IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | **SUPERSEDING INDICTMENT** |
| | ) | |
| Plaintiff, | ) | **FILED UNDER SEAL** |
| | ) | |
| v. | ) | JUDGE DONALD C. NUGENT |
| | ) | |
| ROMEO VASILE CHITA, | ) | CASE NO. 1:10CR392 |
| a/k/a "Rich," | ) | |
| TEODOR VIOREL RADU, | ) | 18 U.S.C. § 1962(d) |
| DANIEL MIHAI RADU, | ) | 18 U.S.C. § 1349 |
| IONUT CHERA, | ) | 18 U.S.C. § 1956(h) |
| a/k/a "Ciceo," | ) | 18 U.S.C. § 371 |
| CLAUDIU VIRGIL TURLEA | ) | 18 U.S.C. § 1963 (forfeiture) |
| a/k/a "Biggie," | ) | 18 U.S.C. § 981 (forfeiture) |
| a/k/a "Bigs," | ) | 18 U.S.C. § 982 (forfeiture) |
| a/k/a "Bighi," | ) | |
| MANUEL TUDOR, | ) | |
| a/k/a "Manu" | ) | |
| a/k/a "Man," | ) | |
| a/k/a "Marius," | ) | |
| CAROL JURJA, | ) | |
| a/k/a "Crapu" | ) | |
| DANIEL UNGUREANU, | ) | |
| a/k/a "Frank," | ) | |
| a/k/a "Dan," | ) | |
| DUMITRU NICOLAITA, | ) | |
| a/k/a "TB," | ) | |
| | ) | |
| Defendants. | ) | |

COUNT ONE
(Racketeering Conspiracy)

The Grand Jury charges:

General Allegations and Definitions

At all times relevant to this indictment, unless otherwise alleged:

1. The Internet is a global network connecting millions of computers and computer networks to each other allowing them to communicate and transfer information. Using, among other things, a system of wires, cables, routers, and circuits, the Internet allows the communication and transfer of information in interstate and foreign commerce. One type of information transferred across the Internet is email, which is an electronic communication or message sent across the Internet. Another type of information involves online banking and information transferred in connection to accessing bank accounts and transferring money over the Internet.

2. "Phishing" is an attempt to fraudulently acquire personal information by sending an email which falsely claims to be from an established legitimate entity. One type of phish email directs the user to open an attachment to the email. Opening the attachment usually results in the installation of malware without the user's knowledge. The malware is often in the form of a keylogger. The keylogger captures sensitive and confidential information entered on the computer by the victim during the course of the victim's business and financial activities.

3. "Spear-phishing" is a term used to describe highly targeted phishing attacks. Spear-phishers send emails that tend to be much more focused and detailed than a typical phish. Spear-phishers also target their victims more carefully than typical phishers or spammers. An

example of "spear-phishing" is sending an email to an individual believed to access on-line banking services using secret passwords for the purpose of stealing that information.

4. "Keylogger" means a computer program or programs that surreptitiously capture the keys typed on a computer and forwards that information to the individuals who caused it to be installed or to a place designated by them. Through this technique, individuals are able to secretly obtain the user identification and passwords for bank accounts as soon as the user of the infected computer logs into their account on-line. After obtaining this information, the individuals execute unauthorized ACH and wire transfers to accounts that they control.

5. "Mule" or "money mule" is an individual recruited to receive and transmit unauthorized electronic funds transfers from deposit accounts to designated individuals in the United States or overseas. Depending on the scheme, a mule is solicited by individuals who (1) have gained unauthorized access to the online deposit account of a business or consumer or (2) have otherwise fraudulently obtained money or funds. In many instances, the mule is located in the United States and opens and controls a deposit account that is intended to accept the unauthorized transfer from a victim's account. Often in these instances, the money mule is then instructed to quickly withdraw the funds and wire them overseas after deducting a commission. In some cases, a money mule may be instructed not to open bank accounts but instead to pick up or send funds using a money transfer service such as Western Union or MoneyGram.

6. "Spam" generally is an email message that is sent in bulk to recipients without prior request or approval. The origin of the spam is almost always masked or falsified to prevent any identification of the sender.

7. "Malware" is an abbreviated term for "malicious software." Malware refers to

software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware. Malware can gather data from a user's system without the user knowing it.

8. "WU" means "Western Union," and "MG" means "Moneygram." As used herein WU and MG are money transfer services that make international wire transfers for a fee. "MCTN" means "Money Control Transfer Number" and is a unique identifier used by Western Union to track wire transfers.

9. An ACH transfer is an abbreviated term for transferring funds from one bank account to another using the Automated Clearing House network. Funds are transferred electronically without any paper money changing hands. A certain period of time is required for an ACH transfer to clear, and thus, funds are not immediately available. A wire transfer also transfers funds from one bank to another without paper and the funds are immediately available.

10. SMS stands for "Short Message Service," which are short text messages that are typically sent from cell phone to cell phone.

11. Online Marketplaces allow goods and services to be traded over the Internet. eBay, Inc. ("eBay"), Craigslist, Autotrader.com and Cars.com are online marketplaces, each operating a commercial interactive online auction and shopping service where consumers can conduct financial transactions to purchase and sell items, including automobiles and boats. Payments are often made and accepted outside the official website. These marketplaces are often vulnerable to items falsely being represented for sale, and payments being made and accepted, for goods that are never delivered.

The Enterprise

12. At all times relevant to this Indictment, defendants ROMEO VASILE CHITA, a/k/a "Rich," TEODOR VIOREL RADU, DANIEL MIHAI RADU, IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a "Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a " "Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," and others known and unknown to the Grand Jury, were conspirators and associates of a criminal organization. This criminal organization constituted an "Enterprise," as that term is defined in Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact, although not a legal entity. The Enterprise constituted an ongoing organization whose conspirators functioned as a continuing unit for a common purpose of achieving the objectives of the Enterprise. The Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

13. The Enterprise, which operated in the Northern District of Ohio and elsewhere in the United States, and in the countries of Romania, Canada, Croatia, Latvia, Hungary, Bosnia, Malaysia, China, Jordan, and elsewhere, operated through groups of individuals responsible for the various fraudulent schemes and criminal activities conducted by the Enterprise. While the overall structure and model of the Enterprise remained constant, the group's and member's responsibilities within the overall structure of the Enterprise were adjusted, altered, reassigned, or otherwise modified as necessary in order to address specific criminal activity of the Enterprise.

Purposes of the Enterprise

14. The principal purpose of the Enterprise was to generate money for its conspirators and associates. This purpose was implemented by conspirators and associates of the Enterprise committing various criminal acts, including wire fraud, trafficking in counterfeit services and money laundering.

15. The conspirators and associates of the Enterprise sought, among other things, to:

a. Preserve and protect the ability of the Enterprise to enrich its conspirators and associates through the corrupt use of false and fictitious identities and entities to hinder detection by law enforcement; and

b. Promote and enhance the criminal activities of the Enterprise and its conspirators and associates.

16. The Enterprise was bound together by, among other things, the conspirators' and associates' common interest, knowledge, and usage of the Internet and its vulnerabilities to fraudulently obtain money from victims pursuant to various fraudulent schemes, including but not limited to, a scheme to cause victims to send money directly to bank accounts controlled by the Enterprise and a scheme to fraudulently obtain bank account information to allow unauthorized access to victims' bank accounts and unauthorized fund transfers out of victims' accounts into bank accounts controlled by the Enterprise. For the common purpose of generating criminal proceeds and for the personal enrichment of the conspirators and associates through the conduct of the above-listed criminal activities, at various times relevant to the indictment, conspirators and associates of the Enterprise engaged in:

a. spear-phishing;

b. fraudulently using confidential bank account information that had been obtained through spear-phishing and conducting unauthorized computer transfers of funds from victim bank accounts to Enterprise controlled bank accounts;

c. fraudulently inducing online marketplace victims to send money for non-existent goods often by using counterfeit service marks of online marketplaces;

d. fraudulently manipulating bank equipment and installing hardware devices to obtain sensitive bank information;

e. making false and fraudulent representations to banks and creating false documents concerning extensions of credit; and

f. using "money mules" to withdraw funds from Enterprise controlled accounts or pick up or transfer funds using money transfer services.

17. Conspirators and associates of the Enterprise regularly used the Internet and telephone communications, including phone calls, phone messages, and SMS text messages, to give directions and share information. At various times relevant to the Indictment, conspirators and associates of the Enterprise used these communication methods to exchange information to further their schemes.

18. Conspirators and associates of the Enterprise regularly used the services of world-wide money transfer services, such as Western Union, MoneyGram, and U.S. financial institutions in order to transfer and conceal the proceeds of their unlawful activities as alleged herein.

The Roles of the Defendants

19. The defendants participated in operating and managing the Enterprise in the

following manner:

a. Defendant CHITA, based in Ramnicu Valcea, Romania, directed other Enterprise conspirators and associates to carry out the affairs of the Enterprise in the United States and elsewhere throughout the world. Defendant CHITA promoted, managed, and supervised the administration of the Enterprise by:

i. Managing and facilitating the various schemes to disseminate false and fraudulent information to victims;

ii. Laundering and directing other Enterprise conspirators and associates to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise;

iii. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities; and

iv. Fraudulently manipulating documents and directing others to do so.

b. Defendant TEODOR RADU directed the technical activity that facilitated the theft from corporate and other victims. The technical activity related to computers and malware and the use of computers to obtain the bank account access information and to transfer funds during the course of the fraudulent activity. As such, he assisted in:

i. Controlling and supervising the use of the Enterprise's malware and information derived therefrom;

ii. Communicating to conspirators and associates of the Enterprise which

victims would be targeted;

iii. Controlling the transmission of victim proceeds to accounts controlled by the Enterprise;

iv. Laundering and directing other Enterprise conspirators and associates to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise;

iv. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using encryption software to make the Enterprises's computers inaccessible to others, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities; and

vi. Fraudulently manipulating bank equipment, devices, and documents, and directing others to do so.

c. Defendant DANIEL RADU directed the technical activity that facilitated the theft from corporate and other victims. The technical activity related to computers and malware and the use of computers to obtain the bank account access information and to transfer funds during the course of the fraudulent activity. As such, he assisted in:

i. Controlling and supervising the use of the Enterprise's malware and information derived therefrom;

ii. Communicating to conspirators and associates of the Enterprise which victims would be targeted;

iii. Controlling the transmission of victim proceeds to accounts controlled by

the Enterprise;

iv. Laundering and directing other Enterprise conspirators and associates to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise; and

v. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using encryption software to make the Enterprises's computers inaccessible to others, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities;

d. Defendant CHERA was responsible for relaying communications between the conspirators and associates of the Enterprise based in the United States, in particular, between defendant TURLEA and defendant CHITA, to further the Enterprise's affairs.

i. Defendant CHERA also laundered and directed other Enterprise conspirators and associates to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise.

ii. Defendant CHERA also evaded law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using encryption software to make the Enterprise's computers inaccessible to others, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities.

e. Defendant TURLEA facilitated the transmission of criminal proceeds stolen by the Enterprise to accounts controlled by the Enterprise by:

i. Recruiting and managing the U.S.-based money mules who physically withdrew the proceeds from the various financial institutions and provided them to other conspirators and associates of the Enterprise;

ii. Directing and facilitating the money mules' establishment and use of bank accounts within U.S. banks to facilitate these transfers;

iii. Laundering and directing other Enterprise conspirators and associates to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise; and

iv. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities.

f. Defendant TUDOR was responsible for managing United States and foreign-based money mules who physically withdrew the criminal proceeds generated through the Enterprise's online marketplace fraud schemes and provided them to other Enterprise conspirators and associates based in the United States and elsewhere. Among other things, TUDOR was responsible for:

i. Directing and facilitating the money mules' use of false and fictitious identities used to receive victim proceeds and transmit them to Enterprise conspirators and associates in the United States and Romania, among other places;

ii. Directing the money mules to travel throughout the United States to collect and distribute proceeds in furtherance of the Enterprise's affairs; and

iii. Laundering and directing other Enterprise conspirators to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise; and

iv. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using encryption software to make the Enterprise's computers inaccessible to others, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities.

g. Defendant JURJA was responsible for managing United States and foreign-based money mules who physically withdrew the criminal proceeds generated through the Enterprise's online marketplace fraud schemes and provided them to other Enterprise conspirators and associates based in the United States and elsewhere. He was also responsible for arranging for conspirators and associates of the Enterprise to fraudulently manipulate bank equipment and devices to obtain sensitive bank information. JURJA was specifically responsible for:

i. Directing and facilitating the money mules' use of false and fictitious identities in receiving victim proceeds and transmitting them to Enterprise conspirators and associates in the United States and Romania, among other places;

ii. Directing the money mules to travel throughout the United States to collect and distribute proceeds in furtherance of the Enterprise's affairs;

iii. Laundering and directing other Enterprise conspirators to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise;

iv. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using encryption software to make the Enterprise's computers inaccessible to others, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities; and

v. Fraudulently manipulating bank equipment and devices, and directing others to do so.

h. Defendant UNGUREANU was responsible for recruiting and managing money mules based in the United States who physically withdrew the criminal proceeds. He was responsible for:

i. Facilitating the transfer of the proceeds generated through the Enterprise's online marketplace fraud schemes and providing them to other Enterprise conspirators and associates based in the United States;

ii. Laundering and causing other Enterprise conspirators to launder fraudulently obtained proceeds through financial institutions to promote, carry on, and/or conceal the illegal activities of the Enterprise; and

iii. Evading law enforcement detection of the criminal activities of the Enterprise by using false and fictitious identities, multiple email accounts, regularly changing phones, using code to speak with other Enterprise conspirators and associates, and directing others to engage in such activities.

i. Defendant NICOLAITA promoted the Enterprise's affairs by acting as a money mule who laundered, and caused other Enterprise conspirators to launder, fraudulently obtained

proceeds through money transfer services to promote, carry on, and/or conceal the illegal activities of the Enterprise and fraudulently manipulating bank equipment and devices.

The Conspiracy

20. From in or about February 2007, and continuing thereafter up to and including July 2008, in the Northern District of Ohio, the District of Nevada, the country of Romania, and elsewhere, the defendants: ROMEO VASILE CHITA, a/k/a "Rich," TEODOR VIOREL RADU, DANIEL MIHAI RADU, IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a "Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a ""Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," being persons employed by and associated with the Enterprise, an Enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown to the Grand Jury, did knowingly and intentionally conspire to conduct and participate, directly and indirectly, in the conduct of the affairs of the Enterprise through a pattern of racketeering activity as defined in Sections 1961(1) and (5) of Title 18, United States Code, which pattern of racketeering activity consisted of multiple acts involving wire fraud, in violation of 18 U.S.C. § 1343, trafficking in counterfeit services, in violation of 18 U.S.C. § 2320, laundering of monetary instruments, in violation of 18 U.S.C. § 1956, and engaging in monetary transactions in property derived from specified unlawful activity, in violation of 18 U.S.C. § 1957.

21. It was a part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering in conducting the affairs of the Enterprise.

Manner and Means of the Conspiracy

22. The manner and means by which the conspirators facilitated the Enterprise's criminal activities included multiple fraud schemes, including acts of wire fraud and money laundering as described below:

Scheme to Steal Sensitive Data, Passwords, and Assets from Corporate Victims

23. It was further part of the conspiracy that conspirators and associates of the Enterprise corruptly sought to enrich the Enterprise by perpetrating a widespread fraud scheme to steal assets, passwords, and other sensitive data from specifically targeted employees of corporate victims located throughout the United States. These employees were often responsible for or had access to their company's online bank accounts.

24. It was further part of the conspiracy that conspirators and their associates, using the Internet and other devices, disseminated false and fictitious emails purporting to be from legitimate entities. The false and fictitious emails purported to be from, among others, the Better Business Bureau (BBB), the Internal Revenue Service (IRS), U.S. Tax Court, SalesForce, and the National Payroll Records Center (NPRC). The false and fictitious emails were designed to induce the victims to open an attachment or link to the email purporting to be an official document which the victims were led to believe were from a legitimate organization. In some cases, the conspirators and their associates used counterfeit service marks in these emails in order to make the emails appear as though they originated from legitimate organizations. The counterfeit service marks used in these emails included, among others, the Better Business Bureau and SalesForce. In truth and fact, these emails were not from the legitimate organizations, but instead were from conspirators and associates of the Enterprise, who sought to trick the victims and infiltrate their computers through the installation of a keylogger. Without

the victims' knowledge, these keyloggers were installed onto the computer when the victims opened an attachment to the email. The keylogger allowed the conspirators and associates of the Enterprise to capture sensitive and confidential information unwittingly entered by victims during the course of the victims' business and financial activities.

25. Once the keylogger had surreptitiously captured the user name and passwords related to victim corporate bank accounts, it was further part of the conspiracy that defendants TEODOR RADU, DANIEL RADU and others used the stolen, sensitive banking information in furtherance of their fraudulent schemes.

26. It was further part of the conspiracy that this stolen, sensitive banking information was transmitted to the conspirators and their associates, for purposes of using it to fraudulently withdraw funds from the victims' accounts. The stolen funds were transferred to a specific United States-based money mule account to be retrieved and further distributed to TURLEA. The stolen funds were thereafter further distributed by TURLEA.

27. It was further part of the conspiracy that a money mule network was established. This network was supervised by defendant TURLEA. Defendant TURLEA and other Enterprise conspirators and associates required that certain money mules possess at least one United States bank account, typically held in a corporate or business name. The money mules provided defendant TURLEA and other conspirators and associates with the mule's account information, including but not limited to, bank name, account number, routing number, and the mules' online user names and passwords for the Enterprise's illicit use. In particular, this information was used by conspirators and associates of the Enterprise to collect and launder the Enterprise's criminal proceeds.

28. It was further part of the conspiracy that defendant TURLEA and other conspirators and associates tracked and assessed the money mules' availability. After considering the status of the various mules and mule accounts, defendant TURLEA and other conspirators and associates decided which money mule would be used and transmitted messages, including SMS text messages, indicating the chosen mule's relevant account information to defendant CHERA. Defendant CHERA transmitted that information to defendant CHITA, who transmitted it to defendants TEODOR RADU, DANIEL RADU and other conspirators and associates of the Enterprise to move the victim's money into the money mule's account. Once the stolen victim proceeds had been moved into the specified mule account, defendants TEODOR RADU, DANIEL RADU, and other conspirators and associates of the Enterprise notified defendant CHITA that the stolen victim proceeds had been transferred. Defendant CHITA then notified defendant CHERA of this information, who notified defendant TURLEA, who, directly and through other conspirators and associates, informed the money mule of the available proceeds and directed that money mule to withdraw the money.

29. It was further part of the conspiracy that defendant CHITA facilitated and directed defendant TEODOR RADU to steal the funds in the identified victim's bank account. Using the victim's online banking username and password, defendant TEODOR RADU, DANIEL RADU and other conspirators and associates would initiate an ACH or wire transfer from Romania to authorize the transfer of the victim's funds to the identified money mule account.

30. It was further part of the conspiracy that, as the ACH or wire transfers were pending, and as described above, defendant TEODOR RADU and DANIEL RADU called or sent SMS text messages to defendant CHITA which identified the amounts transferred and the

relevant account information for the paired victims and money mules.

31. It was further part of the conspiracy that defendant CHITA then forwarded via SMS text message the information described above to defendant CHERA, who then forwarded it to defendant TURLEA in the United States for defendant TURLEA and other conspirators and associates to order the money mule to collect the identified funds, once available.

32. It was further part of the conspiracy that, under the direction of defendant TURLEA and other conspirators and associates, the identified money mule collected the criminal proceeds in a variety of ways, including physically appearing at banking institutions throughout the United States to withdraw the entire amount of targeted proceeds or to structure withdrawals of proceeds to evade U.S. currency reporting laws and detection of the Enterprise's affairs. The identified money mule then traveled to various locations throughout the United States to deliver the criminal proceeds to other conspirators and their associates, who were identified to the mule by defendant TURLEA and other conspirators and associates. These proceeds were then transmitted back to Enterprise conspirators through a money mule network located in Romania to be further distributed among conspirators and associates.

33. It was further a part of the conspiracy that, when the money mule network was not employed, defendants CHITA, TEODOR RADU, and DANIEL RADU initiated and attempted to initiate wire transfers directly from the victims' accounts in the United States to offshore accounts controlled by the Enterprise. These transfers typically involved hundreds of thousands of dollars.

34. It was further part of the conspiracy that the monies collected by the defendants, and other conspirators and associates, were laundered by the defendants to perpetuate the

Enterprise and promote its fraudulent affairs and for the personal enrichment of the defendants.

Online Marketplace Fraud Schemes

35. It was part of the conspiracy that conspirators and associates of the Enterprise would corruptly seek to enrich the Enterprise by perpetrating a widespread fraud scheme using computers and the Internet and causing the posting in interstate and foreign commerce, of numerous misleading advertisements on online marketplaces such as eBay, Craig's List, Autotrader.com, and Cars.com, among others. These advertisements contained photographs and detailed descriptions of the purported vehicles and other high-dollar items that were available for purchase. In truth and fact, the goods were not available for purchase.

36. Conspirators and their associates, using the Internet and other devices, posed as sellers, causing emails to be transmitted to and from unwitting victims in the United States and elsewhere, who were online marketplace consumers interested in buying the advertised items. When a victim emailed the purported seller to inquire about the availability of an advertised vehicle or other high-dollar item, the purported sellers replied to the buyer via email, and not through the real online marketplace websites. After negotiating for the sale of the non-existent item with the potential buyer, the defendants directed the buyer to send payment to what appeared to be a legitimate entity that would receive payment and ensure delivery, but was in fact a false and fictitious entity, often including a fake escrow service purporting to receive payment and ensure delivery of the goods purchased. In some cases, the purported sellers used counterfeit service marks of online marketplaces in their communications with the buyers in order to make the communications appear as though they originated from real online marketplaces. The counterfeit service marks used by the purported sellers included, among others, eBay and

AutoTrader.com.

37. Defendants CHITA, NICOLAITA, JURJA, TUDOR, TURLEA, UNGUREANU, and others routinely exchanged cellular telephone calls and SMS text messages to provide notice of the arrival of a victim's wire transfer of funds through Western Union or MoneyGram. These SMS text messages included information concerning the victim, dollar amount, and MCTN or other identifier unique to that transaction, and the mule's name. Defendants CHITA, JURJA, TUDOR, NICOLAITA, TURLEA, UNGUREANU and money mules acting at their direction soon thereafter withdrew the illegal proceeds from Western Union and MoneyGram locations, or from their money mule bank account, and distributed the proceeds to defendants TURLEA, UNGUREANU, and other conspirators and associates of the Enterprise to promote the scheme and for their own personal enrichment.

38. To further avoid detection from law enforcement and the victims, defendants CHITA, JURJA, TUDOR, TURLEA, NICOLAITA and others created and caused others to create false identification documents, and retrieved proceeds from Western Union and MoneyGram locations using aliases and assumed names.

Other Bank-Related Schemes

39. Defendant CHITA fraudulently manipulated documents and directed others to do so.

40. Defendant TEODOR RADU fraudulently manipulated bank equipment, devices, and documents and directed others to do so.

41. Defendants NICOLAITA and JURJA fraudulently manipulated bank equipment and devices and directed others to do so.

All in violation of Title 18, United States Code, Section 1962(d).

COUNT TWO
(Wire Fraud Conspiracy)

The Grand Jury further charges:

42. From in or about 2005, and continuing up to in or about 2010, in the Northern District of Ohio, District of Nevada, the country of Romania, and elsewhere, the defendants, ROMEO VASILE CHITA, a/k/a "Rich," TEODOR VIOREL RADU, DANIEL MIHAI RADU, IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a"Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a ""Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," did knowingly and willfully conspire, combine, confederate and agree with each other and with other persons both known and unknown to the Grand Jury to devise a scheme and artifice to defraud and to obtain money and property from individuals and corporations by means of false and fraudulent pretenses, representations and promises, using wire communications in interstate and foreign commerce, in violation of Title 18, United States Code, Section 1343.

Manner and Means of the Conspiracy

43. The manner and means by which the defendants and the co-conspirators sought to achieve the purpose and object of the conspiracy included, among others, the allegations set forth in paragraphs 14 through 19 and paragraphs 22 through 41 of Count 1 of this Indictment, which are re-alleged and incorporated herein by reference.

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

COUNT THREE
(Money Laundering Conspiracy)

The Grand Jury further charges:

The Conspiracy

43. From in or about 2005, through in or about 2010, in the Northern District of Ohio, District of Nevada, the country of Romania, and elsewhere, the defendants,

ROMEO VASILE CHITA, a/k/a "Rich," TEODOR VIOREL RADU, DANIEL MIHAI RADU, IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a "Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a ""Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," did knowingly conspire, confederate, and agree with each other and with other persons known and unknown to the Grand Jury to commit offenses against the United States, that is, to violate Title 18, United States Code, Sections 1956(a)(1)(A)(i) and (B)(i) and Section 1957.

The Purpose and Object of the Conspiracy

44. It was the purpose and object of the conspiracy to:

a. knowingly and willfully conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, that is, transferring funds from bank accounts and through money remitter services, which transactions in fact involved the proceeds of specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, with the intent to promote the carrying on of said specified unlawful activity, and knowing the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of said specified unlawful activity and knowing that the property involved represented the proceeds of some form of unlawful activity; and

b. knowingly and willfully engage and attempt to engage in monetary transactions affecting interstate and foreign commerce in criminally derived property that was of a value greater than $10,000, which was from specified unlawful activity, that is wire fraud in violation of Title 18, United States Code, Section 1343.

The Manner and Means of the Conspiracy

45. The allegations set forth in paragraphs 14 through 19 and 22 through 41 of Count 1 are re-alleged and incorporated herein by reference as constituting the manner and means by which the defendants and other co-conspirators sought to achieve the purpose and object of the conspiracy.

All in violation of Title 18, United States Code, Section 1956(h).

COUNT FOUR
(Conspiracy to Traffic in Counterfeit Services)

The Grand Jury further charges:

46. From in or about February 2007, through in or about July 2008, in the Northern District of Ohio, District of Nevada, the country of Romania, and elsewhere, the defendants, ROMEO VASILE CHITA, a/k/a "Rich," IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a"Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a ""Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," did knowingly and willfully conspire, combine, confederate and agree with each other and with other persons known and unknown to the Grand Jury to intentionally traffic and attempt to traffic in services and knowingly used counterfeit marks on or in connection with such services, in violation of Title 18, United States Code, Section 2320(a).

Manner and Means of the Conspiracy

47. The manner and means by which the defendants and the co-conspirators sought to achieve the purpose and object of the conspiracy included, among others, the allegations set forth in paragraphs 14 through 19 and paragraphs 22 through 41 of Count 1 of this Indictment, which are re-alleged and incorporated herein by reference.

Overt Acts

In furtherance of the conspiracy and to effect the objects thereof, within the Northern District of Ohio, District of Nevada, the country of Romania, and elsewhere, the defendants, ROMEO VASILE CHITA, a/k/a "Rich," IONUT CHERA, a/k/a "Ciceo," CLAUDIU VIRGIL

TURLEA, a/k/a "Biggie," a/k/a "Bigs," a/k/a"Bighi," MANUEL TUDOR, a/k/a "Man," a/k/a ""Manu," a/k/a "Marius," CAROL JURJA, a/k/a "Crapu," DANIEL UNGUREANU, a/k/a "Frank," a/k/a "Dan," DUMITRU NICOLAITA, a/k/a "TB," and others committed at least one of the following overt acts:

48. On or about January 13, 2008, a coconspirator sent a victim in Las Vegas, Nevada, a fake and fraudulent email that displayed the counterfeit service mark of eBay, and instructed the victim to make payment by a wire transfer.

49. On or about January 18, 2008, a coconspirator sent a victim in Somerset, Wisconsin, a fake and fraudulent email that displayed the counterfeit service mark of eBay, and instructed the victim to make payment by a wire transfer.

50. On or about January 26, 2008, coconspirators transported approximately $63,000 in cash in or about Westlake, Ohio.

51. On or about February 11, 2008, a coconspirator sent a victim in McComb, Mississippi, a fake and fraudulent email that displayed the counterfeit service mark of AutoTrader.com and instructed the victim to make payment by a wire transfer.

52. On or about April 15, 2008, a coconspirator sent a victim in Sugar Grove, Illinois, a fake and fraudulent email that displayed the counterfeit service mark of eBay, and instructed the victim to make payment by a wire transfer.

53. On or about April 20, 2008, a coconspirator sent a victim in Port Royal, South Carolina, a fake and fraudulent email that displayed the counterfeit service mark of AutoTrader.com and instructed the victim to make payment by a wire transfer.

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

FORFEITURE ALLEGATIONS

Pursuant to Rule 32.2(a), Federal Rules of Criminal Procedure, notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 1963 and 982; and Title 28, United States Code, Section 2461 and Title 18, United States Code, Section 981, in the event of any defendant's conviction(s) under either Count 1, 2, 3 or 4 of this Indictment. If more than one defendant is convicted of Count 1, 2, 3, or 4 of this Indictment, the defendants so convicted are jointly and severally liable for the amount subject to forfeiture.

Racketeering Forfeiture

1. Pursuant to Title 18, United States Code, Section 1963(a), each defendant who is convicted of the offense set forth in Count 1 of this Indictment shall forfeit to the United States the following property:

(a) Any interest acquired or maintained in violation of Section 1962;

(b) Any interest in, security of, claim against, and property and contractual rights of any kind affording a source of influence over, the Enterprise described in Count 1 which the defendant(s) established, operated, controlled, conducted, or participated in the conduct of, in violation of Section 1962;

(c) Any property constituting, or derived from, proceeds obtained directly or indirectly from racketeering activity in violation of Title 18, United States Code, Section 1962;

(d) The property subject to forfeiture shall include, but not be limited to, the following:

i. A sum of money in the amount of at least $4 million in United States currency, representing the total amount of proceeds obtained by defendants, as a result of their violation of Title 18, United States Code, Section 1962.

All pursuant to Title 18, United States Code, Section 1963.

Wire Fraud Forfeiture

1. Pursuant to the provisions of Title 28, United States Code, Section 2461, and Title 18, United States Code, Section 981(a)(1)(C), each defendant who is convicted of the offense set forth in Count 2 [Wire Fraud (Section 1343) Conspiracy] shall forfeit to the United States the following property:

All property, real and personal, which constitutes or is derived from proceeds traceable to such violation.

(a) The property subject to forfeiture shall include, but not be limited to, the following:

i. A sum of money in the amount of at least $10 million in United States currency, representing the total amount of proceeds obtained by defendants, as a result of their violation of Title 18, United States Code, Section 1349.

All pursuant to the provisions of Title 28, United States Code, Section 2461, and Title 18, United States Code, Section 981(a)(1)(C).

Money Laundering Forfeiture

1. Pursuant to Title 18, United States Code, Section 982(a)(1), each defendant who is convicted of the offense set forth in Count 3 (Money Laundering Conspiracy) shall forfeit to the United States the following property:

(a) All property involved in the offense and all property traceable to such property, including, but not limited to, the following:

i. all money or other property that was the subject of each transaction, transportation, transmission and transfer pursuant to Section 1956(h);

ii. all other property constituting proceeds obtained as a result of those violations; and

iii. all property used in any manner or part to commit or to facilitate the commission of those violations.

All pursuant to Title 18, United States Code, Section 982(a)(1).

Traffic in Counterfeit Services Forfeiture

1. Pursuant to the provisions of Title 28, United States Code, Section 2461 and Title 18, United States Code, Section 981(a)(1)(C), each defendant who is convicted of the offense set forth in Count 4 (Conspiracy to Traffic in Counterfeit Services) shall forfeit to the United States the following property:

All property, real and personal, which constitutes or is derived from proceeds traceable to such violation.

(a) The property subject to forfeiture shall include, but not be limited to, the following:

i. A sum of money representing the total amount of proceeds obtained by defendants as a result of their violation of Title 18, United States Code, Section 371.

All pursuant to the provisions of Title 28, United States Code, Section 2461, and Title 18, United States Code, Section 981(a)(1)(C).

Substitute Property

1. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant(s):

(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; it is the intent of the United States, pursuant to Title 18, United States Code, Section 1963(m), Title 21, United States Code, Section 853(p), and Rule 32.2 Fed. R. Crim. P., to seek forfeiture of any other property of said defendant(s) up to the value of the forfeitable property described above.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.