Approved: _____
Rosemary Nidiry
Assistant United States Attorney

Before: HONORABLE SARAH NETBURN
United States Magistrate Judge
Southern District of New York

13 MAG 1313

| | |
|---|---|
| UNITED STATES OF AMERICA | SEALED COMPLAINT |
| - v. - | |
| EDWIN VARGAS, | Violations of 18 U.S.C. § 1030 |
| Defendant. | COUNTY OF OFFENSE: Bronx |

SOUTHERN DISTRICT OF NEW YORK, ss.:

SAMAD D. SHAHRANI, 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 April 2010, up to and including in or about October 2012, in the Southern District of New York and elsewhere, EDWIN VARGAS, 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)(2)(C).

2. It was a part and object of the conspiracy that EDWIN VARGAS, the defendant, and others known and unknown, would and did intentionally access a computer without authorization and exceed authorized access, to wit, VARGAS paid certain e-mail hacking services to hack into numerous e-mail accounts which did not belong to him in order to obtain the log-in credentials for those accounts.

OVERT ACT

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 by EDWIN VARGAS, the defendant:

a. In or about March 2011, VARGAS provided an e-mail hacking service with proof of payment in order to obtain the password and username which he had ordered from the e-mail hacking service for an e-mail account to which he did not have authorized access.

b. On or about June 18, 2012, VARGAS accessed a victim's e-mail account ("Victim 1's E-mail Account") without authorization, from the Bronx, New York.

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

COUNT TWO
**(Unauthorized Access of Law Enforcement Database)**

4. On or about November 5, 2011, in the Southern District of New York, EDWIN VARGAS, the defendant, intentionally and knowingly accessed a computer without authorization and exceeded authorized access and thereby obtained information from a department and agency of the United States, to wit, VARGAS accessed, and obtained information from the federal National Crime Information Center ("NCIC") database, without authorization, and exceeding the scope of his authority.

(Title 18, United States Code, Section 1030(a)(2)(B).)

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

5. I have been a Special Agent with the FBI for approximately one year. Prior to being a Special Agent I was a police officer in Indiana for six years. I am presently assigned to the Cyber Criminal Intrusion Squad of the FBI's New York Field Office. I have conducted investigations into computer hacking and related crimes and am familiar with the ways in which such crimes are commonly conducted.

6. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents and other individuals, and my examination of reports and records. 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, except where otherwise indicated.

## Overview

7. Through conversations with representatives of the New York Police Department ("NYPD") and reviewing documents provided by the NYPD, I have learned that EDWIN VARGAS, the defendant, is a detective with the NYPD assigned to a precinct in the Bronx.

8. As set forth in greater detail below, EDWIN VARGAS, the defendant, hired e-mail hacking services to hack into various e-mail accounts so he could obtain log-in credentials, such as the password and username, for those accounts. In total, VARGAS ordered hacks of at least 43 personal e-mail accounts belonging to at least 30 different individuals including 21 who are affiliated with the NYPD; of those 21, 19 are current NYPD officers, one is a retired NYPD officer, and one is current NYPD administrative staff. VARGAS accessed at least one personal e-mail account belonging to a current NYPD officer after receiving the account's log-in credentials from the hacking service. VARGAS also accessed the NCIC database, a federal database, to obtain information about at least two of those NYPD officers without authorization to do so.

## VARGAS's E-mail Hacking Activities

9. Based on my training and experience and involvement in this investigation, I know that entities advertise that they can gain unauthorized access to any e-mail account in exchange for a fee ("E-mail Hacking Services"). Such E-mail Hacking Services typically work in the following manner: a customer who is seeking unauthorized access to an e-mail account sends an e-mail with the e-mail address of the victim e-mail account to which the customer would like to get access. The E-mail Hacking Service responds with a message demonstrating that such unauthorized access has been successfully obtained, and provides proof, such as a screenshot of the home page of the victim e-mail account. The customer is required to pay a fee prior to receiving the log-in credentials necessary for the customer to get access to the victim e-mail account. The fees, which range between $50 to $250 per account, are typically paid by the customer by credit card or through PayPal or other on-line payment processors.

10. VARGAS's NYPD Hard Drive Material. On or about May 15, 2013, representatives of the NYPD provided me and other FBI agents with a forensic copy of the hard drive from the NYPD computer on the desk of EDWIN VARGAS, the defendant, located at a precinct in the Bronx, which they obtained in or about October 2012 (the "NYPD Hard Drive"). I and other FBI agents examined the NYPD Hard Drive and conducted a review of the contents of the NYPD Hard Drive and also received materials from the NYPD's own review of the NYPD Hard Drive. We identified the material stored on that hard drive under VARGAS's username and profile. Based on my training and experience and conversations with representatives from the NYPD and other FBI personnel, I know that the material stored on that hard drive under his username and profile reflects his username and profile's activity on that computer ("VARGAS's NYPD Hard Drive Material"). Based on these reviews, I have learned that VARGAS's NYPD Hard Drive Material contains, among other things, the following, in substance and in part:

a. A stored file containing the contents of a G-mail account, which, as set forth below, I believe belongs to VARGAS (the "VARGAS G-mail Account"). The Contacts section of the VARGAS G-mail Account includes the following, among other things:

i. A list of at least 20 e-mail addresses along with what appear to be telephone numbers, home addresses, and vehicle information corresponding to those e-mail addresses, as well as what appear to be the passwords for those e-mail addresses.

ii. The list includes information for at least one e-mail address with the name and address of Victim 1. According to the NYPD, Victim 1, as well as a number of the others whose e-mail passwords and other information are listed in this manner, is an NYPD officer. Among these are Victim 2 and Victim 3, discussed below.

iii. At least two e-mail addresses for E-mail Hacking Services.

b. A stored file indicating that an on-line cellular telephone account that appears to belong to Victim 2 was accessed between in or about July and September 2012. The accessed pages include, among other things, the identities of

individuals with whom Victim 2 was communicating via text messaging. As noted above, according to the NYPD, Victim 2 is an NYPD officer.

11. I have reviewed e-mail correspondence between the VARGAS G-mail Account and e-mail accounts belonging to certain E-mail Hacking Services. I have also reviewed e-mail correspondence between a Yahoo e-mail account - which contains the same username as the VARGAS G-mail Account, and which, as set forth below, I believe also belongs to VARGAS (the "VARGAS Yahoo Account") - and the E-mail Hacking Services. The correspondence between the VARGAS Yahoo Account and the E-mail Hacking Services generally took place before the correspondence between the VARGAS G-mail Account and the E-mail Hacking Services. In one of the e-mail exchanges between the VARGAS Yahoo Account and an E-mail Hacking Service, VARGAS indicated, in substance and in part, that he was going to switch to a G-mail account. Shortly thereafter, the correspondence between the VARGAS G-mail Account and the E-mail Hacking Services commenced.

12. March 2011 E-mail Correspondence. From e-mail correspondence that I have reviewed, I have learned the following about communications between EDWIN VARGAS, the defendant, and the E-mail Hacking Services in March 2011, in substance and in part:

a. An e-mail was sent in or about March 2011 from an E-mail Hacking Service to the VARGAS Yahoo Account containing a screenshot of the home page of an e-mail account of a victim ("Victim 4"), with an accompanying message stating, in substance and in part, that the screenshot was proof that Victim 4's e-mail account had been successfully hacked by the E-mail Hacking Service, and demanding payment prior to providing the log-in credentials necessary to access Victim 4's E-mail Account. Shortly thereafter, an e-mail was sent from the VARGAS Yahoo Account providing a proof of payment from an on-line payment processing system.

b. The billing information in the e-mail with the proof of payment listed the payor's name as "Edwin Vargas;" an IP address ("IP Address 1"),[1] with the IP location listed as the Bronx; the VARGAS Yahoo Account e-mail address as the payor's e-mail address; and an address in the Bronx (the "Bronx Address") as the payor's address.

[1] An IP address is a unique numerical address identifying each computer on the Internet. IP addresses are conventionally written in the dot-punctuated form *num1.num2.num3.num4* (e.g., 123.456.7.89).

c. Based on information obtained from the NYPD, the NYPD's employment records show that VARGAS lived at the Bronx Address from at least in or about March 2011 until in or about November 2012.

13. Some of the e-mail correspondence from the VARGAS Yahoo and G-mail Accounts to the E-mail Hacking Services lists either IP Address 1 or a second IP address ("IP Address 2") as their originating IP addresses. Based on information obtained from Yahoo, as well as an internet service provider and the NYPD, I have learned the following about the IP Addresses associated with the VARGAS Yahoo Account:

a. The VARGAS Yahoo Account was created from IP Address 1, which is the IP address that appears as part of the billing information for the payor in the March 2011 e-mail correspondence referenced in ¶12b above.

b. The VARGAS Yahoo Account was accessed through IP Address 2 and five other IP Addresses (the "Five Other IP Addresses") between January 2012 and October 2012.

c. IP Address 2 as well as two of the Five Other IP Addresses through which the VARGAS Yahoo Account was accessed were located within a block of the Bronx Address between January 2012 and October 2012, which was the home address of EDWIN VARGAS, the defendant, during that time. Based on my training and experience, I believe that VARGAS was accessing the VARGAS Yahoo Account while at or near his residence without paying for an Internet connection, by accessing those three IP Addresses which belonged to his neighbors.

d. Based on information obtained from the NYPD, I have learned that the remaining three of the Five Other IP Addresses, through which the VARGAS Yahoo Account was accessed, were assigned to VARGAS's desk computer at the NYPD, during the time period that they were used to access the VARGAS Yahoo Account. According to the NYPD's records, the times of access to the VARGAS Yahoo Account through these IP Addresses match times when VARGAS was logged in as the user of that computer.

14. Between in or about March 2011, and in or about October 2012, the VARGAS Yahoo and G-mail Accounts sent requests to E-mail Hacking Services for log-in credentials to gain unauthorized access to approximately 43 personal e-mail accounts and one mobile phone belonging to at least 30 different individuals, in each case listing the victim's e-mail address or, in one case, a cellular telephone number, and the victim's name.

Based on information provided by the NYPD, I have learned that of these 30 individuals, at least 21 are affiliated with the NYPD, including 19 current officers, one retired officer, and one current administrative staff. The requests include what appear to be the personal e-mail accounts of Victims 1, 2, 3 and 4.

15. The PayPal Account. Both the VARGAS Yahoo and G-mail Accounts paid for most of the hacking services with the same PayPal account (the "PayPal Account"). I have learned the following about the PayPal Account, in substance and in part:

a. Based on records obtained from PayPal, the PayPal Account is subscribed to EDWIN VARGAS, the defendant, at the Bronx Address.

b. The PayPal Account is linked to an e-mail address at Hotmail (the "Hotmail Account"). Based on records obtained from Microsoft, the Hotmail Account is also subscribed to VARGAS at the Bronx Address.

c. Charges on the PayPal Account are paid from a bank account which, based on my review of the bank account records, belonged to VARGAS at the Bronx Address (the "VARGAS Bank Account").

d. Based on my review of the VARGAS Bank Account and PayPal records, between in or about April 2010 and October 2012, approximately $4,050 was paid from the VARGAS Bank Account to entities that I believe, based on my training and experience and involvement in this investigation, to be associated with the E-mail Hacking Services.

16. On or about June 18, 2012, Victim 1's E-mail Account was accessed using IP Address 2. According to e-mail correspondence I reviewed in the VARGAS G-mail Account, an E-mail Hacking Service sent an e-mail containing the log-in credentials for Victim 1's E-mail Account earlier that day to the VARGAS G-mail Account. I believe that EDWIN VARGAS, the defendant, accessed Victim 1's E-mail Account using IP Address 2, see ¶13c, his neighbor's IP Address, while he was at or near his residence at the Bronx Address, on June 18, 2012, after receiving the log-in credentials for Victim 1's E-mail Account earlier that day.

17. In summary, based on my training and experience and involvement in this investigation, I believe that EDWIN VARGAS, the defendant, purchased log-in credentials from E-mail Hacking Services in order to access Victim E-mail Accounts without authorization, and he used the VARGAS Yahoo and G-mail Accounts

and the PayPal and Hotmail Accounts to do so, based on the following, in substance and in part:

a. Based on the IP Address information, I believe that VARGAS was the user of the VARGAS Yahoo Account, which he accessed either from the vicinity of the Bronx Address, where he lived, or from his workstation at the NYPD, also in the Bronx;

b. Based on a review of the e-mail correspondence between the VARGAS Yahoo and G-mail Accounts with the E-mail Hacking Services, as well as my review of VARGAS's NYPD Hard Drive Material, I believe that VARGAS was also the user of the VARGAS G-mail Account;

c. Based on a review of the e-mail correspondence between the VARGAS Yahoo and G-mail Accounts and the E-mail Hacking Services, VARGAS paid for the e-mail hacking services through the PayPal Account which was linked to the Hotmail Account;

d. Based on records from Microsoft, VARGAS was the owner of the Hotmail Account;

e. Based on records from PayPal, VARGAS was the owner of the PayPal Account; and

f. The PayPal Account was automatically linked to the VARGAS Bank Account. Through this method, VARGAS paid approximately $4,050 for e-mail hacking services between in or about April 2010 and in or about September 2012.

## Unauthorized Access of NCIC

18. From my discussions with NYPD representatives, I have learned that on or about November 5, 2011, EDWIN VARGAS, the defendant, accessed the NCIC database and obtained information about Victim 2 and Victim 3. Based on my review of the records provided by the NYPD, I have learned that at the time that he accessed the NCIC database, VARGAS was in his precinct in the Bronx. I have learned that VARGAS did not have authorization

to perform those searches or to access that information about Victim 2 or Victim 3.

WHEREFORE, I respectfully request that an arrest warrant be issued for EDWIN VARGAS, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

SAMAD D. SHAHRANI
Special Agent
Federal Bureau of Investigation

Sworn to before me this
20 day of May 2013

S/ Sarah Netburn

MAY 20 2013

HON. SARAH NETBURN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK