Attorneys for Defendant Andrew Auernheimer

TO:
Michael Martinez
Executive Assistant United States Attorney
Zach Intrater
Erez Lieberman
Assistant United States Attorneys
District of New Jersey
970 Broad Street, Suite 700
Newark, NJ 07102

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon. Susan D. Wigenton
:
v. : Crim. No. 11-470
:
ANDREW AUERNHEIMER, : 18 U.S.C. §§ 371 & 1028(a)(7),
a/k/a "Weev" : & § 2
a/k/a "Weevlos" :
a/k/a "Escher" :

S U P E R S E D I N G I N D I C T M E N T

The Grand Jury, in and for the District of New Jersey,
sitting at Newark, charges:

COUNT ONE

(Conspiracy to Access a Computer Without Authorization)

1. At all times relevant to this Indictment:
 - a. Defendant ANDREW AUERNHEIMER resided in Arkansas, and was a member of an organization called Goatse Security ("Goatse").
 - b. Co-conspirator Daniel Spitler resided in California, and was a member of Goatse.
 - c. Goatse described itself as a "security research" company, and was comprised of Internet hackers (individuals who accessed sites and information to which they did not have authorized access) and so-called "trolls" (individuals who intentionally, and without authorization, disrupt services and content on the Internet). The Goatse website

provided a hyperlink to the website of an organization referred to as the "GNAA."

- d. The GNAA website states that "[t]his website is maintained by the GNAA, world-famous trolling organization." The GNAA website provided hyperlinks to the Goatse website, as well as to defendant AUERNHEIMER's LiveJournal weblog.
- e. The iPad, introduced to the market on or about January 27, 2010, was a device developed and marketed by Apple Computer, Inc. It was a touch-screen tablet computer, roughly the size of a magazine. The iPad allowed users to, among other things, access the Internet, send and receive electronic mail, view photographs and videos, read electronic books, word-process, and create spreadsheets and charts.
- f. The "3G" model of the iPad ("iPad 3G") allowed users to access to the Internet using either Wi-Fi or the 3G wireless network hosted by AT&T Services, Inc. ("AT&T").
- g. AT&T was an interexchange carrier and long distance telephone company, located in Bedminster, New Jersey, among other places.
- h. AT&T's servers and individual iPads were

"protected computers" as defined in Title 18, United States Code, Section 1030(e)(2).

- i. Title 18, United States Code, Section 1030(e)(2)(B)(2) provides, in relevant part, that "the term 'protected computer' means a computer -- . . . (B) which is used in or affecting interstate or foreign commerce or communication."
- j. Among other things, AT&T provided certain iPad users with Internet connectivity via AT&T's 3G wireless network.
- k. iPad 3G users who wished to subscribe to the AT&T 3G network had to register with AT&T. During the registration process, the user was required to provide, among other things, an e-mail address, billing address, and password.
- l. The iPad 3G user e-mail addresses, billing addresses, and passwords were not available to the public and were kept confidential by AT&T.
- m. At the time of registration, AT&T automatically linked the iPad 3G user's e-mail address to the Integrated Circuit Card Identifier ("ICC-ID") of the user's iPad, which was a 19 to 20 digit number unique to every iPad (specifically, unique to the Subscriber Identity Module ("SIM") card in the

iPad).

- n. Due to this feature, each time a user accessed the AT&T website, the user's ICC-ID was recognized and, in turn, the user's e-mail address was automatically displayed. This allowed the user speedier and more user-friendly access to the network.
- o. The ICC-IDs and iPad user e-mail addresses were not available to the public and were kept confidential by AT&T.

GOATSE SECURITY

2. Defendant AUERNHEIMER, as the self-professed spokesman for Goatse, has previously been public and outspoken about his trolling activities.

3. According to the Goatse Security website, the Goatse "Team" included approximately eight members, among whom were defendant AUERNHEIMER, who was also known as "weev," and Spitler.

4. The Goatse website described defendant AUERNHEIMER as having "[e]xtensive offensive web app[lication] vuln[erability] and business logic exploitation experience. . . . Representing antisecc, Bantown and Encyclopedia Dramatica. President of the GNAA." Spitler was described as an "embedded and mobile devices engineer. PPC assembly. GNAA, obviously."

THE CONSPIRACY

5. From on or about June 2, 2010 through on or about June 15, 2010, in the District of New Jersey, and elsewhere, defendant

ANDREW AUERNHEIMER

knowingly and intentionally conspired with Spitler and others to access a computer without authorization and to exceed authorized access, and thereby obtain information from a protected computer, namely the servers of AT&T, in furtherance of a criminal act in violation of the Constitution and laws of the State of New Jersey, namely, N.J.S.A 2C:20-31(a), contrary to Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii).

OBJECTS OF THE CONSPIRACY

6. The objects of the conspiracy were for defendant AUERNHEIMER, Spitler, and others to steal and disclose the personal identifying information of thousands of individuals, to cause monetary and reputational damage to AT&T and to create monetary and reputational benefits for themselves.

MANNER AND MEANS OF THE CONSPIRACY

A. The Account Slurper

7. Prior to mid-June 2010, when an iPad 3G communicated with AT&T's website, its ICC-ID was automatically displayed in the Universal Resource Locator, or "URL," of the AT&T website in plain text. Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, defendant AUERNHEIMER and Spitler conspired to write, and did write, a

script termed the "iPad 3G Account Slurper" (the "Account Slurper") and deployed it against AT&T's servers.

8. The Account Slurper attacked AT&T's servers for several days in or around June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked as follows:

- a. The Account Slurper was designed to mimic the behavior of an iPad 3G so that AT&T's servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the Account Slurper access to AT&T's servers.
- b. Once deployed, the Account Slurper utilized a process known as a "brute force" attack - an iterative process used to obtain information from a computer system - against AT&T's servers. Specifically, the Account Slurper randomly guessed ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

9. From on or about June 5, 2010 through on or about June 9, 2010, the Account Slurper attacked AT&T's servers, gained unauthorized access to those servers, and ultimately stole for its hacker-authors, including defendant AUERNHEIMER and Spitler,

approximately 120,000 ICC-ID/e-mail address pairings for iPad 3G customers. This was done without the authorization of AT&T, Apple, or any of the individual iPad 3G users.

10. Neither defendant AUERNHEIMER, Spitler, nor any other member of Goatse obtained prior authorization from any victim of the breach.

B. Defendant AUERNHEIMER and Goatse Knowingly Disclose Approximately 120,000 ICC-IDs and Corresponding E-Mail Addresses to the Internet Magazine Gawker, and Take Credit for the Breach

11. On or about June 9, 2010, immediately following the theft, the hacker-authors of the Account Slurper knowingly provided stolen e-mail addresses and ICC-IDs to the website Gawker. Gawker was an internet magazine. Gawker proceeded to publish on its website the stolen information, though in redacted form, as well as an article concerning the breach (the "Gawker Article").

12. Also on or about June 9, 2010, defendant AUERNHEIMER made an entry on his LiveJournal weblog, which read, in pertinent part: "Oh hey, my security consulting group just found a privacy breach at AT&T[.]" LiveJournal was a social networking website on which users could set up personal weblogs and post messages. Once a weblog had been created, only the user of that weblog could post messages and content on that weblog. The post further linked to the Gawker Article and stated: "[T]his story has been broken for 15 minutes, twitter is blowing the f[***] up, we are

on the forntpage [sic] of google news and we are on drudge report (the big headline)[.]” The “User Profile” for the LiveJournal weblog, <http://weev.livejournal.com>, listed the user as “weev” with the name “Escher Auernheimer.”

13. On or about June 10, 2010, the website CNET published an article titled, “Hacker defends going public with AT&T’s iPad data breach (Q&A).” The article reported: “On Thursday, CNET talked to a key member of Goatse - Escher Auernheimer, also known as ‘Weev’ - about the group and what motivates them.” In the article, a question and answer dialog was presented, including the following:

- Q: So, one of your members had an iPad and noticed this strange interaction with the AT&T Web site?
A: He used this AT&T security maintenance app. It was part of the normal user experience that tipped him off to something that would allow him to scrape this data.
Q: Then a script was written to do an automated brute force, right?
A: Correct.

C. The Internet Relay Chats

14. On or about June 15, 2010, during the execution of a Court-authorized search warrant, defendant AUERNHEIMER agreed to speak with federal law enforcement officers and stated, among other things, that he and the other members of Goatse often communicated with one another using an online medium known as Internet Relay Chat, or “IRC.”

i. June 5, 2010: Exploiting the Breach

15. On or about June 5, 2010, co-conspirator Spitler was

chatting with fellow Goatse members "Nstyr" and "Pynchon." The three considered the possible benefits of harvesting ICC-ID/e-mail pairings.

Spitler: if you enter valid ICCIDs in this website you can get iPad subscriber email addresses I dont see the point unless we phish¹ for passes [passwords] even then that's boring

Nstyr: data minig *minig you could put them in a database for spamming for example sell them to spammers. . .

Spitler: tru ipad focused spam

Pynchon: harvest all the emails then expose it publicly

Spitler: hahaha

Pynchon: tarnish at&t

Spitler: true

Nstyr: or sell if for thousands to the biggest spammers

16. Later that day, Spitler reported the following to defendant AUERNHEIMER:

Spitler: I just harvested 197 email addresses of iPad 3G subscribers there should be many more . . . weev: did you see my new project?

AUERNHEIMER: no

Spitler: I'm stepping through iPad SIM ICCIDs to harvest email addresses if you use someones ICCID on the ipad service site it gives you their address

. . .
AUERNHEIMER: loool² thats hilarious HILARIOUS oh man now this is big media news . . . is it scriptable? arent there SIM that spoof iccid?

Spitler: I wrote a script to generate valid iccids and it loads the site and pulls an email

. . .
AUERNHEIMER: this could be like, a future massive phishing

¹ "Phishing" involved sending e-mails to users falsely claiming to be an established, legitimate enterprise in an attempt to scam the users into surrendering private information that would be used for identity theft.

² "LOL" and its variants, including "lawlwla," stand for laughing out loud.

operation serious like this is valuable data we have a list
a potential complete list of AT&T iphone subscriber emails
Spitler: ipad but yeah

17. When Spitler announced that he was "in a rut" and
having difficulty determining additional ICC-ID/e-mail pairings,
defendant AUERNHEIMER assisted, offering: "SIM cards may be
allocated by geographic region, either for number administration
or [] network planning reasons. The method of payment (pre-paid,
post-paid) may be allocated on the SIM cards. . . . so sims are
definitely preallocated either by geographic region sales
channes, service providers or MVNOs question is who allocates
them . . . probably AT&T suballocates free IDs to apple hopefully
not at random . . . otherwise we have a real big space to
search[.]"

18. On or about June 5, 2010, and again the following day,
defendant AUERNHEIMER encouraged Spitler to amass as many ICC-
ID/e-mail pairings as possible, writing: "if we can get a big
dataset we could direct market ipad accessories[.]" Likewise,
after learning that Spitler had collected "625 emails," defendant
AUERNHEIMER wrote: "takes like, millions to be profitable re:
spam but thats a start[.]"

ii. June 6, 2010: Collecting Stolen E-Mails

19. Responding to defendant AUERNHEIMER's encouragement, on
or about June 6, 2010, Spitler reported:

Spitler: I hit f[***]ing oil
AUERNHEIMER: looooool nice

Spitler: If I can get a couple thousand out of this set where can we drop this for max lols?

AUERNHEIMER: dunno i would collect as much data as possible the minute its dropped, itll be fixed BUT valleywag i have all the gawker media people on my facecrook friends after goin to a gawker party

20. As Spitler uncovered additional ICC-ID/e-mail pairings, he continued speaking with defendant AUERNHEIMER about releasing the information to the press and the legality of the data breach:

Spitler: do I got to get involved

AUERNHEIMER: no

Spitler: I'd like my anonaminity

AUERNHEIMER: alright

Spitler: sry dunno how legal this is or if they could sue for damages

AUERNHEIMER: absolutely may be legal risk yeah, mostly civil you absolutely could get sued to f[***]

Spitler: D8³

AUERNHEIMER: alright i can wrangle the press just get me the codes and whatnot show me how to run this thing

21. Spitler then proceeded to provide the script to defendant AUERNHEIMER, writing: "heres the script you run it php [redacted]"

22. As the data breach continued, defendant AUERNHEIMER wrote to Spitler: "if we get 1 reporters address with this somehow we instantly have a story . . . the best way to have a leadin on it . . . HI I STOLE YOUR EMAIL FROM AT&T WANT TO KNOW HOW?"

23. Spitler then proceeded to provide defendant AUERNHEIMER

³ The phrase "D8" means "balls deep," i.e., to be deeply involved in an activity or to perform an activity to the fullest extent possible.

with an ICC-ID and e-mail address for a member of the Board of Directors at News Corporation.

24. Defendant AUERNHEIMER sent an e-mail to that board member, which read in relevant part:

"An information leak on AT&T's network allows severe privacy violations to iPad 3G users. Your iPad's unique network identifier was pulled straight out of AT&T's database We have collected many such identifiers for members of the media and major tech companies If a journalist in your organization would like to discuss this particular issue with us[,] I would be absolutely happy to describe the method of theft in more detail."

The e-mail to the board member included the ICC-ID for the board member's iPad.⁴

iii. June 7, 2010: Identifying Information from More Than 100,000 Victims Stolen

25. After Spitler announced that he had stolen over 100,000 ICC-ID/e-mail address pairings, defendant AUERNHEIMER stated:

"the more email addresses we get . . . the more of a freakout we can cause if nothing else we can pack these into a [database] . . . and do a mail merge and mail EVERYONE with an ipad 3g 1 o 1[.]"
To that, Spitler responded simply: "lawlwla[.]"

⁴ In addition to the e-mail sent to the board member at News Corporation, defendant AUERNHEIMER sent similar e-mails to an employee of the *San Francisco Chronicle*, an employee of the Washington Post, and to employees of Thomson-Reuters. Defendant AUERNHEIMER later forwarded these e-mails to yet others, including a reporter at Forbes magazine.

iv. June 10, 2010: Destroying Evidence

26. On or about June 10, 2010, defendant AUERNHEIMER and Spitler had the following conversation during which they discussed destroying evidence of their crime:

AUERNHEIMER: i would like get rid of your shit like are we gonna do anything else with this data?

Spitler: no should I toss it?

AUERNHEIMER: i dont think so either might be best to toss

Spitler: yeah, I dont really give a fuck about it the troll is done

AUERNHEIMER: yes we emerged victorious

Spitler: script is going byebye too

OVERT ACTS

27. In furtherance of the conspiracy and to effect its objects, defendant AUERNHEIMER and his co-conspirators, including Spitler, committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

- a. In or around June 2010, the co-conspirators wrote the Account Slurper.
- b. In or around June 2010, the co-conspirators deployed the Account Slurper against AT&T's servers.
- c. In or around June 2010, defendant AUERNHEIMER sent a series of e-mails to victims that included the ICC-IDs of the victims' iPads, and described his and his co-conspirators' actions as a "theft."
- d. In or around June 2010, defendant AUERNHEIMER and

his co-conspirators disclosed approximately 120,000 stolen ICC-ID/e-mail address pairings for iPad 3G customers -- including thousands of customers who resided in New Jersey -- to the internet magazine Gawker.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

(Fraud in Connection with Personal Information)

1. Paragraphs 1 through 4 and 7 through 27 of Count One of this Superseding Indictment are hereby alleged and incorporated as though set forth in full herein.

2. From on or about June 2, 2010 through on or about June 15, 2010, in the District of New Jersey, and elsewhere defendant

ANDREW AUERNHEIMER

knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including means of identification of New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to Title 18, United States Code, Section 1030(a)(2)(C).

In violation of Title 18, United States Code, Sections 1028(a)(7) and Section 2.

A TRUE BILL

Paul J. Fishman/rah

PAUL J. FISHMAN
UNITED STATES ATTORNEY

CASE NUMBER: 2010R00631

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

ANDREW AUERNHEIMER

SUPERSEDING INDICTMENT FOR

18 U.S.C. §§ 371 and 1028(a) (7)

PAUL J. FISHMAN
UNITED STATES ATTORNEY, NEWARK, NEW JERSEY

MICHAEL MARTINEZ
ZACH INTRATER
ASSISTANT U.S. ATTORNEYS
NEWARK, NEW JERSEY
(973) 645-2728

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA,	:	Criminal No. 11-cr-470 (SDW)
	:	
v.	:	OPINION
	:	
ANDREW AUERNHEIMER,	:	October 26, 2012
	:	
Defendant.	:	

WIGENTON, District Judge.

Before the Court is Defendant Andrew Auernheimer’s (“Defendant” or Auernheimer”) Motion to Dismiss the Superseding Indictment (“Motion”). The United States of America (“Government”) opposed the Motion. For the reasons stated below, the Court DENIES Defendant’s Motion.

FACTUAL AND PROCEDURAL HISTORY

Although the Court assumes the parties’ familiarity with the allegations and procedural history in the case, the Court will briefly review the facts relevant to the present Motion. In June 2010, Defendant and former co-defendant, Daniel Spitler (“Spitler”), created a computer program, the “Account Slurper” (“Program”), designed to exploit AT&T’s automated feature which linked iPad 3G users’ e-mail addresses to their unique iPad 3G Integrated Circuit Card Identifiers (“ICC-ID”). (Superseding Indictment, Count 1, ¶¶ 7-8.) Specifically, the Program “was designed to mimic the behavior of an iPad 3G so that AT&T’s servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the [Program] access to AT&T’s servers.” (*Id.* at Count 1, ¶ 8a.) Between June 5, 2010 and June 9,

2010, Defendant and Spitler's Program gained unauthorized access to AT&T's servers and obtained approximately 120,000 ICC-ID/e-mail address pairings from iPad 3G customers, including thousands of customers in New Jersey. (*Id.* at Count 1, ¶¶ 9, 27d.) Subsequently, Defendant and Spitler disclosed the stolen ICC-ID/e-mail address pairings to Gawker, an Internet magazine, and sent e-mails to members of various news organizations offering "to describe the method of theft in more detail." (*Id.* at Count 1, ¶¶ 11, 12, 24 & n.4, 27c.)

On August 16, 2012, a federal grand jury sitting in Newark, New Jersey returned a two-count Superseding Indictment against Defendant. Count One charged that, from June 2, 2010 through June 15, 2010, Defendant conspired to access a computer without authorization or exceeded authorized access, and thereby obtained information from a protected computer, in furtherance of a criminal act in violation of N.J.S.A. 2C:20-31(a), contrary to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of 18 U.S.C. § 371. Count Two charged that, from June 2, 2010 through June 15, 2010, Defendant knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to 18 U.S.C. § 1030(a)(2)(C), in violation of 18 U.S.C. §§ 1028(a)(7) and section 2.

LEGAL STANDARD

An indictment, if valid on its face and returned by a legally constituted and unbiased grand jury, "is enough to call for trial of the charge on the merits." *United States v. Vitillo*, 490 F.3d 314, 320 (3d Cir. 2007) (quoting *Costello v. United States*, 350 U.S. 359, 363 (1956)). "An indictment is generally deemed sufficient if it: [] (1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to

meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution.” Id. (quoting United States v. Rankin, 870 F.2d 109, 112 (3d Cir. 1989)) (internal quotation marks omitted).

“Federal Rule of Criminal Procedure 12(b)(3)(B) allows a district court to review the sufficiency of the government’s pleadings to . . . ensure that legally deficient charges do not go to a jury.” United States v. Huet, 665 F.3d 588, 595 (3d Cir. 2012) cert. denied, No. 11-10312, 2012 WL 1716258 (Oct. 9, 2012) (quoting United States v. Bergrin, 650 F.3d 257, 268 (3d Cir. 2011)) (internal quotation marks omitted); see United States v. DeLaurentis, 230 F.3d 659, 661 (3d Cir. 2000) (“Federal Rule of Criminal Procedure [12(b)(3)(B)] authorizes dismissal of an indictment if its allegations do not suffice to charge an offense.”) Although the Government is not obligated to bring forward its entire case in the indictment, “if the specific facts” alleged “fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation,” then the indictment fails to state an offense. Huet, 665 F.3d at 595 (quoting United States v. Panarella, 277 F.3d 678, 685 (3d Cir. 2002)). “Evidentiary questions—such as credibility determinations and the weighing of proof—should not be determined at this stage.” Bergrin, 650 F.3d at 265 (quoting United States v. Gallagher, 602 F.2d 1139, 1142 (3d Cir. 1979)) (internal quotation marks omitted). Accordingly, “a district court’s review of the facts set forth in the indictment is limited to determining whether, assuming all of those facts as true, a jury could find that the defendant committed the offense for which he was charged.” Huet, 665 F.3d at 595-96.

DISCUSSION

Defendant moves to dismiss the Superseding Indictment based on five arguments: (1) the CFAA is void for vagueness; (2) Count One poses a merger problem resulting in double jeopardy; (3) the District of New Jersey is not a proper venue for this action; (4) Count Two is

improperly pled because under 18 U.S.C. § 1028(a)(7), the offense cannot be “in connection with” a past crime; and (5) Count Two violates the First Amendment. For the reasons stated below, Defendant’s Motion is denied. Each argument is addressed in detail below.

I. Count One: CFAA is Void for Vagueness Under the Fifth Amendment’s Due Process Clause

A CFAA offense pursuant to 18 U.S.C. § 1030(a)(2)(C) occurs when an individual “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[.]” Defendant argues that the CFAA is unconstitutionally vague as applied because it does not provide notice that the charged conduct was illegal. Specifically, Defendant contends that “[t]he CFAA provides no definition as to what constitutes unauthorized access to a protected computer, and the courts are conflicted as to what unauthorized access means.” (Def. Br. 4.)

Although Defendant is correct that the statute does not define “without authorization,” following a well-established canon of statutory construction, several courts have construed this phrase based on its ordinary, dictionary definition. See Perrin v. United States, 444 U.S. 37, 42 (1979). For instance, in WEC Carolina Energy Solutions LLC v. Miller, the Fourth Circuit concluded that in the context of a CFAA violation, “based on the ‘ordinary, contemporary, common meaning,’ of ‘authorization,’ . . . [an individual] accesses a computer ‘without authorization’ when he gains admission to a computer without approval.” 687 F.3d 199, 204 (4th Cir. 2012) (citations omitted). Similarly, the Sixth Circuit stated in Pulte Homes, Inc. v. Laborers’ Int’l Union of N. Am. that because “Congress left the interpretation of ‘without authorization’ to the courts, we again start with ordinary usage. The plain meaning of ‘authorization’ is ‘[t]he conferment of legality; . . . sanction.’ Commonly understood, then, a defendant who accesses a computer ‘without authorization’ does so without sanction or

permission.” 648 F.3d 295, 303-04 (6th Cir. 2011) (citing 1 Oxford English Dictionary 798 (2d ed. 1989)). Lastly, in examining the CFAA statute in LVRC Holdings LLC v. Brekka, the Ninth Circuit applied “the “ordinary, contemporary, common meaning” of “without authorization.” 581 F.3d 1127, 1133 (9th Cir. 2009) (concluding that based on the plain meaning of the terms, individual did not act “without authorization”).

Additionally, “[i]t is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in light of the facts of the case at hand.” United States v. Moyer, 674 F.3d 192, 211 (3d Cir. 2012) (quoting United States v. Mazurie, 419 U.S. 544, 550 (1975)). “In criminal cases, because vagueness attacks are based on lack of notice, they may be overcome in any specific case where reasonable persons would know their conduct puts [them] at risk of punishment under the statute.” Id. (internal quotation and citation omitted) (alteration in original). Defendant’s vagueness challenge involves the CFAA and not First Amendment freedoms; thus, the Court will conduct its analysis “in light of the facts of the case at hand.” See id.

Based on the circumstances in this case, this Court is satisfied that the CFAA is not unconstitutionally vague and that “reasonable persons would know their conduct puts [them] at risk of punishment under the statute.” See Moyer, 647 F.3d at 211. The Superseding Indictment specifically alleges that Defendant gained unauthorized access to AT&T servers, stole 120,000 ICC-ID email address pairings, and committed the theft without authorization. (Superseding Indictment, Count 1, ¶¶ 9-10, 27d.) In his own words, Defendant even offered to provide the press with details of his “method of theft.” (Id. at Count 1, ¶ 24.) The Superseding Indictment sufficiently alleges the elements of unauthorized access and sufficiently alleges conduct demonstrating Defendant’s knowledge and intent to gain unauthorized access. For the purpose

of Defendant's Motion, accepting the allegations in the Superseding Indictment as true and in light of the facts at hand, the Court finds that the CFAA is not vague. Thus, Defendant's Motion fails with respect to this argument.¹

II. Count One: Double Jeopardy Under the Fifth Amendment

Under the Fifth Amendment's Double Jeopardy Clause, a defendant may not be charged or punished twice for the same offense. U.S. Const. Amend. V ("nor shall any person be subject for the same offense be twice put in jeopardy of life or limb"). A "merger problem tantamount to double jeopardy" occurs "where the facts or transactions alleged to support one offense are also the same used to support another." United States v. Cioni, 649 F.3d 276, 282 (4th Cir. 2011) (internal citations and quotations omitted). For example, in Cioni, the Fourth Circuit found that a merger problem arose where "the indictment [did] not allege facts sufficient to indicate that [] two crimes were based on distinct conduct" and instead were "actually based on [defendant's] single unsuccessful attempt to access [an] electronic e-mail account." Id. at 283. The Fourth Circuit clarified that "[i]f the government had proven that [defendant] accessed [the] e-mail inbox and then used the information from that inbox to access another person's electronic communications, no merger problem would have arisen."² Id.

¹ The Court notes that Defendant requested application of the Rule of Lenity to "narrow the CFAA to mean bypassing code based restrictions such as passwords or firewalls." (Def. Br. 7.) The cases cited by Defendant do not lend support to his argument that CFAA violations must always be read to require the bypassing of computer security measures. See Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 933 (E.D. Va. 2010); Koch Indus., v. Does, 10-cv-1275, 2011 WL 1775765, at *8 (D. Utah May 9, 2011). Additionally, in finding that the CFAA is not constitutionally vague in this case and poses no threat of Defendant's concern that "the government [] pursue expansive interpretations against unpopular defendants and then wield its expansive interpretation arbitrarily," the Court declines to apply the Rule of Lenity. (Def. Br. 7.)

² In Cioni, the Fourth Circuit additionally concluded that a merger problem arose where the Government relied on the same conduct to support an underlying statutory violation as well as the elevating violation. 649 F.3d at 282. Although the two crimes were "distinct and different," the Government's failure to articulate additional evidence in support of the elevating violation posed a merger problem. Id. at 283. Importantly, in Cioni, the Government conceded the merger problem, recognizing that "there was no evidence that the defendant committed this offense 'in furtherance of any' separate and distinct'" elevating violation. Id. at 282 (citations omitted).

Count One of the Superseding Indictment charges Defendant with conspiracy to access a computer without authorization or to exceed authorized access, and thereby obtain information from AT&T's servers (in violation of the CFAA, punishable as a felony), in furtherance of a New Jersey criminal statute, N.J.S.A. 2C:20-31(a). Defendant argues that "Count One violates the Double Jeopardy Clause because it improperly aggravates a CFAA misdemeanor into a felony." (Def. Br. 8.) Specifically, Defendant asserts that the object of the conspiracy—the CFAA offense—relies on proof of the same facts and conduct as the felony aggravator—N.J.S.A. 2C:20-31(a). (Def. Br. 8-9.)

As the Government correctly points out, the CFAA and N.J.S.A. 2C:20-31(a) do not require the same proof of conduct. (See Gov't Br. 23.) Moreover, in this case, the Government does not rely on the same allegations for the two offenses in the Superseding Indictment.

The CFAA requires two elements to establish a violation: (1) defendant "intentionally accesses a computer without authorization or exceeds authorized access" and (2) defendant "thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(2)(A). A CFAA violation is generally a misdemeanor; however, it is punishable as a felony if the offense is "committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 1030(c)(2)(B)(ii).³

An offense under N.J.S.A. 2C:20-31(a) requires three elements to establish a violation: (1) defendant purposely or knowingly accessed data; (2) defendant accessed the data "without authorization, or in excess of authorization;" and (3) defendant "knowingly or recklessly discloses or causes to be disclosed any data . . . or personal identifying information." N.J.S.A. 2C:20-31(a).

³ In this case, the Superseding Indictment alleges that the CFAA violation was in furtherance of a New Jersey felony criminal statute, N.J.S.A. 2C:20-31(a); thus, the offense is elevated to a felony. (Superseding Indictment, Count 1, ¶¶ 5, 27.)

Although there is an overlap of facts for the first two elements of each offense, N.J.S.A. 2C:20-31(a) requires the additional component that defendant “knowingly or recklessly discloses or causes to be disclosed any data . . . or personal identifying information.” Hence, an essential N.J.S.A. 2C:20-31(a) element requires proof of conduct not required for a CFAA offense. The Government specifically alleges in the Superseding Indictment that defendant and his co-conspirators “knowingly disclosed approximately 120,000 stolen ICC-ID/email address pairings for iPad 3G customers . . . to the internet magazine Gawker.” (Superseding Indictment, Count 1, ¶ 27d.) Accordingly, Defendant’s Motion is denied with respect to this argument.

III. Venue in the District of New Jersey For Both Counts of the Superseding Indictment

Defendant contends that this Court lacks jurisdiction over Counts One and Two. In support of his argument, Defendant argues that “no alleged fact which, if ultimately proven, took place in New Jersey.” (Def. Br. 13.)

Count One

In the absence of an express venue provision in a criminal statute, courts determine venue based on the “nature of the crime alleged and the location of the act or acts constituting it.” United States v. Rodriguez-Moreno, 526 U.S. 275, 279 (1999) (internal quotations and citations omitted). Pursuant to 18 U.S.C. § 3237, “any offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed.” For instance, in United States v. Powers, in the context of an alleged violation of the CFAA, “[a]lthough [defendant] may not have been physically present in Nebraska, and the computer used to facilitate the violation was located in Arizona,” venue was proper in the District of Nebraska because defendant’s CFAA violation injured a Nebraska resident and violated

Nebraska tort laws. No. 09-361, 2010 WL 1418172, at *2 (D. Neb. Mar. 4, 2010) (noting that “[v]enue would not only be proper in the District of Arizona where the crime began, but also in the District of Nebraska where the crime was completed”).

The reasoning in Powers is instructive in this case with respect to Count One. Although Defendant was not present in New Jersey and did not gain access to a computer in New Jersey, his alleged CFAA violation, in furtherance of the alleged conspiracy, was completed in New Jersey. Defendant’s purported conduct—knowing disclosure of personal identifying information to the press—affected thousands of New Jersey residents and violated New Jersey law. Similar to the reasoning in Powers, because a defendant can be prosecuted in any district where the crime began, continued, or completed, this Court finds that venue is proper in the District of New Jersey regarding Count One.

Count Two

“Where . . . a defendant is charged with multiple crimes in a single indictment, the government must satisfy venue with respect to each charge.” United States v. Davis, 689 F.3d 179, 185 (2d Cir. 2012). As the Third Circuit has noted, “[t]he locality of a crime for the purpose of venue extends ‘over the whole area through which force propelled by an offender operates.’” United States v. Root, 585 F.3d 145, 156 (3d Cir. 2009) (citing United States v. Johnson, 323 U.S. 273, (1944)).

Section 1028(a)(7) disallows certain conduct “in connection with, any unlawful activity that constitutes a violation of Federal law[.]” Thus, the predicate federal offense is an essential element to a § 1028(a)(7) charge. Accordingly, venue for § 1028(a)(7) violations is likely proper in any district in which venue is proper for the predicate violation of federal law. See e.g., United States v. Magassouba, 619 F.3d 202, 206 (2d Cir. 2010) (holding that “venue properly

lies with respect to an aggravated identity theft offense in any district in which venue lies for the predicate”). The predicate federal offense in this case is Defendant’s alleged CFAA violation. As the CFAA violation is a key factor to the § 1028(a)(7) charge, venue lies in any district where the crime began, continued, or completed. See 18 U.S.C. § 3237(a). Because there is venue in the District of New Jersey for the predicate federal offense—the CFAA violation which is the object of Count One’s conspiracy charge—this Court finds that venue is also proper for Count Two.⁴

IV. Count Two: Improper Violation Under 18 U.S.C. § 1028(a)(7)

The criminal statute at issue in Count Two, 18 U.S.C. § 1028(a)(7), states in pertinent part:

“[w]hoever . . . transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law . . . shall be punished as provided in subsection (b) of this section.”

18 U.S.C. § 1028(a)(7). According to Defendant, the statute requires alleged violations to be “in connection with” a present or future criminal activity and not a past criminal act. (See Def. Br. 16.) Based on this interpretation, Defendant argues that Count Two improperly pleads a § 1028(a)(7) violation because Defendant’s alleged transfer, possession, and use of others’ identification commenced after the CFAA violation was complete. (See Def. Br. 16.)

Defendant’s interpretation of § 1028(a)(7) is contrary to the statute’s legislative history and is unsupported by case law. As the Government points out, Congress amended the statute in

⁴ Although unnecessary to address, the Court acknowledges the Government’s additional venue arguments. The Government argues that venue is proper on both Counts as they charge “continuing” offenses under 18 U.S.C. § 3237(a). (Gov’t Br. 33.) Moreover, according to the Government, “[w]here an offense requires the United States to prove the failure to do or obtain something, that offense may be prosecuted in the district where the failure occurs.” (Gov’t Br. 34.) The Government contends that venue is proper on both Counts as the Government must prove that defendant accessed AT&T’s computers “without authorization” from AT&T or its customers, the victims in New Jersey. (Gov’t Br. 34.)

2004 to include the words “in connection with” to “broaden the reach of section 1028(a)(7).” H.R. Rep. No. 108-528, at 10 (2004), available at 2004 WL 1260964, at *10 (stating that the phrase “in connection with” would serve to “make possible the prosecution of persons who knowingly facilitate the operations of an identity-theft ring . . . but who may deny that they had the specific intent to engage in a particular fraud scheme[, and] it will provide greater flexibility for the prosecution of section 1028(a)(7) offenses”). Neither the face of the statute nor legislative history indicates that the statutory phrase “in connection with” necessitates a temporal restriction for § 1028(a)(7) violations.

Additionally, the two cases to which Defendant cites do not lend support for his argument that the phrase “in connection with” requires an allegation of a present or future crime and not a past crime. See U.S. v. Sutcliffe, 505 F.3d 944, 959 (9th Cir. 2007) (analyzing § 1028(a)(7) violation pursuant to pre-2004 Amendment language which did not include the phrase “in connection with”); U.S. v. Villanueva-Sotelo, 515 F.3d 1234, 1245-46 (D.C. Cir. 2008) (referencing the amended § 1028(a)(7) in passing, but not indicating that Congress intended only to prosecute those engaging in present or future crimes). However, even using Defendant’s interpretation of the statute, the Superseding Indictment alleges that at least part of Defendant’s unauthorized computer access overlapped with his possession and transfer of persons’ identification, from June 2, 2010 through June 15, 2010. (Superseding Indictment, Count 1, ¶ 5; Count 2, ¶ 2.) Accordingly, the Court finds that the Superseding Indictment sufficiently and properly pleads a § 1028(a)(7) violation; thus Defendant’s Motion fails with respect to this argument.

V. Count Two: Violation of the First Amendment

Defendant argues that Count Two violates the First Amendment because it criminalizes Defendant's "transmission of publicly available information on matters of important public concern to the press." (Def. Br. 18.) In further support of his argument, Defendant contends that he "served the public by exposing AT&T's non-existent security and cavalier disregard of its customers' information." (Def. Br. 18.)

As specifically noted in the Superseding Indictment, "[t]he ICC-IDs and iPad user e-mail addresses were not available to the public and were kept confidential by AT&T." (Superseding Indictment, Count 1, ¶ 10; see Count 2, ¶ 1 (incorporating ¶¶ 1-4; 7-27).) The very conduct at issue involves Defendant's allegedly unauthorized access to a protected computer and the subsequent transfer of such confidential information. Additionally, as the Supreme Court has held, "[i]t rarely has been suggested that the constitutional freedom for speech and press extends its immunity to speech or writing used as an integral part of conduct in violation of a valid criminal statute." New York v. Ferber, 458 U.S. 747, 761-62 (1982) (internal citations and quotations omitted). Accordingly, Defendant's Motion fails with respect to this argument.

CONCLUSION

For the reasons stated above, this Court DENIES Defendant's Motion.

s/Susan D. Wigenton, U.S.D.J.

UNITED STATES DISTRICT COURT
District of New Jersey

UNITED STATES OF AMERICA

v.

Case Number 2:11-470-01

ANDREW AUERNHEIMER

Defendant.

JUDGMENT IN A CRIMINAL CASE
(For Offenses Committed On or After November 1, 1987)

The defendant, ANDREW AUERNHEIMER, was represented by Tor B. Ekeland, Esq. (Retained)

The defendant was found guilty on count(s) 1(s), 2(s) by a jury verdict on 11-20-12 after a plea of not guilty. Accordingly, the court has adjudicated that the defendant is guilty of the following offense(s):

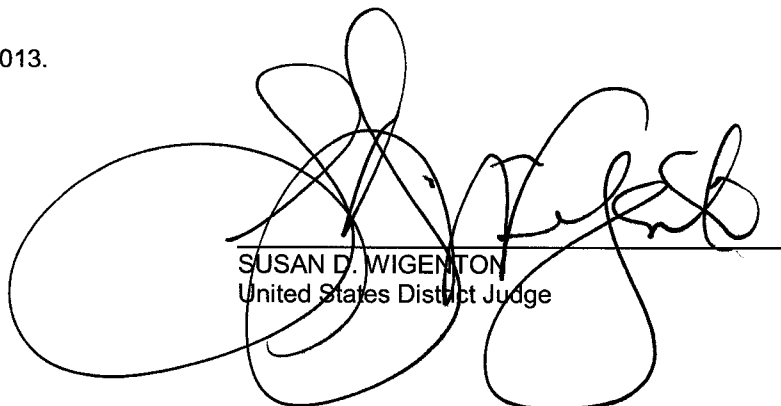
<u>Title & Section</u>	<u>Nature of Offense</u>	<u>Date of Offense</u>	<u>Count Number(s)</u>
18:371	CONSPIRACY TO ACCESS A COMPUTER WITHOUT AUTHORIZATION	6/2/2010-6/15/2010	1(s)
18:1028(a)(7) and 2	FRAUD IN CONNECTION WITH PERSONAL INFORMATION	6/2/2010-6/15/2010	2(s)

As pronounced on 3/18/13, the defendant is sentenced as provided in pages 2 through 7 of this Judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

It is ordered that the defendant shall pay to the United States a special assessment of \$200.00, for count(s) 1(s), 2(s), which shall be due immediately. Said special assessment shall be made payable to the Clerk, U.S. District Court.

It is further ordered that the defendant shall notify the United States Attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this Judgment are fully paid. If ordered to pay restitution, the defendant shall notify the court and United States Attorney of any material change in the defendant's economic circumstances.

Signed this the 19th day of March, 2013.



 SUSAN D. WIGENTON
 United States District Judge

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a term of 41 Months on each of Counts 1(s) and 2(s) to run concurrently.

The defendant is remanded to the custody of the United States Marshal.

RETURN

I have executed this Judgment as follows:

Defendant delivered on _____ to _____
at _____, with a certified copy of this Judgment.

United States Marshal
By _____
Deputy Marshal

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be placed on supervised release for a term of 3 years on each of Counts 1(s) and 2(s) to run concurrently.

Within 72 hours of release from custody of the Bureau of Prisons, the defendant shall report in person to the Probation Office in the district to which the defendant is released.

While on supervised release, the defendant shall comply with the standard conditions that have been adopted by this court as set forth below.

The defendant shall submit to one drug test within 15 days of commencement of supervised release and at least two tests thereafter as determined by the probation officer.

If this judgment imposes a fine, special assessment, costs, or restitution obligation, it shall be a condition of supervised release that the defendant pay any such fine, assessments, costs, and restitution that remains unpaid at the commencement of the term of supervised release and shall comply with the following special conditions:

ALCOHOL/DRUG TESTING AND TREATMENT

You shall refrain from the illegal possession and use of drugs, including prescription medication not prescribed in your name, and the use of alcohol, and shall submit to urinalysis or other forms of testing to ensure compliance. It is further ordered that you shall submit to evaluation and treatment, on an outpatient or inpatient basis, as approved by the U.S. Probation Office. You shall abide by the rules of any program and shall remain in treatment until satisfactorily discharged by the Court. You shall alert all medical professionals of any prior substance abuse history, including any prior history of prescription drug abuse. The Probation Officer shall supervise your compliance with this condition.

COMPUTER MONITORING

You shall submit to an initial inspection by the U.S. Probation Office, and to any unannounced examinations during supervision, of your computer equipment. This includes, but is not limited to, personal computer, personal digital assistants, entertainment consoles, cellular telephones, and/or any electronic media device which is owned or accessed by you. You shall allow the installation on your computer of any hardware or software systems which monitor computer use. You shall pay the costs of the computer monitoring program. You shall abide by the standard conditions of computer monitoring. Any dispute as to the applicability of this condition shall be decided by the Court.

MENTAL HEALTH TREATMENT

You shall undergo treatment in a mental health program approved by the United States Probation Office until discharged by the Court. As necessary, said treatment may also encompass treatment for gambling, domestic violence and/or anger management, as approved by the United States Probation Office, until discharged by the Court. The Probation Officer shall supervise your compliance with this condition.

NEW DEBT RESTRICTIONS

You are prohibited from incurring any new credit charges, opening additional lines of credit, or incurring any new monetary loan, obligation, or debt, by whatever name known, without the approval of the U.S. Probation Office. You shall not encumber or liquidate interest in any assets unless it is in direct service of the fine and/or restitution obligation or otherwise has the expressed approval of the Court.

SELF-EMPLOYMENT/BUSINESS DISCLOSURE

You shall cooperate with the U.S. Probation Office in the investigation and approval of any position of self-employment, including any independent, entrepreneurial, or freelance employment or business activity. If approved for self-employment, you shall provide the U.S. Probation Office with full disclosure of your self-employment and other business records,

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

including, but not limited to, all of the records identified in the Probation Form 48F (Request for Self Employment Records), or as otherwise requested by the U.S. Probation Office.

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

STANDARD CONDITIONS OF SUPERVISED RELEASE

While the defendant is on supervised release pursuant to this Judgment:

- 1) The defendant shall not commit another federal, state, or local crime during the term of supervision.
- 2) The defendant shall not illegally possess a controlled substance.
- 3) If convicted of a felony offense, the defendant shall not possess a firearm or destructive device.
- 4) The defendant shall not leave the judicial district without the permission of the court or probation officer.
- 5) The defendant shall report to the probation officer in a manner and frequency directed by the Court or probation officer.
- 6) The defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer.
- 7) The defendant shall support his or her dependents and meet other family responsibilities.
- 8) The defendant shall work regularly at a lawful occupation unless excused by the probation officer for schooling, training, or other acceptable reasons.
- 9) The defendant shall notify the probation officer within seventy-two hours of any change in residence or employment.
- 10) The defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute or administer any narcotic or other controlled substance, or any paraphernalia related to such substances.
- 11) The defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered.
- 12) The defendant shall not associate with any persons engaged in criminal activity, and shall not associate with any person convicted of a felony unless granted permission to do so by the probation officer.
- 13) The defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view by the probation officer.
- 14) The defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer.
- 15) The defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court.
- 16) As directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics, and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.
- (17) You shall cooperate in the collection of DNA as directed by the Probation Officer.

(This standard condition would apply when the current offense or a prior federal offense is either a felony, any offense under Chapter 109A of Title 18 (i.e., §§ 2241-2248, any crime of violence [as defined in 18 U.S.C. § 16], any attempt or conspiracy to commit the above, an offense under the Uniform Code of Military Justice for which a sentence of confinement of more than one year may be imposed, or any other offense under the Uniform Code that is comparable to a qualifying federal offense);

- (18) Upon request, you shall provide the U.S. Probation Office with full disclosure of your financial records, including co-mingled income, expenses, assets and liabilities, to include yearly income tax returns. With the exception of the financial accounts reported and noted within the presentence report, you are prohibited from maintaining and/or opening any additional individual and/or joint checking, savings, or other financial accounts, for either personal or business purposes, without the knowledge

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

and approval of the U.S. Probation Office. You shall cooperate with the Probation Officer in the investigation of your financial dealings and shall provide truthful monthly statements of your income. You shall cooperate in the signing of any necessary authorization to release information forms permitting the U.S. Probation Office access to your financial information and records;

- (19) As directed by the U.S. Probation Office, you shall participate in and complete any educational, vocational, cognitive or any other enrichment program offered by the U.S. Probation Office or any outside agency or establishment while under supervision;
- (20) You shall not operate any motor vehicle without a valid driver's license issued by the State of New Jersey, or in the state in which you are supervised. You shall comply with all motor vehicle laws and ordinances and must report all motor vehicle infractions (including any court appearances) within 72 hours to the U.S. Probation Office;

For Official Use Only - - - U.S. Probation Office

Upon a finding of a violation of probation or supervised release, I understand that the Court may (1) revoke supervision or (2) extend the term of supervision and/or modify the conditions of supervision.

These conditions have been read to me. I fully understand the conditions, and have been provided a copy of them.

You shall carry out all rules, in addition to the above, as prescribed by the Chief U.S. Probation Officer, or any of his associate Probation Officers.

(Signed) _____
Defendant Date

U.S. Probation Officer/Designated Witness Date

Defendant: ANDREW AUERNHEIMER
Case Number: 2:11-470-01

RESTITUTION AND FORFEITURE

RESTITUTION

The defendant shall make restitution in the amount of \$73,167. The Court will waive the interest requirement in this case. Payments should be made payable to the **U.S. Treasury** and mailed to Clerk, U.S.D.C., 402 East State Street, Rm 2020, Trenton, New Jersey 08608, for distribution to AT&T, Attn: Security Office 340 Mount Kemble Avenue - N-315 Morristown, NJ 07960.

The restitution is due immediately and shall be paid in full within 30 days of sentencing.

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) community restitution, (6) fine interest, (7) penalties, and (8) costs, including cost of prosecution and court costs.