IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA TALLAHASSEE DIVISION

UNITED STATES OF AMERICA

v. **CASE NUMBER: 4:15cr33-RH**

MICHAEL DANIEL RUBENS
_____/

STATEMENT OF FACTS

The Defendant admits that were this case to proceed to trial, the government could prove the following facts beyond a reasonable doubt:

1.) Introduction

Beginning in 2012 and continuing until January 2015, Michael Daniel Rubens engaged in a pattern of publicly humiliating dozens of young women by (1) hacking into their email accounts, social media accounts, and other accounts, (2) stealing nude and clothed photographs and other personal information, (3) using the photographs to create pornography, and (4) posting the pornographic images on the social media websites and a revenge pornography website that was recently shut down by the FBI. Rubens engaged in most of the conduct from his residence in Tallahassee, but he used an onion router (also known as an IP address anonymizer) on occasion to conceal his conduct and his whereabouts.

2.) Conduct directed at M.R.

On December 12, 2012, M.R., a student at Florida State University, went to the Florida State University Police Department ("FSUPD") to report that an unknown

person(s) compromised her Florida State University ("FSU") Blackboard email account and repeatedly changed her password to prevent her from accessing the account (a/k/a "denial of service" attack). M.R.'s account was hacked multiple times between July 29, 2012, and December 12, 2012, to change M.R.'s password. FSU records indicate that on three occasions, the account was accessed through an IP address assigned by an Onion Router IP anonymizer, and on two occasions, the account was accessed from a computer using Comcast IP address of 98.230.41.169. On or around December 9, 2012, shortly after a password change was made from an onion router assigned anonymous IP address, someone used M.R.'s account to send emails to M.R.'s sister and boyfriend asking for "Sexy pictures". FSUPD preserved a copy of one such email from M.R.'s account.

In addition, M.R. stated that she was an employee of Harry's Restaurant in Tallahassee between March 2012 and September 2012. While M.R. was employed there, someone gained access to Harry's Facebook page and posted a picture of M.R. in her bikini with a caption inviting customers to come to Harry's for happy hour and oral sex provided by M.R. M.R. stated several of her friends and coworkers saw the image, and she had to go to her employer, Harry's, to ask them to remove the embarrassing photograph. Investigators were unable to recover the image or identify an IP address from which the image was posted.

In response to a subpoena, Comcast provided subscriber information regarding the user of IP address 98.230.41.169 (the "Home IP Address") between July 29, 2012, and December 12, 2012. The records indicate the IP was assigned to a residential high-speed internet account in the name of "SEMINOLE APTS 418 BULK DUAL HSI

ACCT," which is located at Seminole Ridge Apartments on Pullen Road in Tallahassee. According to Comcast records, Rubens was also utilizing the same IP address from July 12, 2014, until January 7, 2015. The manager of Seminole Ridge Apartments stated that the only resident of Apartment 418 during that time period was Michael Rubens.

M.R. recognized Rubens as a regular patron of Harry's Seafood Bar and Grill. Rubens typically sat alone at the bar and often used coupons when paying for his food.

On March 14, 2013, an FSUPD officer executed a search warrant for Ruben's residence and seized a Blackberry 8900 AT&T phone, an Apple iPad 16gb (S/N DKWGQ0M4DFHM) and an Apple MacBook Pro (S/N W89481QM7XK), Compact Disks, Floppy Disks, Thumb Drives, and SD Cards. Rubens was the sole occupant of the apartment. A detective with the Leon County Sheriff's Office ("LCSO") conducted forensic examinations on these devices.

A forensic examination of Ruben's MacBook Pro revealed that there were two user profiles on the computer, one for "mikerubens" and one for "stevewilson". Investigators believe that "stevewilson" is a fictitious name used by Rubens. The "mikerubens" account had numerous search queries related to M.R. in its internet history folders. Rubens' MacBook contained 470 files with over 5,000 references to M.R. The searches appeared to be focused on finding personal identifying information for M.R., such as past addresses, family information, and other information that could be used as answers to security questions. Among other things, the detective also found an archived web page from M.R.'s FSU identity management account showing that Rubens had logged in to M.R.'s account. There was also an archived "reset password" web page for

M.R.'s account, which indicates the computer was used to access M.R.'s FSU account for the purpose of resetting her password. To reset M.R.'s password, Rubens had to use either (1) M.R.'s user ID and existing password or (2) M.R.'s FSU Card number and social security number.

The detective found evidence that the computer was used to hack at least two of M.R.'s email accounts. One of those accounts was the AOL email account that M.R. had since she was eight years old.

M.R. described 2012 as a very difficult year of her life. Because Rubens was hacking into her personal email accounts, she became afraid to do anything online, and described the series of incidents as "very disturbing" and "terrifying." She lost the ability to use an email account that she had since she was eight years old. She said the incident on Harry's Facebook account was very embarrassing. She said that the harassment continued even until September 10, 2014, when Rubens sent a message to her boyfriend from M.R.'s Instagram account regarding "sexy" pictures. Instagram records show that Rubens logged into M.R.'s account from his Home IP address multiple times on September 10, 2014. Rubens continued to conduct web searches for information related to M.R. on his new iPad until at least December 29, 2014.

3.) Conduct directed at A.D. and L.B.

Investigators interviewed A.D., who stated that she had been the victim of cyber stalking beginning in or before 2012 and continuing until 2014. A.D. worked at Altrua Marketing for a period of time until 2011. Altrua has an office in the same building as Rubens' employer, Gexpro Services, Inc., in Tallahasse, Florida. A.D. does not know

Rubens, but may have bumped into him in the building where they worked. She recalls that she first found out that someone had hacked her yahoo.com email account when her mother received an email message from A.D.'s email account with a picture of A.D. in blue lingerie attached.

In the fall of 2011, A.D. received an odd message from her sister-in-law, L.B., through Facebook. L.B. advised that she did not send the message. A.D. concluded that L.B.'s Facebook account had been hacked. Indeed, Facebook records reveal that on January 4, 2012, Rubens changed L.B.'s password from his Home IP Address.[1]

In October 2012, A.D. did a Google search of her name and was shocked to see that her name was associated with the website pinkmeth.com.[2] A.D. stated that she clicked on the link and found that someone had posted nude images of her, along with her name, telephone number, address, and resume. Some of the images were photographs she had taken of herself and sent to her husband while he was deployed overseas in the United States Military in 2007. A.D. stated the photographs were private and only meant for her husband. She advised that the photographs were stolen from one of her yahoo.com email accounts, which is the email account she had used to send the

[1] At that time, a Facebook password reset required the user to answer two security questions, and then a new temporary password would be emailed to the account-holder's primary email address.

[2] Pinkmeth.com was a darknet website wherein users commonly posted or sold pornography of ex-girlfriends or ex-wives as a means of revenge for something they had done. The site was shut down in the fall of 2014 as a result of an investigation by law enforcement.

photographs to her husband. She has never shared them with anyone other than her husband. A.D.'s husband has never shared the images with anyone.

A.D. stated that the images from pinkmeth.com have been replicated and appear on numerous websites under her real name. She has attempted to ask various websites to remove the pictures, but she has not been successful because the pictures are continuously reposted to new websites. If she conducts a search query for her name on Google.com, the first search results that appear are links to her photographs on pornographic websites.

A.D. determined from her yahoo.com email account login history that her primary yahoo.com email account was hacked 14 times between May 23, 2012, and March 8, 2013.

Investigators found numerous web searches on Rubens' electronic devices using terms associated with A.D. These web searches are consistent with someone who is engaging in social hacking.[3] In fact, the detective found evidence that Rubens' computer contained answers to security questions for his victims (e.g. what is the name of your first pet?). The investigators found web strings and other data that prove that computer was used to log in to both of A.D.'s Yahoo email accounts.

[3] "Social or human hackers specialize in exploiting personal connections through social networks. Social hackers, sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or online). By exploiting a victim's personal connections, the hacker is able to gain information about the victim that the hacker can then use to answer security questions that permit the hacker to "reset" the victim's password to a particular account. Evidence found on Rubens' electronic devices suggests that he was primarily a "social hacker."

In addition, on his iPad, Rubens saved screen shots of Facebook account pages of L.B. and A.D.[4] On L.B.'s Facebook page, Rubens captured a post while he was logged in to L.B.'s Facebook page that contained a blue lingerie picture of A.D. with the caption "My sister-in-law showing you what Halloween is all about." A.D. states that this occurred in or around October 2012. Rubens also had screenshots of A.D.'s homepage on Facebook showing that A.D. was tagged in the photo Rubens posted on L.B.'s account.

On Rubens' iPad, Investigators also found screen shots of photograph collages of A.D. posted on two websites: 4chan and on pinkmeth. The collages consisted of various images of A.D. clothed and unclothed, including the nude images stolen from A.D.'s yahoo email account. EXIF data from the collages indicated that they were made on Rubens' computer using Adobe Photoshop between 2012 and 2013. Rubens also saved copies of private email conversations between A.D. and her husband regarding the images that A.D. was sending to her husband. The conversations were extremely personal in nature. A.D. indicates that these emails were stolen from her Yahoo email account. Investigators also found a saved copy of an online invoice for the purchase of lingerie from Victoria's Secret that A.D. made in February of 2008. Investigators found a wide range of personal information belonging to A.D. on Rubens' devices (resumes, cover letters, etc.).

[4] Rubens appeared to save screen shots of his stalking/hacking work. Many of the screen shots reflect the reactions of others to the photographs he was posting.

In late 2012, A.D. was working for Adventure Products. On Adventure Products' online blog, A.D. states that someone commented on Rubens' pornographic collage photos of her by stating "Damn (A.D.) your ass is fucking H.O.T. girl. I would bang you so hard." This occurred on October 18, 2012. The photos have also been reposted to other pornography sites, and even to this day, a Google search of A.D.'s name results in multiple links to pornography sites in the first page of search results. A.D. reports that "knowing that strangers are viewing her pictures and making comments like 'I came buckets,' 'Destroy this slave,' and 'I would bang you so hard' has been damaging." She states that she has felt helpless at times, and the public nature of the photos makes her feel like there is a scarlet letter attached to her name online. Although she would not have gone through with it, she even had suicidal thoughts in 2012 and 2013. When she talks about the traumatic experience, it is difficult for her not to break down into tears.

Evidence from Rubens' newest iPad seized incident to arrest and searched pursuant to state search warrant shows that he continued to stalk A.D. after March 2013. His internet history showed multiple web searches for information about A.D. (as well as M.R.) on December 29, 2014. His new iPad contained several saved search results from Intelius that included name, address, email address, telephone numbers, and familial information for A.D. and L.B. In addition, he had more photographs of A.D. on his new iPad, which suggests his stalking was ongoing until December 29, 2014.

4.) Conduct relating to M.P.T. and B.W.

In 2012, M.P.T. worked for General Dynamics in Tallahassee, Florida. General Dynamics is a client of Ruben's employer, Gexpro Services, Inc., which is a supply chain

management company. M.P.T. advised an FSUPD investigator she had been severely victimized by an unidentified cyber stalker since 2012. M.P.T. advised that the cyber stalking became so frequent she had to delete all of her email accounts and social media accounts. Once the accounts were deleted, the cyber-stalker reactivated some of the accounts without authorization and continued to send messages to her friends. The messages often contained pornographic images of M.P.T. that appeared to be altered photos that were stolen from M.P.T.'s social media accounts. M.P.T. also reported that her and her friend's Facebook accounts were compromised as well.

M.P.T. advised that, in or around October 2012, the cyber stalker posted altered pornographic images on B.W.'s Facebook account and other social media websites. B.W. is M.P.T.'s friend on Facebook. M.P.T. advised she still frequently checks the internet and social media websites for fraudulent profiles and altered images that depict her. M.P.T. advised she has spent a lot of time and money attempting to repair the damages to her reputation caused by the cyber-stalker.

M.P.T. even went to the trouble of hiring a private investigator who specialized in computer crimes to determine who the stalker was. The private investigator determined the cyber-stalker had hacked M.P.T.'s old yahoo.com email address on August 4, 2014, and August 5, 2014. The cyber-stalker sent M.P.T.'s friend a message asking for pictures of M.P.T. The friend who was contacted thought the message was suspicious so she called M.P.T. to inquire about the message. M.P.T. notified the private investigator about the fraudulent activity and asked her to investigate the incident. The investigator

obtained IP information from Yahoo and learned that Rubens had hacked M.P.T.'s Yahoo account from his Home IP Address.

The detective who examined Rubens' MacBook seized in March 2013 found M.P.T.'s name and other personal information on Rubens' MacBook. The files on Rubens' devices show that he was surveilling M.P.T. for a long period of time, stealing personal photographs from her, and manipulating the photographs using Adobe Photoshop.

Rubens' internet history revealed that he accessed M.P.T.'s Yahoo and Gmail accounts without authorization, which would have required Rubens to obtain and use M.P.T's username and password. Moreover, on Rubens' Apple iPad, the detective found images of M.P.T. in her wedding dress and digitally altered versions of those images. The altered images depict M.P.T. posing in her undergarments at her wedding. EXIF data shows that Adobe Photoshop was used to modify the images on October 2, 2012. The detective also found a saved screenshot on Rubens' iPad showing that he was logged into M.P.T.'s facebook account when he posted a collage of the aforementioned photos onto her Facebook account for her friends to see. This occurred in October 2012. Numerous files on Rubens' devices show that he was collecting user names and passwords for social media, dental insurance, and other online accounts belonging to M.P.T.

Moreover, the detective located a screenshot on Rubens' older iPad depicting Rubens logged into the Facebook account of M.P.T.'s friend, B.W. The screenshot

shows that Rubens posted a digitally modified image showing M.P.T. performing oral sex. It is unknown when this photo was posted and deleted.

Facebook records reveal that Rubens hacked into B.W.'s Facebook account on August 13, 2014, and received multiple private messages from M.P.T., wherein M.P.T. asks if B.W. had posted any photos from M.P.T.'s bachelorette party. On January 3, 2015, M.P.T. contacted FSUPD again and advised that a cyber-stalker hacked her Snapchat account and sent out pictures of her in a bikini. In response to a subpoena, Snapchat confirmed that Rubens' Home IP Address was used to log in to M.P.T.'s Snapchat account (Snapchat does not retain dates associated with the log in). Photographs of M.P.T. in a bikini were found on Rubens' new iPad that was seized incident to his arrest.

M.P.T. states that what Rubens did to her was devastating. She knew Rubens from her job, but only in passing. They had never been friends. She said the stalking made her distrust everyone around her. She has completely eradicated her social media presence, which has caused her to lose contact with longtime friends. The pornographic photos posted to B.W.'s account and to the account of M.P.T.'s sister insinuated that M.P.T. had cheated on her husband. She said that for a brief period of time, the photos made her husband distrustful of her.

5.) Conduct relating to P.L., L.L., and B.K.

P.L. worked at Altrua Global Solutions in Tallahassee, Florida, from May 2007 until December 2013. P.L. advised that two of her email accounts were hacked in 2012,

and the hacker reset P.L.'s password to prevent her from logging back in to her own account.

P.L. advised that photographs of her were taken from her accounts, digitally altered, and then posted to her the Facebook page of her mother, L.L. P.L. was tagged in the photographs. One such photograph is a collage of P.L. in an FSU branded bathing suit and in the other half of the collage, she is in business clothes at standing next to the BCS national championship trophy. The caption posted by Rubens says "Nole Pride." In another image posted by Rubens, P.L. is in the bathtub. According to P.L., this image was stolen from P.L.'s husband's (B.K.) Hotmail email account. Rubens' laptop had a data string in unallocated space associated with a login to the Hotmail account with a time stamp of August 3, 2012.

In yet another screenshot showing Rubens logged into L.L.'s Facebook account, he posted another collage of P.L. in her bathing suit with the caption, "Please vote for the best marketing campaign." Another screen shot was taken while Rubens was logged into P.L.'s Facebook page posting a similar collage with the caption "Which outfit do I wear tomorrow?" Similarly, Rubens had a screen shot of a collage he posted on P.L.'s LinkedIn account, which was dated September 19, 2012. This screenshot shows that Rubens was logged into P.L.'s LinkeIn account at the time the picture was posted. Rubens' MacBook also had data fragments showing that it had been used to change the password on L.L.'s aol.com email account.

Finally, Rubens new iPad contained search strings dated January 12, 2015, showing that he was still searching for information related to P.L.

P.L. described the stalking as terrifying and embarrassing.

6.) Conduct relating to N.L. and J.L.

Investigators interviewed N.L. N.L. is a nurse who works with T.F. (also a nurse) at a hospital near Boston Massachusetts. T.F. dated Rubens while the two were in college at Syracuse University around 10 years ago. T.F. and Rubens have maintained their friendship since that time. In August or September of 2009, a group of female nurses in Boston, including T.F. and N.L. took a pole-dancing class for fun. Several revealing photographs were taken of N.L. by others during the class.

Beginning in late 2011, N.L. began receiving notifications from Yahoo that someone was trying to change her password. These notifications continued until approximately May 2012. In early May 2012, N.L.'s friend, M.P., received an email she believed to be sent by T.F. requesting photographs of the pole dancing class. M.P. sent the photographs as requested on May 7, 2012. Data from Rubens' devices shows that he was searching for information on M.P. using personal history websites, such as Piplsearch.

On or about May 23, 2012, Rubens posted a collage of N.L., M.P., and T.F. on N.L.'s Facebook page. The collage consisted of images from the pole dancing class. N.L. states that M.P. and T.F. were tagged. N.L. deleted the image the following morning. Investigators found the photo-shopped collage and its individual images on Rubens' iPad. Rubens also took a screenshot of the reactions he received on 4chan when he posted the collage on that site and asked users their opinion of M.P.

On September 16, 2012, M.P. and her husband received messages from N.L.'s Facebook account stating that N.L. had a question. N.L. did not send these messages.

On or about October 10, 2012, Rubens used an onion router IP anonymizer to change the password on the Facebook account of N.L.'s sister, J.L. On or about October 13, 2012, Rubens hacked into J.L.'s Facebook account and posted a photograph of N.L. The photograph was a collage consisting of two images. One of the images depicted N.L. fully clothed and the other image was a digitally altered image depicting a female performing oral sex on a male. Rubens represented both images to be N.L. by posting a tagline next to the photograph that said, "Late night eats :) #stuffed with (N.L.)." Rubens captured a screenshot of the post and the responses it generated and saved it to his Apple iPad, which investigators found when examining the data from the iPad. Within minutes of posting the image, Rubens logged into N.L.'s Facebook account and posted a message about the picture to make the picture appear authentic. Investigators found a screen shot of Rubens logged into N.L.'s Facebook account on Rubens' old iPad.

Rubens continued to harass N.L. until December 27, 2014, when another pole dancing class image of N.L. was posted on J.L.'s snapchat account with the caption, "North Pole Dancer (N.L.) can get low." These images and related collages were also found on Rubens' new iPad after his arrest. Rubens' newer iPad contained numerous photographs of all of the young women referenced above, as well as saved Intelius searches with their addresses, phone numbers, and email addresses. Most of this information was obtained in 2014.

Rubens hacked N.L.'s brother's account and had a sexually explicit conversation with N.L.'s 15 year old nephew and showed him the digitally altered image of N.L. performing oral sex.

N.L. states that being stalked by Rubens has been highly distressing. She feels awkward being around her nephew now. She has filed multiple police reports and has been frustrated by the slow progress of the investigation by Boston area law enforcement. For over a year, she went to work believing her stalker was someone she worked with. It made her feel very uncomfortable.

7.) Conduct Relating to J.M. and K.T.

J.M. and K.T. were Rubens' high school classmates. She knew Rubens in high school, but they never spoke. Rubens began stalking J.M. on or about September 22, 2012. For the next month, Rubens hacked into email and social media accounts of K.T. and B.D., also a friend of J.M. Evidence of Rubens' hacks into these accounts was found on his electronic devices. The purpose of the hacks was to request photographs of J.M. from her family friends and to seek information about J.M., such as her childhood pet's name. On October 13, 2012, Rubens posted a collage on K.T.'s Facebook wall, which consisted of two images of J.M. fully clothed and one image of J.M. in her underwear. Investigators found screen shots from K.T.'s Facebook page on Rubens' old iPad showing that Rubens was signed into K.T.'s Facebook account when he posted the collage. Rubens also had all of the images he used to create the collage saved separately on his old iPad.

Rubens' iPad also contained a saved screen shot on October 14 showing a post by J.M. wherein J.M. states:

> Stalker alert: Friends, for the past 4 weeks, someone has been trying to access my personal information and pictures by impersonating a friend whose accounts they've hacked. They have impersonated my friend in at least 4 conversations, collecting photos of me and answers to my security questions (e.g. name of my first pet). Last night, they posted an inappropriate fake photoshopped photo of me on my friend's Facebook account. This is clearly unacceptable on all levels and illegal. So I ask:
>
> (1) If you've been contacted in the past month by anyone asking questions about me please let me know asap, and
>
> (2) If you have the photos that were posted last night, please send them to me (no judgments). To pursue legal action, we need as much info as possible.

Rubens continued to stalk J.M. and her friends through at least January 1, 2015, as reflected in the numerous searches and saved information relating to them that was found on Rubens' new iPad after his arrest. Both J.M. and K.T. have been distraught by Rubens' conduct.

Rubens also took a screen shot of an order confirmation from Gap while he was signed into J.M.'s consumer account for Gap. The order confirmation reflected an order made by J.M. on December 10, 2014. Rubens also took a screenshot while logged into the Yahoo email account of J.M.'s friend, B.D., on December 27, 2014. The screen shot shows a Christmas shopping list made by B.D.

J.M. has stopped using Facebook, and is now suspicious of everything she does online. She says the fact that he was able to have conversations with five of her friends through her Facebook account and K.T.'s Facebook account was extremely

"disconcerting" because he successfully obtained personal information about her. She feels like her most personal information is not safe anywhere or with anyone.

8.) Conduct relating to B.M.

B.M. works for the same company as Rubens did. B.M. works in Dallas, Texas. She has never been to Tallahassee, but she worked on a team with Rubens and had talked to him by telephone on numerous occasions. On January 23, 2015, B.M. was interviewed by an FSUPD investigator. B.M. stated that her mother's Facebook account was hacked on or about March 5, 2013. She says her mother's Facebook account is actually an account dedicated to her mother's pet dog. Three images were uploaded to an album entitled "B.M.'s Honeymoon" with the caption "Found ur pics, Sis. Lol yum". The images consisted of the following:

- Image 1: Bathing suit/Beach picture of B.M. and her on their honeymoon, which was an authentic image that was taken from my B.M.'s Facebook page.
- Image 2: B.M.'s head is photoshopped onto someone's body performing a sexual act; and
- Image 3: The upper part of B.M's face is photoshopped onto someone's mouth performing a sexual act.

On October 27, 2014, B.M. was unable to login to her Gmail account. The password had been changed.

On November 10, 2014, B.M.'s Facebook account was hacked. Two private messages were sent to B.M.'s co-worker, K.S. The first message contained a fake swimsuit calendar from the company for which B.M. works, Gexpro Services. The fake calendar contained photoshopped pictures of a coworker, L.L. The photo shopped image was found on Rubens' iPad. Based on EXIF data associated with the image, Rubens created the image with Adobe Photoshop on April 9, 2013. Rubens used images from B.M's Facebook page as well as images from Gexpro's public drive.

When K.S. and L.L. confronted B.M. about the incident, B.M. denied sending the message, but K.S. and L.L. did not believe B.M. was telling the truth. Accordingly, they reported B.M. to Gexpro's human resources department. The human resources department conducted an investigation into B.M.'s alleged conduct. B.M. was out on maternity leave at the time (otherwise, she may have been suspended), but she says she was viewed as a pervert by co-workers, and she and K.S. and L.L. are no longer on friendly terms. She says the intrusion into her life by Rubens has left her disgusted, angry, and confused.

Rubens' MacBook contained evidence of numerous name searches, username searches, and other web-related searches for B.M.'s maiden name.

In addition, on December 27, 2014, B.M. reports that someone posted partially nude photoshopped images of her on her Instagram account. Investigators found a screen shot of the post saved on Rubens' new iPad, which reflected that he was logged into B.M.'s account. The new iPad had dozens of photographs of B.M. and L.L.

ELEMENTS

The elements of a violation of 18 U.S.C. §§ 2261A(2) and 2261(b)(5) (stalking), which are applicable to Counts One through Seven of the Indictment, are as follows:

(1) The Defendant used an interactive computer service, or any electronic communication service or electronic communication system of interstate commerce to engage in a course of conduct;

(2) The course of conduct caused, attempted to cause, or would reasonably be expected to cause substantial emotional distress to another person ; and

(3) The defendant intended to:

a. kill, injure, harass the person;

b. place the person under surveillance with intent to kill, injure, harass, or intimidate that person; or

c. cause substantial emotional distress to the person

The elements of a violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii) (felony unauthorized access of a protected computer), which are applicable to Counts Eight through Twelve:

(1) The defendant intentionally accessed a computer without authorization;

(2) As a result of his intentionally accessing the computer, the defendant obtained information;

(3) The computer being accessed was used in or affected interstate commerce (e.g., it was connected to the internet); and

(4) The defendant accessed the information in furtherance of a criminal or tortious act in violation of the laws of the United States or of any State.

The elements of a violation of 18 U.S.C. § 1028A(a)(1) (aggravated identity theft), which are applicable to Count Thirteen of the Indictment, are as follows:

(1) The Defendant knowingly transferred, possessed, or used another person's means of identification;

(2) The Defendant did so without lawful authority;

(3) The Defendant knew the means of identification belonged to an actual person; and

(4) The Defendant did so during and in relation to a violation of 18 U.S.C. §§ USC 1030(a)(2)(C) and (c)(2)(B)(ii) (felony unauthorized access to a protected computer).

_____
Tor Friedman
Attorney for Defendant

_____
Date

_____
Michael Daniel Rubens
Defendant

_____
Date

CHRISTPHER P. CANOVA
Acting United States Attorney

_____
Jason S. Beaton
Florida Bar No. 0040652
Assistant United States Attorney
Northern District of Florida
401 SE First Ave, Suite 211
Gainesville, Florida 32601
Telephone: (352) 378-0996
Facsimile: (352) 337-2653

_____
Date