(C) "Phishing" is a fraud technique by which cybercriminals send emails to acquire sensitive information, including usernames and passwords that are used to log in to computer systems. Phishing emails are typically designed to resemble emails from trustworthy entities, such as legitimate companies or acquaintances, in an attempt to defraud unwitting recipients. For example, cybercriminals can phish by sending an email that directs the recipient to click a link to an Internet site. When clicked, the link surreptitiously and automatically downloads malicious computer software ("malware") onto the victim's computer, allowing the cybercriminals covert remote access ("backdoor access") to the victim's computer. Alternatively, the malware may provide the cybercriminals the ability to covertly record the victim's keystrokes while the victim performs routine computer tasks such as logging into accounts ("keylogging").

(D) "Affiliate marketing" is a type of marketing business. With respect to affiliate marketing and the Internet, affiliates enter into marketing agreements with companies to generate sales of certain products through the Internet. Affiliates earn commissions on sales to customers who purchase the products from websites associated with the affiliate.

VICTIM EMAIL SERVICE PROVIDERS

3. At all times relevant to this Indictment:

(A) An ESP referred to in this Indictment as "ESP1" maintained a registry of other legitimate ESPs. Various Internet Service Providers used this registry to identify emails coming from legitimate ESPs as opposed to spam. ESP1 allowed employees and customers to access their ESP1 services through the Internet.

(B) An ESP referred to in this Indictment as "ESP2" provided bulk email services to its customers. ESP2 allowed customers to access the customers' accounts and control and customize email campaigns through the Internet. ESP2 had computer systems located in the Northern District of Georgia.

(C) An ESP referred to in this Indictment as "ESP3" provided bulk email services to its customers. ESP3 allowed customers to access their accounts and control and customize email campaigns through the Internet.

(D) An ESP referred to in this Indictment as "ESP4" provided bulk email services to its customers. ESP4 allowed customers to access their accounts and control and customize email campaigns through the Internet. ESP4 had computer systems located in the Northern District of Georgia.

(E) An ESP referred to in this Indictment as "ESP5" provided bulk email services to its customers. ESP5 allowed

customers to access their accounts and control and customize email campaigns through the Internet.

(F) An ESP referred to in this Indictment as "ESP6" provided bulk email services to its customers. ESP6 allowed customers to access their accounts and control and customize email campaigns through the Internet.

(G) An ESP referred to in this Indictment as "ESP7" provided bulk email services to its customers. ESP7 allowed customers to access their accounts and control and customize email campaigns through the Internet.

(H) An ESP referred to in this Indictment as "ESP8" provided email services and products that allowed its customers to send and manage transactional and marketing emails. Transactional emails are emails that are sent automatically by computer programs in response to specific events, such as a user purchasing an item from an online store.

DEFENDANTS

4. Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, is a computer hacker who, during the relevant time period, resided in or around Deventer, Netherlands and Hanoi, Vietnam. As described below, Defendant NGUYEN hacked into victim ESPs' computer systems and stole confidential information including email addresses. He also coordinated the sending of unauthorized email

campaigns, and he has profited from those campaigns as an affiliate marketer.

5. Defendant GIANG HOANG VU, a/k/a Lee Vu, during the relevant time period, resided in or around Deventer, Netherlands. As described below, Defendant VU assisted Defendant NGUYEN by sending unauthorized email campaigns, and producing artwork and other elements used in affiliate-marketing websites.

MANNER AND MEANS

6. It was part of the conspiracy that:

(A) Defendants NGUYEN and VU acquired tools used to facilitate intrusions into computer systems, including (1) crypters, which are designed to hide malware from anti-virus programs; (2) covert monitoring programs; and (3) malware. Some of these tools were subsequently used to facilitate computer intrusions into victim ESPs' computer systems.

(B) Defendant NGUYEN directed email phishing campaigns at employees of ESPs, including ESP1, ESP2, ESP5, and ESP7. The phishing campaigns delivered malware, which allowed Defendant NGUYEN backdoor access to the victim employees' computer systems and enabled him to steal sensitive information, including the employees' access credentials for their employers' computer systems.

(C) Using stolen access credentials, Defendant NGUYEN gained unauthorized access to victim ESPs' computer systems.

In some instances, such as with respect to ESP2, ESP3, ESP5, ESP6, and ESP7, Defendant NGUYEN stole confidential information by downloading the information from the victim ESPs' computer systems to a server controlled by Defendant NGUYEN. The confidential information included tens of millions of email addresses belonging to some of the victim ESPs' customers.

(D) With respect to ESP2, from on or about October 21, 2010 through on or about November 23, 2010, Defendant NGUYEN gained unauthorized access to ESP2's computer systems through the Internet using the compromised account of a former ESP2 employee with the initials KT. After doing so, Defendant NGUYEN used KT's account to access various ESP2 customer accounts and steal millions of customers' email addresses by downloading them to a server controlled by Defendant NGUYEN located in the Netherlands. This resulted in computer commands being sent between ESP2's servers located in the Northern District of Georgia and the server located in the Netherlands. The acts specified in Counts Two through Eleven of this Indictment are representative examples of the intrusions and thefts described in this subparagraph.

(E) In some instances, Defendant NGUYEN or other co-conspirators gained unauthorized access to victim ESPs' computer systems, including ESP2's and ESP5's, and, using those computer systems, launched unauthorized email phishing campaigns directed at

other ESPs' employees. These campaigns were designed to obtain access credentials to gain unauthorized access into other ESPs' computer systems. These unauthorized campaigns were often preceded by seed emails that Defendant NGUYEN or other co-conspirators sent to email accounts under Defendant NGUYEN's control.

(F) In some instances, Defendant NGUYEN or other co-conspirators gained unauthorized access to victim ESPs' computer systems, including ESP4's and ESP6's, and, using those computer systems, launched unauthorized email campaigns using stolen email addresses. The unauthorized campaigns included spam emails directing recipients to Defendant NGUYEN's affiliate-marketing websites. These unauthorized campaigns were often preceded by seed emails that Defendant NGUYEN or other co-conspirators sent to email accounts under Defendant NGUYEN's control.

(G) Defendant NGUYEN acted as an affiliate marketer, and he used unauthorized email campaigns to drive Internet traffic to affiliate-marketing websites associated with him. Defendant NGUYEN was paid by an affiliate-marketing company a percentage of all sales completed through those websites, thereby obtaining money from the unauthorized email campaigns.

(H) Defendant VU assisted Defendant NGUYEN in setting up some of the affiliate-marketing websites associated with Defendant NGUYEN. In addition, Defendant VU used an account at an ESP to upload

an email contact list that had been stolen from another ESP, and send two unauthorized email campaigns using those email addresses.

(I) Defendant NGUYEN controlled at least two servers in the Netherlands that were used to gain unauthorized access to victim ESPs' computer systems, store hacking tools, and store stolen email addresses. As part of the conspiracy, those two servers had several electronic communications with victim ESPs' servers, including servers located in the Northern District of Georgia, as well as different States and foreign countries.

All in violation of Title 18, United States Code, Section 1349.

COUNTS TWO THROUGH ELEVEN
Wire Fraud
18 U.S.C. § 1343

7. The Grand Jury re-alleges and incorporates by reference the factual allegations set forth in Paragraphs 2 through 6 of this Indictment as if fully set forth here.

8. Beginning on a date which is unknown to the Grand Jury, but at least as early as in or about February 2009, through in or about June 2012, in the Northern District of Georgia and elsewhere, Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, aided and abetted by others known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the scheme and artifice to defraud described in Count One of this Indictment, and to obtain money and property by means of materially false and

fraudulent pretenses, representations, and promises, as well as by omission of material facts, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, including computer commands transmitted in interstate and foreign commerce.

Execution of the Scheme and Artifice

9. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, in the Northern District of Georgia and elsewhere, for the purpose of executing the scheme and artifice to defraud and to obtain money and property as set out in Count One of this Indictment, Defendant NGUYEN, aided and abetted by others known and unknown to the Grand Jury, did knowingly cause computer commands to be made between at least one ESP2 server located in the Northern District of Georgia and a server located in the Netherlands, which had the Internet Protocol address 85.17.136.169 ("85.17.136.169 server"). As a result, Defendant NGUYEN stole email addresses associated with the ESP2 customers whose initials are in Column C, by downloading email addresses associated with those customers from the ESP2 server to the 85.17.136.169 server.

A	B	C
Count	Date (On or About)	ESP2 Customer
2	10/22/2010	MS
3	10/22/2010	SB
4	10/23/2010	PM
5	10/23/2010	AHM
6	10/23/2010	HG
7	10/23/2010	BT
8	10/23/2010	WG
9	10/24/2010	BIC
10	10/24/2010	TI
11	10/24/2010	JMS

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT TWELVE
Conspiracy to Commit Computer Fraud
18 U.S.C. § 371

10. The Grand Jury re-alleges and incorporates by reference the factual allegations set forth in Paragraphs 2 through 6, and 9 of this Indictment as if fully set forth here.

11. Beginning on a date which is unknown to the Grand Jury, but at least as early as in or about February 2009, through in or about June 2012, in the Northern District of Georgia and elsewhere, Defendants VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, and GIANG HOANG VU, a/k/a Lee Vu, with others known and unknown to the Grand Jury, did knowingly and willfully conspire to:

(A) intentionally access a computer without authorization and exceed authorized access to a computer, and thereby obtain and attempt to obtain information from a protected computer, and the offense was committed for the purpose of private financial gain, and the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);

(B) knowingly and with intent to defraud access a protected computer without authorization and exceed authorized access to a protected computer, and by means of such conduct further the intended fraud and obtain things of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A); and

(C) knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage and attempt to cause damage without authorization to a protected computer, causing loss aggregating $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

OVERT ACTS

12. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following overt acts, among others:

(A) On or about February 8, 2009, Defendant NGUYEN and Defendant VU obtained a crypter, which was designed to hide malware from anti-virus software.

(B) On or about March 15, 2010, Defendant VU uploaded stolen email addresses to ESP7's computer systems and launched two unauthorized email campaigns targeting those stolen email addresses.

(C) On or about September 2, 2010, Defendant NGUYEN accessed without authorization the ESP6 account of the individual with the initials MH. MH was an employee of an ESP6 business customer. Using MH's account, NGUYEN accessed without authorization ESP6's web-based application that allows customers to

access their accounts and to control and customize email campaigns. Using that access, Defendant NGUYEN sent approximately 100,000 unauthorized emails.

(D) On or about September 5, 2010, Defendant NGUYEN accessed without authorization the ESP6 account of the individual with the initials EM. EM was an employee of an ESP6 business customer. Using EM's account, NGUYEN accessed without authorization ESP6's web-based application that allows customers to access their accounts and to control and customize email campaigns. Using that access, Defendant NGUYEN sent approximately 450,000 unauthorized emails.

(E) On or about September 10, 2010, Defendant NGUYEN established an account at ESP4, using ESP4's web-based application, purportedly on behalf of a real company with the initials NS. In setting up the account, Defendant NGUYEN used the name of NS' president, an individual with the initials BM, without NS' or BM's knowledge or authorization.

(F) On or about September 13, 2010, Defendant NGUYEN, using the fake NS account, attempted to send approximately 11 million emails on behalf of NS as part of a spamming campaign.

(G) From on or about September 10, 2010 through on or about September 13, 2010, Defendant NGUYEN paid for services with

ESP4 purportedly on behalf of NS using a credit card belonging to the victim with the initials LP, without LP's knowledge or consent.

(H) From on or about October 19, 2010, through on or about October 20, 2010, Defendant NGUYEN sent phishing emails to ESP2 employees. The phishing emails contained a link that, once clicked, installed malware onto the victim's computer. The ESP2 employee with the initials CW clicked on the link in one of the phishing emails, resulting in malware being installed on CW's computer located in the Northern District of Georgia.

(I) On or about October 21, 2010, Defendant NGUYEN accessed without authorization CW's account at ESP2. CW was an ESP2 employee with administrator access. Using CW's account, Defendant NGUYEN accessed without authorization ESP2's web-based application that allows customers to access their accounts and control and customize email campaigns. The unauthorized access to CW's ESP2 account occurred from an Internet Protocol address outside the State of Georgia, and ESP2's servers were located in the Northern District of Georgia.

(J) After gaining unauthorized access to CW's account at ESP2, Defendant NGUYEN reactivated KT's account at ESP2. KT was a former ESP2 employee with administrator access. From on or about October 21, 2010, through on or about November 23, 2010, Defendant NGUYEN made over one hundred unauthorized accesses into ESP2's

web-based application using KT's account. In some instances, after gaining unauthorized access, NGUYEN used KT's account to access various customer accounts and downloaded the customers' email addresses to at least one server controlled by Defendant NGUYEN located in the Netherlands. The acts specified in Counts Thirteen through Twenty-Four of this Indictment are representative examples of the unauthorized accesses described in this subparagraph.

(K) On or about November 1, 2010, Defendant NGUYEN sent phishing emails to ESP7 employees. At least one employee clicked on the link in the phishing emails, resulting in malware being installed on the victim's computer.

(L) On or about November 11, 2010, Defendant NGUYEN accessed without authorization ESP1 account of the individual with the initials JC. JC was an ESP1 employee with administrator access. Using JC's account, Defendant NGUYEN accessed without authorization the web-based application that ESP1's employees and customers use to access their ESP1 services from the Internet. After gaining such unauthorized access, Defendant NGUYEN stole confidential information including email addresses.

(M) On or about March 5, 2011, Defendant NGUYEN accessed without authorization the ESP3 account of the individual with the initials CB. CB was an employee of ESP3. Using CB's account, Defendant NGUYEN accessed without authorization ESP3's web-based

application that allows customers to access their accounts and to control and customize email campaigns. Defendant NGUYEN then used CB's account to download ESP3 customer email addresses relating to the ESP3 business customer with the initials AR.

(N) On or about March 23, 2011, Defendant NGUYEN accessed without authorization the ESP3 account of the individual with the initials CD. CD was an ESP3 employee. Using CD's account, Defendant NGUYEN accessed without authorization ESP3's web-based application that allows customers to access their accounts and to control and customize email campaigns. Defendant NGUYEN then used CD's account to download ESP3 customer email addresses relating to the ESP3 business customer with the initials BB.

(O) On or about February 23, 2012, using ESP8's web-based application, Defendant NGUYEN established an account at ESP8 purportedly on behalf of a company with the initials FF. On or about March 13, 2012, using the FF account, Defendant NGUYEN attempted to send spam.

(P) On or about March 21, 2012, Defendant NGUYEN accessed without authorization the ESP4 account of the company with the initials MB. On or about March 22, 2012, Defendant NGUYEN, using MB's account, attempted to send spam.

(Q) On or about June 5, 2012, Defendant NGUYEN accessed without authorization the ESP8 account of the company with the initials IS. On the same day, Defendant NGUYEN, using IS's account, attempted to send spam.

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

COUNTS THIRTEEN THROUGH TWENTY-FOUR
Computer Fraud and Abuse
18 U.S.C. § 1030

13. The Grand Jury re-alleges and incorporates by reference the factual allegations in Paragraphs 2 through 6, 9, and 12 of this Indictment as if fully set forth here.

14. Beginning on a date which is unknown to the Grand Jury, but at least as early as in or about February 2009, through in or about June 2012, in the Northern District of Georgia and elsewhere, Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer without authorization and exceed authorized access to a computer, and thereby obtain and attempt to obtain information from a protected computer, and the offenses were committed for the purpose of private financial gain.

15. On or about the dates identified in Column B of the chart set forth below, each date constituting a separate count as set forth in Column A, Defendant NGUYEN accessed without authorization and exceeded authorized access of at least one ESP2 server, which was

damage and attempt to cause damage without authorization to a protected computer, and the offense caused and would, if completed, have caused loss to persons during a one-year period from the Defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 2.

COUNT TWENTY-SIX
Spamming
18 U.S.C. § 1037

18. The Grand Jury incorporates by reference the factual allegations in Paragraphs 2 through 6, 9, and 12 of this Indictment as if fully set forth here.

19. On or about November 23, 2010, Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, aided and abetted by others known and unknown to the Grand Jury, did knowingly access a protected computer located in the Northern District of Georgia without authorization and intentionally initiate the transmission of multiple commercial electronic mail messages from and through such computer, in violation of Title 18, United States Code, Sections 1037(a)(1), (b)(2)(A), and 2.

COUNT TWENTY-SEVEN
Aggravated Identity Theft
18 U.S.C. § 1028A

20. The Grand Jury incorporates by reference the factual allegations set forth in Paragraphs 2 through 6, 9, and 12 of this Indictment as if fully set forth here.

21. On or about September 10, 2010, in the Northern District of Georgia and elsewhere, Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, aided and abetted by others known and unknown to the Grand Jury, during and in relation to the crime of conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349, as more fully set forth in Count One above, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, the name of the victim having the initials BM, in violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(5), and 2.

COUNT TWENTY-EIGHT
Aggravated Identity Theft
18 U.S.C. § 1028A

22. The Grand Jury incorporates by reference the factual allegations set forth in Paragraphs 2 through 6, 9, and 12 of this Indictment as if fully set forth here.

23. On or about October 21, 2010, in the Northern District of Georgia and elsewhere, Defendant VIET QUOC NGUYEN, a/k/a Vandehiu, a/k/a Peter Nguyen, aided and abetted by others known and unknown

software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

29. If any of the property subject to forfeiture herein, as a result of any act or omission of Defendants:

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

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

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

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1029(c)(2) and Title 28, United States Code, Section 2461(c).

[redacted]

[redacted]

FOREPERSON

SALLY QUILLIAN YATES
UNITED STATES ATTORNEY

NICHOLAS A. OLDHAM
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar No. 592701

for

PETER V. ROMAN
TRIAL ATTORNEY
COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION
UNITED STATES DEPARTMENT OF JUSTICE
D.C. Bar No. 984996

600 U.S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
Telephone 404-581-6000
Facsimile 404-581-6181