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

UNITED STATES OF AMERICA,	)	I N D I C T M E N T
	)	
Plaintiff,	)	CASE NO.
	)	
	)	JUDGE
v.	)	
	)	18 U.S.C. § 1343 and 1349,
BOGDAN NICOLESCU,	)	18 U.S.C. § 1030(a)(4),
TIBERIU DANET, and	)	18 U.S.C. § 1030(a)(5),
RADU MICLAUS,	)	18 U.S.C. § 371,
	)	18 U.S.C. § 2320(a)(1),
Defendants.	)	18 U.S.C. § 1028A,
	)	18 U.S.C. § 1956(h),
	)	18 U.S.C. § 3559(g)(1),
	)	18 U.S.C. § 2

The Grand Jury charges:

General Allegations

1. Defendants BOGDAN NICOLESCU (NICOLESCU), TIBERIU DANET (DANET), and RADU MICLAUS (MICLAUS), and others presently known and unknown to the Grand Jury (herein after referred to as the BAYROB GROUP), are members of a criminal conspiracy located in and around Bucharest, Romania.

2. Some of the victims of the criminal schemes carried out by the BAYROB GROUP resided in the Northern District of Ohio. Specifically, some of the computers infected with malware by the BAYROB GROUP were in the Northern District of Ohio, some of the computers accessed by the BAYROB GROUP without authorization were in the Northern District of Ohio, and some of the victims who had their identities, money, or personal identifying

information (PII) stolen by the BAYROB GROUP as a result of these schemes resided in the Northern District of Ohio.

Definitions

For purposes of this Indictment, it is alleged that:

3. "Malware" is malicious or intrusive software that is installed on a computer without the knowledge or permission of the owner.

4. A "trojan" is a type of malware which masquerades as a routine download request or as an opportunity to download files of interest to the user in order to persuade the victim to install it. Many trojans, including the Bayrob Trojan discussed below, act as an unauthorized access point to the victim computer that allows an unauthorized computer to access and communicate with the infected computer.

5. A "botnet" is an interconnected network of computers infected with malware without the knowledge of the computers' users that is controlled by a remote party, often referred to as a "botherder," who does not have authorization to control the computers on the network.

6. A "bot" is one of the infected computers that is part of a botnet and controlled by a remote party who does not have authorization to control the computer. For purposes of this Indictment, all "bots" are infected computers, and all infected computers are bots.

7. A "command and control server" is a centralized computer that issues commands to the bots in a botnet and receives reports back from the bots.

8. A "virtual private network" (VPN) is a technology that creates a secure network connection over a public network such as the Internet or private network owned by an Internet Service Provider. By using a VPN, a user can conceal his true IP address from those with whom he is communicating.

9. An "Internet Service Provider" (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Services commonly provided by ISPs include Internet access, Internet transit, domain name registration, email services, and web hosting.

10. "Internet Protocol Address" (IP Address) is defined as a numerical label assigned to a device logged onto the Internet that provides information that is useful for identifying and locating the device.

11. A "domain name" is used to identify the IP address of a website on the Internet. For example, the domain name "www.google.com" locates an IP address for Google.

12. "Cryptocurrency" is any digital currency in which encryption techniques, known as cryptography, are used to regulate the generation of units of currency and verify the electronic transfer of funds. Examples are Bitcoin and Burst coin.

13. "Cryptomining" is the technique of using a computer's processing power to solve the mathematics behind the generation of cryptocurrency or the validation of cryptocurrency transactions. The solver of the mathematical problem is generally compensated with a small amount of new cryptocurrency, in the case of the initial generation of the currency, or a small percentage of a cryptocurrency transaction between two parties involved in a cryptocurrency transaction.

The BAYROB GROUP

14. In or before 2007, the BAYROB GROUP began to develop and deploy proprietary malware, referred to herein as the "Bayrob Trojan."

15. The BAYROB GROUP disseminated the Bayrob Trojan through malicious emails purporting to be from legitimate entities such as Western Union, Norton AntiVirus, and the United States Internal Revenue Service (IRS). The emails prompted the recipient to click on

an attached file for information about a cash receipt or deficiency. When victims clicked on the attached file, the Bayrob Trojan was surreptitiously installed onto their computer.

16. At all times relevant to this Indictment, the computers infected as part of any and all of the schemes associated with the Bayrob Botnet were used in and affecting interstate and foreign commerce and communication.

17. The Bayrob Trojan allowed the BAYROB GROUP to control and manipulate each bot. Among other things, the BAYROB GROUP used the Bayrob Trojan to harvest email addresses from the bot, such as from the bot's Outlook contact lists or the victim's Yahoo! email account.

18. The Bayrob Trojan forced the infected computer to register email accounts (named based on a Bayrob algorithm) with America Online (AOL). These AOL accounts were then used by the BAYROB GROUP to send additional malicious emails to all of the contacts harvested from the infected computers. This allowed the BAYROB GROUP to continually infect more computers.

19. Since at least 2007, the BAYROB GROUP has successfully infected and controlled more than 60,000 individual computers with versions of the Bayrob Trojan. These infected computers were located primarily in the United States. Collectively, this network of more than 60,000 computers is referred to as the Bayrob Botnet.

The Structure of the Bayrob Botnet

20. The Bayrob Botnet is centrally controlled by the BAYROB GROUP through one or more command and control servers (C&C servers), which enable the BAYROB GROUP to send code and issue commands to any or all bots in the Bayrob Botnet.

21. To ensure the stability and reliability of the Bayrob Botnet against disruption by law enforcement or other interruptions, the BAYROB GROUP paid to have their C&C servers

hosted by reliable Internet Service Providers in the United States, maintained redundant C&C servers with different ISPs, and regularly backed up the data and information on those servers.

22. In addition, to ensure reliability and anonymity, the BAYROB GROUP used at least two levels of C&C servers. The BAYROB GROUP communicated with the top-level C&C servers. The messages, updates, or commands provided by the BAYROB GROUP were then sent from the top-level C&C servers to the second-level C&C servers (or relays). The second-level servers, serving as a relay between the top-level C&C servers and other tiers of bots, then pushed those communications to the bots. In this way, an infected computer could, at best, be used to investigate the IP address of a second-level C&C server, but could not identify the top-level C&C servers or the BAYROB GROUP, itself.

23. In order to receive commands from the BAYROB GROUP, the bots automatically checked in with Internet domains registered by the BAYROB GROUP via infected computers, using stolen identity and credit card information. These domains were automatically generated by the Bayrob Trojan's Domain Generation Algorithm (DGA) and had nonsensical names such as storeladder.net, lookuncle.net, or necessaryfather.net. Upon successfully contacting a domain registered and controlled by the BAYROB GROUP, the bot was able to connect to a second-level C&C server, and receive commands from the BAYROB GROUP.

24. Furthermore, to conceal their identities, members of the BAYROB GROUP never communicated directly with the C&C servers. Instead, members connected using multiple proxies to obscure their identities. For example, BAYROB GROUP members logged into one or more encrypted VPNs and/or infected computers before logging into the C&C server.

25. Additionally, communication between BAYROB GROUP members and the BAYROB GROUP infrastructure used Secure Shell (SSH), which is an encrypted network

protocol to allow remote login and other network services to operate securely over an unsecured network.

26. Furthermore, when communicating with each other, members of the BAYROB GROUP used secure end-to-end encryption, encrypted any attachments, and used other secure methods of communication, including an instant messaging technology known as Jabber, which the BAYROB GROUP administered through a private and secure server.

27. At all times relevant to this Indictment, the Defendants did not seek, nor were they given, permission to install the Bayrob Trojan on victims' computers or to use the victims' computers as part of the Bayrob Botnet.

28. In addition to enabling further infection, the Bayrob Trojan allowed the BAYROB GROUP to: (a) harvest personal information from the infected computer (e.g., credit card information, usernames, passwords, and email accounts); (b) communicate through the infected computer to conceal the identity of the BAYROB GROUP's members; (c) order the infected computer to send out malicious emails or instant messages to a list of target accounts; (d) use the processing power of the computer to solve complex algorithms for the financial benefit of the BAYROB GROUP, (i.e., cryptocurrency mining); (e) disable the victim's malware protection and block the victim's access to websites associated with law enforcement; and (f) inject fake pages into legitimate websites, such as eBay, to make victims believe they were receiving and following instructions from the legitimate websites, when they were actually following the instructions of the BAYROB GROUP.

29. The BAYROB GROUP also designed the Bayrob Trojan to link the infected computers into a network, referred to as a "botnet" (the "Bayrob Botnet"), to enable the entire network of infected computers to be centrally controlled by the BAYROB GROUP through one or more C&C servers located in the United States.

30. Among other things, this structure allowed members of the BAYROB GROUP to efficiently send commands or updates to any and all bots in the botnet without directly revealing the ultimate source of the directive.

The Bayrob Botnet Furthered Three Criminal Schemes

31. The BAYROB GROUP relied on the Bayrob Botnet to further three basic criminal schemes designed to defraud victims.

Identity Theft Scheme

32. The first scheme engaged in by the BAYROB GROUP involved the theft of credit card and other personal account access information from infected computers. When a victim with an infected computer visited websites such as Facebook, PayPal, Gmail, Yahoo!, Walmart, or eBay, the Bayrob Trojan would intercept the request to visit that website and redirect the system to a virtually identical website created by the BAYROB GROUP, which would steal account credentials or prompt the users to validate their accounts by entering their identities and credit card information. The BAYROB GROUP used these stolen credit cards and identities to fund their online criminal infrastructure, including renting server space, paying for VPNs which further concealed their identities, and registering domain names using fictitious and fraudulent identities.

33. At all times relevant to this Indictment, eBay, Facebook, PayPal, Gmail, Google, Walmart, Western Union, Norton Security, and Yahoo! all had trademarks and service marks registered on the principal register of the United States Patent and Trademark Office (USPTO). These marks were in use by the trademark holders, or their licensee, at all relevant times to this Indictment, and were used in connection with the type of goods or services for which the marks were registered.

34. At all times relevant to this Indictment, NICOLESCU, DANET, and MICLAUS did not have authorization to use any trademark or service mark registered on the principal register of the USPTO by eBay, Facebook, PayPal, Gmail, Google, Walmart, Western Union, Norton Security, or Yahoo!.

Auction Fraud Scheme

35. The BAYROB GROUP's second scheme involved online auction fraud. The BAYROB GROUP placed hundreds or thousands of listings for automobiles, motorcycles, and other high priced goods on eBay and similar auction sites. Photographs of the items were infected with the Bayrob Trojan. Once infected, victim computers were redirected to fictitious webpages using counterfeit service marks designed by the BAYROB GROUP to resemble legitimate eBay pages. The fictitious webpages prompted users to pay for the goods through a non-existent "eBay Escrow Agent," who was supposed to hold the money until the buyer received the item and confirmed his or her satisfaction, but who, in reality, was a person hired by the BAYROB GROUP.

36. To further give the veneer of legitimacy to the fraudulent webpage, the BAYROB GROUP created software that allowed users to use "eBay Live Chat" in real time with members of the BAYROB GROUP holding themselves out to be customer service agents of eBay.

37. Believing the remitted funds would be sent to an eBay escrow agent, the user paid for the goods, sending wire transfers to individuals employed by the BAYROB GROUP in the United States, commonly referred to as "money mules." The money mules, in turn, sent funds via wire transfers or Western Union to money mules based in Eastern Europe, who withdrew the money and gave it to members of the BAYROB GROUP. Ultimately, the payors/victims never received the items for which they paid, and never got their money back.

38. The domestic money mules were often unsuspecting participants in the criminal scheme because the BAYROB GROUP recruited them through seemingly legitimate companies advertising on Monster.com, Craigslist.com, Indeed.com, and Beyond.com. These fake companies created by the BAYROB GROUP, each having its own legitimate-appearing website, purported to hire individuals as "international transfer agents" who would allegedly allow the company to legally avoid paying Value Added Tax (VAT) on international wire transfers.

39. From 2007 to the present, the fraudulent schemes of the BAYROB GROUP have resulted in at least 3 to 4 million dollars in fraudulent eBay schemes reported to the FBI.

Cryptomining Scheme

40. The third scheme employed by the BAYROB GROUP involved forcing computers infected with the Bayrob Trojan to use their computing power to "mine" for cryptocurrency, a service for which the BAYROB GROUP was paid. Once a bot was instructed to mine for cryptocurrency, much of its processing speed and power would be unavailable to its legitimate owner.

41. The legitimate owner of an infected computer was typically completely unaware of the malware installed on their computer, nor was the owner able to access the botnet or use the functionality of the botnet for any personal benefit.

COUNT 1

(Conspiracy to Commit Wire Fraud, 18 U.SC. §§1343 and 1349)

42. Paragraphs 1 through 41 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

43. From on or about January 1, 2007, through the date of the Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did knowingly combine, conspire, confederate, and agree to devise and intend to devise a scheme and artifice to defraud and to obtain money and property, by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signals, signs, pictures, and sounds, that is, to knowingly cause computer commands to be transmitted from outside of the State of Ohio to computers in the Northern District of Ohio, in violation of Title 18, United States Code, Sections 1343 and 1349.

Objects of the Conspiracy

44. The BAYROB GROUP executed its scheme for four principal objects. The four objects, described below, are generally referred to as the "Infection Scheme," the "Identity Theft Scheme," the "Online Fraud Scheme," and the "Cryptocurrency Mining Scheme."

45. It was an object of the conspiracy that the BAYROB GROUP used wire communications to deploy malware in order to control computers and obtain online account information from infected computers without permission of the owners, in order to infect and control additional computers.

46. It was a further object of the conspiracy for the BAYROB GROUP to use wire communications to command infected computers to send malicious emails and inject fraudulent

webpages to deceive users into providing credit card information, usernames, passwords, account information, and other personal information. The BAYROB GROUP used this information to, among other things, support the infrastructure of the Bayrob Botnet and Bayrob Trojan.

47. It was a further object of the conspiracy for the BAYROB GROUP to deploy code over wire communications that altered the appearance of webpages and online transactions on infected computers. The users of the infected computers viewed what they believed to be legitimate online offerings of goods, but as a result of the malware, they were deceived into sending thousands of dollars via wire to pay for expensive goods that were never provided.

48. It was a further object of the BAYROB GROUP to infect computers with malware that damaged the infected computer by, among other things, stealing any cryptocurrency on the infected computer, and forcing each infected computer to use its processing power to assist the BAYROB GROUP in the widespread mining of cryptocurrencies for the sole financial benefit of the BAYROB GROUP. The BAYOB GROUP knew that using the infected computers to mine cryptocurrency would damage the infected computers and intentionally caused such damage.

49. To achieve these objects, members of the BAYROB GROUP employed an extensive and sophisticated manner of communication, software installation, and money remittance that was designed to obscure their identities and make it difficult to trace their routes of communication from computer to computer over the Internet.

Manner and Means of the Conspiracy

50. It was part of the conspiracy that, in furtherance of the scheme and artifice described in Paragraphs 1 through 41 herein, the Defendants developed and updated the Bayrob Trojan malware that, when installed on an infected computer, was designed to both receive commands and send information from the infected computer back to the BAYROB GROUP.

51. The members of the BAYROB GROUP sent, and directed other computers to send, malicious emails or instant messages through the Internet in order to trick victims into running a malicious executable file on their computers in order to gain unauthorized access to the victims' computers and all the information stored thereon, or to trick the victims into providing them with account information.

52. The malicious emails purported to be from legitimate companies or U.S. federal agencies, and contained seemingly authentic logos and other indicia of reliability. The malicious emails encouraged recipients to open attachments to obtain important information. In addition, the malicious emails concealed the material fact that the attachments were intentionally embedded with malicious code.

53. Once each computer was infected with the Bayrob Trojan, the BAYROB GROUP harvested email addresses from the infected machine, or associated online email services. To harvest the email addresses, the BAYROB GROUP activated plugins, such as "Yahoomailcrawler.js," which used stolen email credentials to copy a victim's Yahoo! email contacts. A similar plugin for Microsoft Outlook, "libpff," collected Outlook email contacts from infected computers.

54. Through the Bayrob Trojan, the BAYROB GROUP also activated files that forced infected computers to register email accounts with America Online (AOL). Using this method, the BAYROB GROUP was able to command infected computers to register over 100,000 email accounts that were controlled by the BAYROB GROUP.

55. The BAYROB GROUP, through the C&C server, commanded the infected computers to send malicious email to their contact lists. Through this method, the BAYROB GROUP used the Bayrob Botnet to send more than 11 million malicious emails.

56. These malicious emails provided a method through which infected computers under the control of the BAYROB GROUP were continually being created.

57. Once a computer was infected, exfiltration of credit card or account information was primarily accomplished through "injection." The C&C server was configured to "set_injects" or website injections for certain sites. A member of the BAYROB GROUP had to manually enter a database on the C&C server, and turn on "injections." Once injections were turned on, when an infected system visited Facebook, for example, the Bayrob Trojan intercepted the request and redirected the system to a non-Facebook server provided by the BAYROB GROUP, which would prompt victims to validate their account by entering their identity and credit card information.

58. The credit card information was collected by the BAYROB GROUP and used to fund their online criminal infrastructure, allowing the BAYROB GROUP to fund the renting of server space, the use of VPNs which further concealed their identities, and the registering of domain names using fictitious and fraudulent identities.

59. The BAYROB GROUP also used injection to collect account access credentials (e.g., usernames and passwords) for a number of online services including Facebook, PayPal, eBay, Yahoo!, Hotmail, and Gmail. These accounts were then primarily used to harvest additional target email addresses for malicious email campaigns, or to send malicious instant messages to victims' instant messaging contacts.

60. The BAYROB GROUP also relied on the Bayrob Trojan to facilitate online auction fraud. The BAYROB GROUP placed over 1,000 listings for non-existent automobiles and other expensive items on websites such as eBay. When consumers clicked on photo viewer attachments associated with the listings, their computers became infected with a version of the Bayrob Trojan.

61. Once infected, the victims' computers were redirected to fraudulent eBay webpages which appeared legitimate, but contained false information.

62. The fraudulent eBay pages were designed to mimic authentic eBay pages and contained a number of features intended to lull the user into a false sense of security. These fraudulent features included links to fictitious positive seller reviews, live chats with an eBay agent, and an "eBay Escrow Agent Protection" function, ostensibly to securely pay for the auction items.

63. In reality, the "eBay Escrow Agent" function was an entirely fictitious service created by the BAYROB GROUP to funnel payments from unwitting victims through money mules working for sham transfer agencies created by the Defendants.

64. The BAYROB GROUP also used the Bayrob Trojan to install cryptomining tools on infected computers which used the computing power of the infected computers to mine cryptocurrencies. As with injection, a member of the BAYROB GROUP had to manually activate the cryptocurrency mining option. Once mining was activated, the bots would be directed to download and run new software in order to begin mining.

65. Additionally, the malicious software searched the infected computer for existing cryptocurrency "wallets," and transferred those wallets to members of the BAYROB GROUP without the owner's permission.

66. In order to achieve the objects of this conspiracy, members of the BAYROB GROUP relied on several manners and means to evade detection by both victims and law enforcement.

67. These efforts included: (a) using stolen credit cards and false credentials to pay for servers, domains, VPNs, and other infrastructure; (b) using multiple proxies to communicate, including the C&C server, infected computers, commercial VPNs, and commercial proxies (e.g.,

AOL); (c) encrypting emails and attachments, and communicating over an encrypted private messaging server located in a Romanian apartment protected with a high security lock; (d) using cryptic subject headers for emails; (e) using different monikers when communicating over different channels; (f) regularly moving infrastructure and changing communication channels to avoid detection; (g) maintaining strict silence about criminal activity and infrastructure when communicating over the telephone; (h) using U.S.-based and foreign money mules; and (i) installing malware on victims' computers to disable access to law enforcement websites.

Execution of the Scheme

Defendants committed and attempted to commit various acts in furtherance of the conspiracy in the Northern District of Ohio, and elsewhere, including:

68. From January 1, 2007, through the date of this Indictment, from outside the United States, the BAYROB GROUP used networked facilities located in the United States to send encrypted emails amongst each other. The encrypted emails related to such topics as the infection of victim computers, personal identification information from victims, and maintenance of the Bayrob Botnet and the Bayrob C&C.

Infection Scheme

69. On or about March 7, 2014, the C&C server began deploying a file entitled "casper.js" to infected computers. The "casper.js" file contained computer code used by the BAYROB GROUP to further the infection scheme by instructing infected systems to do various tasks such as automatically register domains using Yahoo!, stealing email data from stolen Yahoo! and Gmail accounts, making the systems click on advertisements, and harvesting email accounts from websites on the Internet to further the conspiracy.

70. Between September 11, 2014 and September 24, 2014, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a

C&C Server located in the United States and deployed a malicious file entitled "wu00[x].htm," which was an email template used by the BAYROB GROUP to cause bots in the Bayrob Botnet to send malicious email purporting to be from Western Union. The emails indicated the recipient had received money and included an attachment, which was to be printed out and taken to Western Union in order to receive the funds. In reality, the attachment installed malware on the recipient's computer.

71. On or about January 13, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C Server in the United States and deployed a malicious file entitled "norton01.htm," which was an email template used by the BAYROB GROUP to cause bots in the Bayrob Botnet to send malicious email purporting to be from Norton AntiVirus. The email indicated the recipient was entitled to a year of free computer virus protection and provided a link to obtain it. In reality, the link installed malware on the recipient's computer.

72. On or about January 13, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C Server in the United States and deployed a malicious file entitled "irs0[x].htm," which was an email template used by the BAYROB GROUP to cause bots in the Bayrob Botnet to send malicious email purporting to be from the IRS. The email indicated the recipient was being served with a "Notice of Deficiency" and included an attachment explaining the deficiency. In reality, the link installed malware on the recipient's computer.

73. On or about January 14, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C Server in the United States and deployed a malicious file entitled "flappy0[x].htm," which was an email template used by the BAYROB GROUP to cause bots in the Bayrob Botnet to send malicious

email purporting to be from a video game producer. The email template encouraged the recipient to install an attachment which was purportedly a game entitled "Flappy Bird." In reality, the attachment installed malware on the recipient's computer.

Identity Theft Scheme

74. Between May 2013 and April 2014, the BAYROB GROUP created workspaces on the C&C servers to allow members of the BAYROB GROUP to perform tasks on the C&C server. One set of files using such workspace on the C&C server was titled "hosting.txt," and contained files with personal identifying information for over 40 individuals, including records of stolen credit cards that were used to register the domains. The following "hosting.txt" files were identified:

../phantomjs/workspace/**amy**/yahoo.hosting/hosting.txt

../phantomjs/workspace/**mf**/yahoo.hosting/hosting.txt

../phantomjs/workspace/**min**/yahoo.hosting/hosting.txt

The above directory structure indicated that DANET (amy), NICOLESCU (mf), and MICLAUS (min) all had their own workspace, and all were directly involved in registering domains using stolen credit card information in support of the BAYROB GROUP's operations.

75. On or about July 23, 2013, from outside the United States, a member of the BAYROB GROUP logged into a C&C server located in the United States and created a back-up of 59 individual database tables entitled "abcdef.sql." These tables included "my_4_mules," "cc," "sox3_ping," and "auto_listings" on the C&C server. These tables contained information about stolen credit cards, malicious software code to be deployed, and templates used in past and to be used in future auto auction fraud schemes.

76. On or about March 7, 2014, the C&C server began deploying a file entitled "casper.js" to infected computers. The "casper.js" file contained computer code used by the

BAYROB GROUP to further the identity theft scheme by instructing infected systems to do various tasks such as automatically register domains using Yahoo!, stealing email data from stolen Yahoo! and Gmail accounts, making the systems click on advertisements, and harvesting email accounts from websites on the Internet to further the conspiracy.

77. On or about and between May 2014 and June 2014, from outside the United States, the BAYROB GROUP, communicating through a C&C server located in the United States, sent "yahoomailcrawler.js," a malicious plugin that targeted Yahoo! mail accounts, to infected systems over 10,000 times and received communications containing collected data over 10,000 times.

78. On or about and between March 14, 2014 and August 19, 2014, from outside the United States, members of the BAYROB GROUP commanded a C&C server located in the United States to send "cc_page.htm"—a phishing page purporting to seek credit card and PII data to verify a user's eBay account—over 200 times to infected victim systems.

79. On or about and between October 21, 2014 and October 23, 2014, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C server located in the United States and deployed a malicious file entitled "walmart0[x].htm," which caused bots in the Bayrob Botnet to inject fictitious webpages advertising electronics for sale at Walmart.com. Victims were prompted by the injected webpage to enter their personal identifying information and credit card information, which information was then provided to the BAYROB GROUP.

80. On or about January 20, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C server in the United States and deployed a malicious file entitled "walmart0[x].htm," which was used by the BAYROB GROUP to cause bots in the Bayrob Botnet to inject fictitious webpages advertising

electronics for sale at Walmart.com. Victims were prompted by the injected webpage to enter their personal identifying information and credit card information. This information was then provided to the BAYROB GROUP.

Cryptomining Scheme

81. On or before January, 2014, the BAYROB GROUP began to use infected systems in the Bayrob Botnet to mine for cryptocurrency. The BAYROB GROUP instructed infected systems to download and run cryptocurrency miners, using the processing power of the infected systems to earn cryptocurrencies for the financial gain of the BAYROB GROUP. The BAYROB GROUP used the Bayrob Botnet to mine a number of different cryptocurrencies, including Bitcoin, Monero, Darkcoin, Yacoin, as well as other currencies. The mining of cryptocurrencies resulted in the target computers being unusable or extremely slow.

Auction Fraud Scheme

82. On or about the dates listed below, the BAYROB GROUP, for purposes of executing the Auction Fraud scheme, caused the following individuals, whose identities are known to the Grand Jury, through the use of the following email addresses controlled by the BAYROB GROUP, to send money to money mules for vehicles that did not exist and were not actually for sale:

Approximate Date	**Victim**	**Email Used By Bayrob Group (full address known by the grand jury)**	**Vehicle**	**Money Mule**	**Approximate Amount**
7/11/2013	R.M.	MH1@aol.com	1965 Ford Mustang	D.W.	$9,200
8/1/2013	M.B.	CF1@aol.com	unknown vehicle	D.W.	$10,700
8/1/2013	T.V.	PY@aol.com	1971 Dodge Charger	H.P.	$7,000

Effect of the Scheme

83. As a result of the scheme, the BAYROB GROUP sent millions of malicious emails and infected more than 60,000 computers. In addition, the BAYROB GROUP obtained credit card information from over 500 victims, as well as personal identifying information from tens of thousands of victims. Furthermore, the BAYROB GROUP engaged in malware-enabled online auction fraud more than 1,000 times and derived at least 3 to 4 million dollars from the scheme. As a result of cryptocurrency mining, more than 33,000 infected computers were damaged due to loss of processing power.

All in violation of Title 18, United States Code, Sections 1343 and 1349.

COUNTS 2-13
(Wire Fraud, 18 U.S.C. §1343)

The Grand Jury further charges that:

84. Paragraphs 1 through 41 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

85. From on or about January 1, 2007, through the date of the Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud and to obtain money by means of materially false and fraudulent pretenses, representations and promises, and transmitted and caused to be transmitted by means of wire and radio communications in interstate commerce, writings, signals, signs, and pictures, for the purposes of executing such scheme and artifice in violation of Title 18, United States Code, Section 1343.

Manner and Means of the Scheme

86. To accomplish these objectives the BAYROB GROUP employed the manner and means described in Paragraphs 1 through 41, 50 through 65, and 67 of the Indictment which are re-alleged and incorporated by reference as if fully set forth herein.

Execution of the Scheme

87. On or about the following dates, victims transferred funds to U.S.-based money mules working for the BAYROB GROUP via wire transfer under the incorrect belief that they were purchasing an actual item listed on the authentic eBay site. In reality, each transaction involved a non-existent item listed on a fraudulent eBay page, created by the BAYROB GROUP, which was injected onto the victim computer by the Bayrob Trojan; each of which was an interstate or foreign wire communication constituting a separate and distinct offense:

Count	Approximate Date	Source of Funds	Recipient of Funds	Approximate Amount of Transaction
2	7/5/2013	Victim #2 D.P. Webster, NY Victim Bank Unknown	D.W. Charter One Bank Account #: XXXXXX0118 Cleveland, Ohio	$7,858.50
3	7/6/2013	Victim #5 R.M. Seal Beach, CA	D.W. Charter One Bank Account #: XXXXXX0118 Cleveland, Ohio	$9,269.00
4	7/8/2013	Victim #1 J.C. Bythe, CA Victim Bank Unknown	D.W. Charter One Bank Account #: XXXXXX0118 Cleveland, Ohio	$7,254
5	7/9/2013	Victim #3 A.K. Jefferson, ME TD Bank	D.W. US Bank Account #:XXXXXXXX1134 Cleveland, Ohio	$ 8,852.30
6	7/14/2013	Victim #6 M.H. Saint Charles, MO	D.W. US Bank Account #:XXXXXXXX1134 Cleveland, Ohio	$7,808.13
7	7/14/2013	Victim #7 C.R. Webster, MA	D.W. US Bank Account #:XXXXXXXX1134 Cleveland, Ohio	$7,707.38
8	7/14/2013	Victim #8 S.W. Abilene, TX	D.W. Charter One Bank Account #: XXXXXX0118 Cleveland, Ohio	$2,484.00
9	7/14/2013	Victim #9 M.M. Reno, NV	D.W. PNC Account #:XXXXXX5205 Cleveland, Ohio	$5893.88
10	7/14/2013	Victim #10 T.H. Bedford, NY	D.W. Charter One Bank Account #: XXXXXX0118 Cleveland, Ohio	$9,350
11	7/14/2013	Victim #11 J.R. Renton, WA	D.W. Key Bank Cleveland, Ohio	$6,000.00

Count	Approximate Date	Source of Funds	Recipient of Funds	Approximate Amount of Transaction
12	7/14/2013	Victim #12 W.P. New Orleans, LA	D.W. Key Bank Cleveland, Ohio	$12,500.00
13	8/11/2013	Victim #4 M.B. Tyler, TX Victim Bank Unknown	D.W. PNC Account #:XXXXXX5205 Cleveland, Ohio	$10,729.88

All in violation of Title 18, United States Code, Section 1343.

COUNT 14
(Conspiracy)
(18 U.S.C. §371)

The Grand Jury further charges that:

88. Paragraphs 1 through 41, 50 through 65, and 67 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

89. From on or about January 1, 2007, through the date of the Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, knowingly and intentionally conspired and agreed together and with each other, and with other persons both known and unknown to the Grand Jury, to violate the laws of the United States, namely:

(i) to intentionally access a computer without authorization, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C); and

(ii) to intentionally access a computer without authorization and by means of such conduct furthered the intended fraud and obtained something of value, specifically, money, in excess of 3 to 4 million dollars, in violation of Title 18, United States Code, Section 1030(a)(4); and

(iii) to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and the offense caused damage affecting ten or more protected computers in a one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B).

Objects of the Conspiracy

90. It was the object of the conspiracy for Defendants to access computers and steal personal identifying information, credit card information, and cryptocurrencies to use for their commercial advantage and private financial gain.

91. It was a further object of the conspiracy to use the Bayrob Trojan to deceive users of infected computers to send money and other things of value to members of the BAYROB GROUP.

92. It was an additional object of the conspiracy to infect computers with malware that allowed members of the BAYROB GROUP to use infected computers to mine cryptocurrencies for their own personal gain, but to the detriment of the infected computer's processing power.

Manner and Means of the Conspiracy

93. Paragraphs 50 through 65 and 67 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

94. In order to gain access to victim computers without authorization, the BAYROB GROUP employed several techniques.

95. From on or about January 1, 2007, through the date of the Indictment, the BAYROB GROUP collected account access credentials in the form of usernames and passwords for a number of online services to include Facebook, PayPal, eBay, Yahoo!, Hotmail, and Gmail.

96. When an infected computer attempted to visit Facebook, Paypal, eBay, Yahoo!, Hotmail, or Gmail, the Bayrob Trojan would redirect the user to a web page provided by the BAYROB GROUP, which contained counterfeit trademarks and service marks that deceived the user into believing they were on the authentic website. Thus deceived, the victims would

provide their account information and additional verification information, all of which was collected by the BAYROB GROUP.

97. The BAYROB GROUP deployed these fraudulent webpages purporting to be legitimate eBay, Facebook, Gmail, and other sites at least 40,000 times, in an effort to deceive victims into sending them their personal credit card information, account information, or to install malware on their computers.

98. Likewise, members of the BAYROB GROUP placed hundreds or thousands of fraudulent advertisements on eBay for non-existent automobiles for sale by online auction.

99. The automobile listings generated multiple requests and bids from potential unsuspecting purchasers, however, in the end there were no actual auction winners, either because the auction's reserve price was intentionally set too high, or the auction was won by an account created by the BAYROB GROUP to ensure they would win.

100. The BAYROB GROUP would then email every person who bid or requested information regarding the item. The email explained that the item was still available and could be purchased through eBay. The email also contained an attachment with pictures of the car, or a link to a website to see pictures of the car. When the victim clicked the link or attachment to see the pictures, they were instructed to download a picture viewer which showed pictures of the vehicle, which simultaneously infected their computer with a particular version of the Bayrob Trojan, designed to defraud online commerce victims.

101. By infecting these computers with the Bayrob Trojan, the BAYROB GROUP intended to inject webpages and other content to deceive the victims into wiring them more than $5,000 each for expensive items that never existed.

102. Members of the BAYROB GROUP sent spam emails purporting to be from legitimate companies concerning urgent information about the recipient. By clicking on the link about the information, the victim would unwittingly install the Bayrob Trojan.

Overt Acts

103. On or about the following dates and in the Northern District of Ohio and elsewhere, members of the BAYROB GROUP infected the computers of the listed victims, whose identities are known to the Grand Jury, and were able to gain unauthorized access to their computers, each constituting a separate act in furtherance of the conspiracy:

Victim ID	Location	Approximate Date of Infection
L.G.E.	Kenton, OH	5/31/2013
N.M.A.	Painesville, OH	5/31/2013
A.V.C	Fremont, OH	6/10/2013
M.D.P.	Toledo, OH	6/19/2013
D.A.V.	Youngstown, OH	6/20/2013
J.B.I.	New Bremen, OH	6/23/2013
O.H.I	Mentor, OH	6/29/2013
P.E.S.	Chardon, OH	6/29/2013
B.O.W.	Tallmadge, OH	7/2/2013
B.O.N	Youngstown, OH	7/3/2013
K.J.B.	Massillon, OH	7/3/2013
S.P.A.	Lakewood, OH	7/10/2013
E.A.R.	Avon, OH	7/12/2013
S.N.Y.	Louisville, OH	7/17/2013
D.E.N.	Bryan, OH	7/19/2013
P.H.A.	Lima, OH	7/28/2013
B.U.I	Toledo, OH	7/30/2013
S.G.A.	Findlay, OH	7/30/2013
T.S.C.	Cleveland, OH	7/30/2013
T.R.I	Cuyahoga Falls, OH	8/7/2013
D.E.L.	Findlay, OH	8/12/2013
B.I.G.	Toledo, OH	8/12/2013
L.A.R.	Wapakoneta, OH	9/27/2013
B.T.H	Kent, OH	10/17/2013
E.W.A.	Westlake, OH	11/7/2013
R.O.N.	Youngstown, OH	11/8/2013
T.H.E.	Northwood, OH	11/8/2013

104. Between 2014 and 2015, members of the BAYROB GROUP, through unauthorized access to computers created by the Bayrob Trojan, installed an additional file entitled "miner_forced" on at least 33,000 computers, including the infected computers below, to force the computers to use their computing power to mine for cryptocurrency, thereby damaging the infected computers by significantly decreasing the processing power available to the user, and each constituting a separate act in furtherance of the conspiracy

Bayrob's Assigned Victim ID	Location	Approximate Date of Cryptomining Inject
820283904	Akron, OH	February 21, 2014
524900352	Grand River, OH	March 5, 2014
274822144	Helena, OH	November 20, 2014
1218086401	Cleveland, OH	December 17, 2014
1219513346	Toledo, OH	December 17, 2014
1254965760	New Philadelphia, OH	March 1, 2015
1255713792	Beachwood, OH	March 5, 2015
1257811968	Mansfield, OH	March 5, 2015
1231890944	Toledo, OH	March 5, 2015
1227656704	Fremont, OH	March 5, 2015
1211592704	Magnolia, OH	March 5, 2015
1228333057	Cleveland, OH	March 5, 2015
1229966336	Cleveland, OH	March 6, 2015
1237189632	Toledo, OH	March 6, 2015
451089408	Saint Mary, OH	March 6, 2014
1223239168	Toledo, OH	March 6, 2015
431675402	Cleveland, OH	March, 30, 2014
822290433	Sycamore, OH	April 4, 2014
1011375617	Avon Lake, OH	Between 2014-2015
1197571072	Toledo, OH	Between 2014-2015
1197983235	Independence, OH	November 20, 2014
1218005504	Akron, OH	Between 2014-2015
1223293952	Macedonia, OH	Between 2014-2015
1227095552	Cleveland, OH	Between 2014-2015
1227706368	Cleveland, OH	Between 2014-2015
1228264960	Youngstown, OH	Between 2014-2015
1228651008	Geneva, OH	Between 2014-2015
1228895744	Youngstown, OH	Between 2014-2015
1228931584	Willoughby, OH	Between 2014-2015
1228968960	Canfield, OH	Between 2014-2015
1229006336	Akron, OH	Between 2014-2015
1229018624	Cuyahoga, OH	Between 2014-2015

Bayrob's Assigned Victim ID	Location	Approximate Date of Cryptomining Inject
1229064704	Bloomville, OH	Between 2014-2015
1229130240	Toledo, OH	Between 2014-2015
1229373952	Ashtabula, OH	Between 2014-2015
1229694464	Cleveland, OH	Between 2014-2015
1229770752	Cleveland, OH	Between 2014-2015
1229927424	Hubbard, OH	Between 2014-2015
1231949312	Canton, OH	Between 2014-2015
1232317952	Toledo, OH	Between 2014-2015
1232367616	Strongsville, OH	Between 2014-2015
1232616960	Lima, OH	Between 2014-2015
1248447488	Cleveland, OH	Between 2014-2015
1248764930	Cleveland, OH	Between 2014-2015
1257831937	Toledo, OH	Between 2014-2015
1262999040	Cleveland, OH	Between 2014-2015
1250711040	North Olmsted, OH	February 28, 2015

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

COUNT 15

(Conspiracy to Traffic in Counterfeit Service Marks, 18 U.SC. § 2320(a)(1))

The Grand Jury further charges that:

105. Paragraphs 1 through 41, of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

106. On or about the January 1, 2007, through the date of the Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did conspire to intentionally traffic in services, namely internet commerce services, knowingly using counterfeit marks on and in connection with such services, in violation of Title 18, United States Code, Section 2320(a)(1).

Objects of the Conspiracy

107. It was an object of the conspiracy for the BAYROB GROUP to use the counterfeit trademarks and service marks of Western Union and Norton AntiVirus to provide seemingly-legitimate communications to deceive victims into clicking on links or attachments that installed malware on their computers.

108. It was a further object of the conspiracy for the BAYROB GROUP to use counterfeit trademarks and service marks of eBay, Facebook, PayPal, Gmail, Google, Yahoo!, and Walmart to deceive online consumers to send credit card account information, personal identifying information, or wire transfers to members of the BAYROB GROUP posing as legitimate online companies.

109. It was a further object of the BAYROB GROUP to use counterfeit trademarks and service marks of Google and Yahoo! to deceive job-seekers into providing bank account information, personal information, conducting wire transfers, and unwittingly participating in a criminal conspiracy.

Manner and Means of the Conspiracy

110. Paragraphs 50 through 65 and 67 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

111. To accomplish these objectives, the BAYROB GROUP used fraudulent webpages and emails that contained counterfeit trademarks and service marks that were not genuine or authentic.

112. The fraudulent trademarks and service marks on the webpages and emails were designed to be substantially indistinguishable from the legitimate marks, and in fact, the webpages and emails themselves appeared to contain identical or similar functionalities as the webpages and emails used by the legitimate mark holders.

113. The BAYROB GROUP further enhanced the seeming legitimacy of the counterfeit trademarks and service marks by employing them in the same types of services for which the legitimate mark holders had registered and used such marks.

114. By making the counterfeit marks substantially indistinguishable from the authentic marks, the BAYROB GROUP deceived victims into either sending personal information or money to the BAYROB GROUP or installing malware onto their computers that furthered the BAYROB GROUP's criminal schemes.

115. Additionally, the BAYROB GROUP used counterfeit marks to further their money laundering scheme. On or before October 2014, members of the BAYROB GROUP injected fraudulent Google and Yahoo! pages when users of infected computers attempted to visit those websites. The injected pages contained counterfeit Google and Yahoo! marks, and otherwise appeared to function normally, except the pages contained advertisements in which Google and Yahoo! purported to be hiring "financial agents" to receive wire transfers and send them to "European clients" via Western Union. The advertisements suggested that those hired

could make between $2,000 and $3,500 per month. Individuals responding to the advertisements provided the BAYROB GROUP with their personal information, bank account information, and some were unwittingly used to wire transfer the criminal proceeds of the BAYROB GROUP's scheme to Romania and elsewhere in Europe.

Acts in Furtherance of the Conspiracy

116. Between on or about September 11, 2014, and on or about September 24, 2014, from outside the United States members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C Server located in the United States, and deployed a malicious file entitled "wu00[x].htm," which was an email template used by bots in the Bayrob Botnet to send malicious email purporting to be from Western Union. The email contained a counterfeit "Western Union" mark, indicated the recipient had received money, and provided an attachment with information on how to obtain it. In reality, the attachment installed malware on the recipient's computer.

117. Between on or about October 21, 2014, and on or about October 23, 2014, from outside the United States members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C server located in the United States, and deployed a malicious file entitled "walmart0[x].htm," which was used the BAYROB GROUP to cause bots in the Bayrob Botnet to inject fictitious webpages advertising electronics for sale at Walmart.com. Victims were prompted by the injected webpage, which contained a counterfeit "Walmart" mark, to enter their personal identifying information and credit card information, which information was then provided to the BAYROB GROUP.

118. On or about January 13, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C Server in the United States and deployed a malicious file entitled "norton01.htm," which was an email

template used by the BAYROB GROUP to cause bots in the Bayrob Botnet to send malicious email purporting to be from Norton AntiVirus. The email contained a counterfeit Norton mark and indicated the recipient could obtain a year of free computer virus protection by opening the included attachment. In reality, the attachment installed malware on the recipient's computer.

119. On or about January 20, 2015, from outside the United States, members of the BAYROB GROUP, including DANET and NICOLESCU, logged into a C&C server in the United States, and deployed a malicious file entitled "walmart0[x].htm," which was used by bots in the Bayrob Botnet to inject fictitious webpages containing counterfeit Walmart marks, and advertising electronics for sale at Walmart. Victims were prompted by the injected webpage to enter their personal identifying information and credit card information, which information was then provided to the BAYROB GROUP.

120. In total, the BAYROB GROUP sent counterfeit trademarks and service marks associated with eBay, Facebook, Gmail, and others to at least 40,000 victims, including the victims listed below, in an effort to deceive these victims into sending them their personal credit card information, account information, or to install malware on their computers.

Bayrob's Assigned Victim ID	**Location**	**Trademark**	**Approximate Date Counterfeit Mark Used**
736823296	Seville, OH	Facebook / Yahoo!	February 18, 2013
274822144	Helena, OH	Gmail	December 2, 2014
274822144	Helena, OH	Facebook	December 2, 2014
1229064704	Bloomville, OH	eBay	January 22, 2015
1229373952	Ashtabula, OH	eBay	January 27, 2015
1124592640	Cleveland, OH	Facebook	March 5, 2015
1228371457	Sandusky, OH	Facebook	March 6, 2015

All in violation of Title 18, United States Code, Section 2320(a)(1).

COUNTS 16-20

(Aggravated Identity Theft, 18 U.S.C. §§ 1028A(a)(1) and 2)

The Grand Jury further charges that:

121. The factual allegations contained in Paragraphs 1 through 41 of this Indictment are re-alleged and hereby incorporated by reference as if fully set forth herein.

122. The term "means of identification," for purposes of this Indictment, means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual and includes any name, social security number, date of birth, and unique electronic identification code, address or routing code, including a credit or debit card number.

123. From on or about February 25, 2013, through on or about July 1, 2015, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did knowingly use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, the commission of Computer Fraud, a violation of Title 18, United States Code, Section 1030, and Wire Fraud, a violation of Title 18, United States Code, Section 1343, knowing that the means of identification belonged to another actual person, in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

Manner and Means of the Aggravated Identity Theft Scheme

124. Members of the BAYROB GROUP used the C&C servers to send malicious emails, attachments, and executable files to infect the computers of unsuspecting victims with the Bayrob Trojan.

125. Once infected, the members of the BAYROB GROUP commanded the infected computers to inject fraudulent webpages when users attempted to visit legitimate websites such as eBay, Walmart, Facebook, Yahoo!, Gmail, or PayPal.

126. The users of the infected computers would see a webpage that appeared to be a legitimate webpage, but that prompted them to verify their identity by entering personal information and credit card account information.

127. Because the personal information was entered by users attempting to gain access to their own accounts, the BAYROB GROUP could rely on the accuracy of the information provided by users.

128. The information entered by the victim would be transmitted to the BAYROB GROUP, where it was stored and catalogued for future use in paying for domain name registrations, to lease server space, and to cover other costs associated with the maintenance and growth of the Bayrob Botnet infrastructure and the criminal scheme in general.

129. The BAYROB GROUP stored the credit card information in tables on the C&C server. Each record in the table would typically include the card holder's full name, credit card numbers, expiration dates, and mailing addresses. When individual members of the BAYROB GROUP used a stolen credit card, that member would "reserve" the card, notate what the card was used to purchase, and if the card was still active. Members would also circulate credit card information via email.

130. The BAYROB GROUP collected and used more than 500 stolen credit cards through their scheme, including credit cards owned by the victims listed below:

Count	Victim ID	Location	Approximate Date of Theft and/or Use
16	C.M.B.	Fort Recovery, OH	2/25/13 – 5/27/13
17	T.M.	Celina, OH	3/12/13 –6/16/13
18	D.W.	Seville, OH	5/22/14 – 6/1/15
19	A.M.S.	N. Canton, OH	4/6/14 – 11/1/15
20	L.J.K.	Wapakoneta, OH	6/4/14 – 7/1/15

131. Members of the BAYROB GROUP knew, and had reason to know, that the information collected was from actual individuals because the means by which it was collected was specifically designed to required response and affirmative action by the victim to provide his or her own verification information.

132. Moreover, members of the BAYROB GROUP knew, and had reason to know, the credit card information was from actual individuals because the members successfully used the cards to make purchases, and often repeated purchases over an extended period of time.

All in violation of Title 18, United States Code, Section 1028A.

COUNT 21

(Conspiracy to Commit Money Laundering, 18 U.SC. § 1956(h))

The Grand Jury further charges that:

133. Paragraphs 1 through 41 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

The Conspiracy

134. From on or about January 1, 2007, through the date of the Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, and agree with each other and with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, to wit:

i. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Wire Fraud in violation of Title 18, United States Code, Section 1343, Fraudulent Access to Computers, in violation of Title 18, United States Code, Section 1030, and Trafficking in Counterfeit Goods, in violation of Title 18, United States Code, Section 2320(a), knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

ii. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument or funds involving the proceeds of specified unlawful activity, that is, Wire Fraud in violation of Title 18, United States Code, Section 1343, Fraudulent Access to

Computers, in violation of Title 18, United States Code, Section 1030, and Trafficking in Counterfeit Goods, in violation of Title 18, United States Code, Section 2320(a), from a place in the United States to or through a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i).

Objects of the Conspiracy

135. It was an object of the conspiracy that the Defendants used a network of money mules and wire transfers conducted under the guise of legitimate businesses in order to obscure and disguise the ultimate recipients of the criminal proceeds of their Wire Fraud, Fraudulent Access to Computers, and Trafficking in Counterfeit Goods and Services schemes.

136. It was a further object that the Defendants transferred money obtained from the Wire Fraud, Fraudulent Access to Computers, and Trafficking in Counterfeit Goods and Services schemes overseas for personal financial gain.

Manner and Means of the Conspiracy

137. The manner and means used to accomplish the objectives of the conspiracy included, among others, the following:

138. Using stolen credit card information and identification features obtained through the Wire Fraud, Fraudulent Access to Computers, and Trafficking in Counterfeit Goods and Services schemes, the BAYROB GROUP placed listings for “money transfer agents” on job posting websites including Monster.com, Indeed.com, Craigslist.com, and Beyond.com, among others.

139. The BAYROB GROUP created fictitious companies, such as US Wires Services, ITP Solution, ITP, MTS Solution, ITP Services, KPS, KFP Partners, KGT, KPL Partners, RBS Wire, MTPL, KPL, GlassTrust, Global Partners Hungaria KFT, and KST, and created fraudulent websites for each business to give the impression that they were actual businesses which engaged in legitimate international transactions.

140. The BAYROB GROUP also claimed to be hiring agents for legitimate companies such as Yahoo! and Google to entice individuals interested in working from home. The BAYROB GROUP injected fraudulent Google and Yahoo! pages when users of infected computers attempted to visit those websites. The injected pages contained counterfeit Google and Yahoo! logos, and otherwise appeared and functioned normally, except the pages contained advertisements in which Google and Yahoo! purported to be hiring "financial agents" to receive wire transfers and send them to "European clients" via Western Union.

141. The BAYROB GROUP, posing as these legitimate businesses, typically explained that the hiring company regularly received payments from companies in the United States, and the company could legally avoid paying a 19% Value Added Tax (VAT) if the payments were wired directly from American citizens. The BAYROB GROUP typically explained that the agents could keep six percent of any funds wired, or the agents could send the entire amount and later receive a check for ten percent of the funds. However, the "wire transfer agents" who elected to receive the ten percent option were not actually paid.

142. Individuals responding to the listings provided the BAYROB GROUP with their personal information and bank account information, and then received instructions from the BAYROB GROUP via email and text message. The BAYROB GROUP provided the "transfer agents" with information about incoming wire transfers, as well as information about where to wire those funds.

143. The BAYROB GROUP provided the name and bank account information for the "transfer agent" to victims of online auction fraud, who were led to believe that this information was for an "eBay Escrow Agent." Beyond their name and bank account information, the victims of online auction fraud were not provided with any contact information for the transfer agent. Any question a victim might raise about the transaction was redirected by the Bayrob Trojan to members of the BAYROB GROUP posing as eBay Customer Support.

144. Once victims wired the funds to the "transfer agent," the "transfer agent" withdrew the funds from his or her bank account, and wired the funds, less any commission, via Western Union or MoneyGram, to individuals in Romania or surrounding countries.

145. European "money mules," paid by the BAYROB GROUP, avoided detection by using fake identity documents, and by collecting the wired funds at random Western Union or MoneyGram offices in Romania or surrounding countries. Eventually, these funds were transferred to members of the BAYROB GROUP.

Acts in Furtherance of the Conspiracy

146. The following acts were committed in furtherance of the conspiracy in the Northern District of Ohio and elsewhere.

The Creation of Fictitious Online Companies Offering Transfer Agent Jobs

147. From approximately October 2007, to the date of this Indictment, members of the BAYROB GROUP recruited potential money mules by posing as legitimate online companies seeking "transfer agents." The BAYROB GROUP, collectively, used three types of false company profiles. The BAYROB GROUP either created fictitious companies and recruited "transfer agents" via the company's website; assumed the profile of a job recruiter for Yahoo! or Google; or, posted recruitment ads on legitimate employment websites. These false and fictitious profiles and websites allowed the BAYROB GROUP to obscure and disguise the

ultimate recipients of the criminal proceeds of Wire Fraud, Fraudulent Access to Computers, and Trafficking in Counterfeit Goods and Services schemes.

Concealment of the BAYROB GROUP's Identity Through the Use of Stolen Credit Cards To Pay For the Webhosting and ISP Services to Recruit Money Mules

148. Moreover, the BAYROB GROUP further obscured and disguised their actual identities, locations, and criminal intentions by using stolen credit cards and identities to pay for the domain names, websites, and ISPs hosting the fictitious entities.

149. On or about March 31, 2013, NICOLESCU sent an encrypted email with the subject "cc2013031" to DANET, MICLAUS, and two members of the BAYROB GROUP unknown to the Grand Jury. The email contained a password protected file attachment named "20130331cc.txt.asc." The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

150. On or about November 20, 2013, NICOLESCU sent an encrypted email with the subject "20131119cc" to DANET, MICLAUS, and three members of the BAYROB GROUP unknown to the Grand Jury. Attached to this email were encrypted files "20131119cc.txt.pgp" and "20131119cc.xls.pgp." The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

151. On or about December 10, 2013, NICOLESCU sent an encrypted email with the subject "more ccs" to DANET, MICLAUS, and two members of the BAYROB GROUP unknown to the Grand Jury. Attached to this email was an encrypted file "20131210cc.txt.pgp." The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

152. On or about July 23, 2014, DANET sent an encrypted email with the subject "Ccs" to NICOLESCU. This email attached a password protected file "cccs.rar.pgp." The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

153. On or about December 5, 2014, DANET sent an encrypted email with the subject "Cc" to MICLAUS. The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

154. On or about December 5, 2014, NICOLESCU sent an encrypted email with the subject "cc" to DANET and MICLAUS. The email contained a password protected file attachment named "20141205cc.txt.asc." The C&C server contained a database table named "cc" that maintained a list of stolen credit cards available and used by the members of the BAYROB GROUP to pay for infrastructure.

Using the Money Mules to Send Money Overseas to Evade Detection and Identification

155. On or about July 1, 2013, an individual, "R.M.," whose identity is known to the Grand Jury, corresponded with an email address at America Online to negotiate the purchase of a 1965 Ford Mustang listed on eBay. As a result, R.M. sent $9,200 to D.W. via bank wire transfer to Charter One Bank, 7700 Brookpark Rd, Brooklyn, Ohio 44129.

156. On or about August 1, 2013, an individual, "M.B.," whose identity is known to the Grand Jury, communicated with an email address at America Online regarding the purchase of a car listed on eBay. As a result, M.B. sent a bank wire transfer of $10,700 to D.W. at PNC Bank in Cleveland, Ohio.

157. On or about July 9, 2013, an individual, "A.K.," whose identity is known to the Grand Jury, communicated with an email address at America Online regarding the purchase of a

car listed on eBay. As a result, A.K. sent a bank wire transfer of $8,918.62 to D.W. at US Bank in Cleveland, Ohio.

158. On or about July 25, 2013, an individual, "D.P.," whose identity is known to the Grand Jury, communicated with an email address at America Online regarding the purchase of a car listed on eBay. As a result, D.P. sent a bank wire transfer of $7,858.50 to D.W. at Charter One Bank in Cleveland, Ohio.

159. On or about August 6, 2013, an individual, "J.G.," whose identity is known to the Grand Jury, communicated with an email address at America Online regarding the purchase of a car listed on eBay. As a result, J.G. sent a bank wire transfer of $7,254.00 to D.W. at Charter One Bank in Cleveland, Ohio.

160. On or about August 1, 2013, an individual, "T.V.," whose identity is known to the Grand Jury, corresponded with an email address at America Online about a 1971 Dodge Charger offered for sale on eBay. As a result, T.V. sent a bank wire transfer of $7,000 to H.P. at US Bank, 15215 Manchester Rd, Ballwin, Missouri 63011.

161. From in or around October 2007 to the date of this Indictment, in the Northern District of Ohio, Eastern Division, and elsewhere, the BAYROB GROUP directed United States-based money mules, including D.W. and H.P. to transmit and transfer, and attempt to do so, monetary instruments and funds, including, wire transfers of funds obtained by money mules in the United States, from a place in the United States to members of the BAYROB GROUP and to European-based money mules located at a place outside of the United States, including Romania and elsewhere in Eastern Europe.

162. In order to track the payments sent from victims to mules, the members of the BAYROB GROUP created files, including but not limited to, a spreadsheet called "amounts final" that tracked the progress of wire transfers and amounts received, as well as a table titled

"my4_mules," which contained a list of mules recruited in the United States. These tables were stored and maintained on the C&C server. The members of the BAYROB GROUP could review and update the information in the tables.

163. On or about August 23, 2013, using the C&C server, a member of the BAYROB GROUP whose identity is unknown to the grand jury sent an encrypted email to DANET, with the subject line of "amounts final." This email contained a table of active money mules in the United States and Europe on which they tracked the progress of wire transfers and amounts received.

164. The BAYROB GROUP was able to transfer over $1,100,000 overseas via Western Union.

165. The proceeds of the wires received by the BAYROB GROUP were intended to be divided in the following manner: NICOLESCU receiving 25%, DANET receiving 25%, and MICLAUS receiving 10%, the remaining funds were to be divided amongst individuals unknown to the Grand Jury.

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

ENHANCEMENT PURSUANT TO TITLE 18,
UNITED STATES CODE, SECTION 3559(g)(1)
(False Registration of a Domain Name)

The Grand Jury further charges that:

166. Paragraphs 1 through 41 of the Indictment are re-alleged and incorporated by reference as if fully set forth herein.

167. Between on or about April 14, 2014 and on or about July 25, 2014, in the Northern District of Ohio and elsewhere, Defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS, and others presently known and unknown to the Grand Jury, did knowingly and intentionally falsely register the below-listed domain names, in that the Defendants did register and cause to be registered the below-listed domain names with hosting services using a false contact, and further that the Defendants did knowingly and intentionally use at least one of the below-listed domain names in the course of the commission of the felony offenses alleged in this Indictment.

168. Knowing that the domain names were registered using false names, stolen credit cards, and fictitious identifying information, NICOLESCU, DANET, and MICLAUS registered the following domain names on or about the below-listed dates:

Date	Domain	Identity Used
04/17/14	recordcontinue.net	F.G.
04/20/14	spendmarry.net	F.G.
04/20/14	frontride.net	D.S.
04/26/14	wrongthrew.net	D.S.
04/27/14	chieftraining.net	F.G.
04/28/14	hangcold.net	F.G.
04/28/14	middleevery.net	D.S.
04/29/14	suffermeeting.net	J.S.
05/01/14	husbandbeauty.net	J.S.
05/12/14	electricelectricity.net	R.M.
05/12/14	againstspread.net	R.M.
05/13/14	captaingarden.net	R.M.
05/14/14	gathermayor.net	R.M.
05/14/14	presentchance.net	R.M.
05/15/14	morningelectricity.net	R.M.

Date	Domain	Identity Used
05/16/14	weathersquare.net	K.C.
05/17/14	historyperfect.net	K.C.
05/19/14	seasonproduce.net	J.R.
05/19/14	decidebrought.net	J.R.
05/20/14	chiefbroad.net	J.R.
05/21/14	rockknew.net	T.J.
05/21/14	rathernearly.net	T.J.
05/21/14	collegesuppose.net	J.R.
05/21/14	hangclock.net	O.K.
05/22/14	calloctover.net	R.G.
05/22/14	spendstudy.net	R.G.
05/22/14	westweight.net	R.B.
05/22/14	likrlend.net	S.H.
05/22/14	septemberwall.net	A.Q.
05/22/14	favoroctober.net	D.L.
05/22/14	classwrite.net	T.J.
05/22/14	pointdeal.net	J.D.
05/22/14	historymethod.net	R.G.
05/22/14	ringfirst.net	C.M.
05/23/14	torebuild.net	C.M.
05/23/14	viewcome.net	A.Q.
05/23/14	takestood.net	S.H.
05/23/14	lrstnfeed.net	R.B.
05/23/14	strengthkitchen.net	D.L.
05/23/14	ringoctober.net	J.D.
05/23/14	muchouter.net	D.L.
05/23/14	fallworld.net	T.J.
05/23/14	doublewhose.net	J.D.
05/25/14	pointfine.net	R.B.
05/25/14	strengthfinger.net	A.Q.
05/25/14	foreignladder.net	R.B.
05/25/14	wellshirt.net	C.M.
05/25/14	storeenough.net	S.H.
05/25/14	resultfurther.net	T.J.
05/25/14	likrhers.net	J.D.
05/25/14	noseheld.net	A.Q.
05/27/14	machineproud.net	S.H.
05/27/14	familybecome.net	R.B.
05/27/14	thoughnature.net	C.M.
05/27/14	fiftyserve.net	A.Q.
05/27/14	soilserve.net	C.M.
05/27/14	childrenwhose.net	J.D.
05/27/14	soilonly.net	R.S.
05/27/14	fiftyopen.net	R.B.
05/27/14	soilopen.net	D.S.
05/27/14	soilhear.net	S.H.

Date	Domain	Identity Used
05/27/14	fiftyonly.net	J.D.
05/28/14	southsing.net	C.M.
05/28/14	fiftysing.net	D.S.
05/28/14	triedpage.net	S.H.
05/28/14	triedserve.net	R.S.
05/29/14	fellowmodern.net	C.M.
05/29/14	mightadvance.net	S.H.
05/29/14	thoughfinger.net	A.Q.
05/29/14	strengthforever.net	J.D.
05/30/14	stillsister.net	S.H.
05/30/14	storestation.net	C.M.
07/24/14	watercaught.net	J.M.
07/25/14	knownguard.net	J.M.
07/25/14	experiencedevice.net	J.M.
07/25/14	enemydont.net	J.M.

169. Once registered, members of the BAYROB GROUP used the above-listed domain names to carry out fraud schemes in violation of the law as described in Counts 1 through 20.

170. Additionally, members of the BAYROB GROUP registered the below-listed domain names using false names, stolen credit cards, and fictitious identifying information in order to further the criminal money laundering scheme charged in Count 21 of this Indictment.

171. On or about April 5, 2011, the BAYROB GROUP purchased the domain name KPL-business.com, and used it to publish a website for the fictitious company, KPL. The KPL website was registered in the name of R.L., of Norwood, Ohio, whose identity is known to the Grand Jury.

172. On or about May 23, 2008, the BAYROB GROUP purchased a domain name for the website, ITPSolution.net, and used it to publish a website for the fictitious company, ITP Solution. The ITP Solution website was registered in the name of J.N., of Bellingham, WA. Money mules working for the BAYROB GROUP communicated with an email account known to the grand jury ending in @itpsolution.co.uk from on or about May 26, 2008 through on or about June 15, 2008.

173. On or about July 22, 2008, the BAYROB GROUP purchased a domain name for the website ITPServices.us and used it to publish a website for the fictitious company ITP Services. The ITP Services website was registered in the name of G.G., of Savannah, GA.

174. On or about March 10, 2009, the BAYROB GROUP purchased a domain name for the website KPS-online.com, and used it to publish a website for the fictitious company KPS. The KPS website was registered in the name of S.W., of Compton, CA.

175. On or about February 25, 2010, the BAYROB GROUP purchased a domain name for the website KFP-partners.com and used it to publish a website for the fictitious company KFP Partners. The KFP Partners website was registered in the name of R.P., of Sunnyvale, CA.

176. On or about February 26, 2010, the BAYROB GROUP purchased a domain name for the website KGT-online.com and used it to publish a website for the fictitious company KGT. The KGT website was registered in the name of T.S., of Post Falls, ID.

177. On or about February 26, 2010, the BAYROB GROUP purchased a domain name for the website KPL-Partners.com and used it to publish a website for the fictitious company KPL Partners. The KPL Partners website was registered in the name of C.K., of Sunnyvale, CA.

178. On or about February 26, 2010, the BAYROB GROUP purchased a domain name for the website KPL-online.com and used it to publish a website for the fictitious company KPL. The KPL website was registered in the name of E.P., of Sunnyvale, CA.

179. On or about October 7, 2010, the BAYROB GROUP purchased a domain name for the website KPL-Solutions.com and used it to publish a website for the fictitious company KPL Solutions. The KPL Solutions website was registered in the name of G.W., of Bryan, TX.

180. On or about March 31, 2011, the BAYROB GROUP purchased a domain name for the website MTPL-program.com and used it to publish a website for the fictitious company MTPL. The MTPL website was registered in the name of K.M., of East Grand Rapids, MI.

181. On or about January 11, 2012, the BAYROB GROUP purchased a domain name for the website MTPL-expert.com and used it to publish a website for the fictitious company MTPL. The MTPL website was registered in the name of G.D., of New Port Richey, FL.

182. On or about February 21, 2013, the BAYROB GROUP purchased a domain name for the website GlassTrust.net and used it to publish a website for the fictitious company GlassTrust. The GlassTrust website was registered in the name of G.L., of Brooklyn, NY.

183. On or about February 27, 2013, the BAYROB GROUP purchased a domain name for the website TradeLength.net and used it to publish a website for the fictitious company Global Partners Hungaria KFT. The Global Partners Hungaria KFT website was registered in the name of R.G., of Henry, VA.

184. On or about April 24, 2012, the BAYROB GROUP purchased a domain name for the website KST-online.com and used it to publish a website for the fictitious company KST. The KST website was registered in the name of R.K., of Hollywood, FL.

185. On or about February 28, 2013, the BAYROB GROUP purchased a domain name for the website, streetlaughter.net, and used it to publish a website for the fictitious company Global Partners Hungaria KFT. The Global Partners Hungaria KFT website was registered in the name of M.S., of Des Plaines, IL.

186. On or about March 15, 2013, the BAYROB GROUP purchased a domain name for the website forwarding-service-group.com and used it to publish a website for the fictitious company Global Partners Hungaria KFT. The Global Partners Hungaria KFT website was registered in the name of J.U., of Costa Mesa, CA.

In violation of Title 18, United States Code, Section 3559(g)(1).

FORFEITURE: COUNTS 1-13

The Grand Jury further charges:

187. The allegations of Counts 1 through 13, inclusive, are hereby re-alleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c). As a result of the foregoing offenses, defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit to the United States all property, real and personal, which constitutes, or is derived from, proceeds traceable to the commission of such offenses; including, but not limited to, the following:

a.) MONEY JUDGMENT: defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit property, including, but not limited to, a sum of money equal to the proceeds of Counts 1 through 13.

FORFEITURE: COUNT 14

The Grand Jury further charges:

188. The allegations of Count 14 are hereby re-alleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(2)(B) and Title 18, United States Code, Section 1030(i). As a result of the foregoing offense, defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit to the United States all property, real and personal, constituting or derived from proceeds that the defendants obtained, directly or indirectly, as the result of such offense; and, all personal property that was used, or was intended to be used, to commit or to facilitate the commission of such offense; including, but not limited to, the following:

a.) MONEY JUDGMENT: defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit property, including, but not limited to, a sum of money equal to the proceeds of Count 14.

FORFEITURE: COUNT 15

The Grand Jury further charges:

189. The allegations of Count 15 are hereby re-alleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 2323(b). As a result of the foregoing offense, defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit to the United States all property constituting or derived from any proceeds obtained directly or indirectly as the result of the commission of such offense; and, all property used, or intended to be used, in any manner or part to commit or facilitate the commission of such offense; including, but not limited to, the following:

a.) MONEY JUDGMENT: defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit property, including, but not limited to, a sum of money equal to the proceeds of Count 15.

FORFEITURE: COUNT 21

The Grand Jury further charges:

190. The allegations of Count 21 are hereby re-alleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 982(a)(1). As a result of the foregoing offense, defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit to the United States all property, real and personal, involved in Count 21, and all property traceable to such property; including, but not limited to, the following:

a.) MONEY JUDGMENT: defendants BOGDAN NICOLESCU, TIBERIU DANET, and RADU MICLAUS shall forfeit property, including, but not limited to, a sum of money equal to the value of all property involved in Count 21.

SUBSTITUTE PROPERTY

191. In the event that any property subject to forfeiture under Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), Title 18, United States Code, Section 982(a)(2)(B), Title 18, United States Code, Section 1030(i), Title 18, United States Code, Section 2323(b), and/or Title 18, United States Code, Section 982(a)(1), as a result of any act or omission of the defendant(s):

a.) cannot be located upon 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 this 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 21, United States Code, Section 853(p), to seek forfeiture of any other property of the 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.

A TRUE BILL.

_____
FOREPERSON

_____
CAROLE S. RENDON
Acting United States Attorney

LESLIE R. CALDWELL
Assistant Attorney General
Criminal Division
U.S. Department of Justice