UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

SEALED

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
v.	)	4:11CR 3074
	)	
VYACHESLAV IGOREVICH PENCHUKOV, also known as "tank;"also known as "father;"	)	
IVAN VIKTORVICH KLEPIKOV, also known as "petr0vich;" also known as "nowhere;"	)	FIRST SUPERSEDING INDICTMENT
ALEXEY DMITRIEVICH BRON, also known as "thehead;"	)	18 U.S.C. § 1962(d)
ALEXEY TIKONOV, also known as "kusanagi,"	)	18 U.S.C. §§ 1344, 1349
YEVHEN KULIBABA, also known as "jonni;"	)	18 U.S.C. §§ 371 & 1028 & 1030
YURIY KONOVALENKO, also known as "jtk0;"	)	18 U.S.C. § 1028A
JOHN DOE #1, also known as "lucky12345;"	)	18 U.S.C. §§ 981(a)(1)(C),
JOHN DOE #2, also known as "aqua;"	)	982(a)(2)(A)
JOHN DOE #3, also known as "mricq;"	)	
	)	
	)	
Defendants.	)	

COUNT I
(Conspiracy to Participate in Racketeering Activity, 18 U.S.C. § 1962(d))

Introduction

The Grand Jury charges that:

1. At all times material to this Superseding Indictment:

   a. VYACHESLAV IGOREVICH PENCHUKOV was a resident of Ukraine. He used the online nickname "tank" and also used the online nickname "father."

b. IVAN VIKTORVICH KLEPIKOV was a resident of Ukraine. He used the online nickname "petr0vich" and also used the online nickname "nowhere."

c. ALEXEY DMITRIEVICH BRON was a resident of Ukraine. He used the online nickname "thehead."

d. ALEXEY TIKONOV was a resident of Russia. He used the online nickname "kusanagi."

e. YEVHEN KULIBABA was a resident of the United Kingdom. He used the online nickname "jonni."

f. YURIY KONOVALENKO was a resident of the United Kingdom and Ukraine. He used the online nickname "jtk0."

g. JOHN DOE #1 was a resident of Russia. His true name is not known to the Grand Jury. He used the online nickname "lucky."

h. JOHN DOE #2 was a resident of Russia. His true name is not known to the Grand Jury. He used the online nickname "aqua."

i. JOHN DOE #3 was a resident of Ukraine. His true name is not known to the Grand Jury. He used the online nickname "mricq."

j. BANK OF AMERICA was a financial institution insured by the Federal Deposit Insurance Corporation, was headquartered in Charlotte, North Carolina, and had offices in Nebraska.

k. BULLITT COUNTY FISCAL COURT was a municipal government office in Shepherdsville, Kentucky.

l. DOLL DISTRIBUTING was a business located in Des Moines, Iowa.

m. FIRST FEDERAL SAVINGS BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Elizabethtown, Kentucky.

n. FIRST NATIONAL BANK OF OMAHA was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Omaha, Nebraska. It offered online banking services through computer servers located in Nebraska.

o. FRANCISCAN SISTERS OF CHICAGO was a religious congregation headquartered in Homewood, Illinois.

p. HUSKER AG, LLC was a business located in Plainview, Nebraska.

q. KEY BANK was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Sylvania, Ohio.

r. LIBERTY USA CONTRACTORS LLC was a business.

s. ODAT LLC, doing business as AIR TREATMENT COMPANY, was a business located in Clifton, Virginia.

t. PARAGO, INC. was a business located in Lewisville, Texas.

u. SALISBURY BANK & TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Salisbury, Massachusetts.

v. TOWN OF EGREMONT was a town in Massachusetts with its own municipal government.

w. UNION BANK AND TRUST was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Lincoln, Nebraska.

x. UNION BANKSHARES CORPORATION was a financial institution insured by the Federal Deposit Insurance Corporation, and was located in Ruther Glen, Virginia.

y. UNITED DAIRY, INC. was a business located in Martins Ferry, Ohio.

z. The Automated Clearing House ("ACH") Network is a network of computers which provided for the interbank clearing of electronic payments for participating depository financial institutions across the United States. Instead of using paper to carry necessary transaction information, ACH transactions are transmitted electronically between financial institutions through data transmission, using wires and cables.

aa. A "money mule" was a person who received funds into a bank account, and then moved the money to other accounts, or withdrew

the funds and transported it overseas as smuggled bulk cash.

bb. A personal identification number, or "PIN," was a numeric password, used in conjunction with other information to uniquely identify a specific individual.

cc. An "RSA SecureID token code" was a short, rapidly changing numeric code used in conjunction with a password and with other information to uniquely identify a specific individual.

dd. The Internet is a global network of computers and other electronic devices that communicate with each other via both network cables and radio transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders.

ee. A "chat" was text-based communication sent over the Internet.

ff. "Jabber" was a method of sending and receiving chat.

gg. "Zeus" or "Zbot" was a form of malicious software that collected and transmitted personal information from infected computers, including information necessary to enter users' bank accounts.

The Racketeering Enterprise

2. The defendants and others known and unknown to the grand jury (collectively, the "Jabber Zeus Crew"), constituted an "enterprise" as defined in Section 1961(4) of Title 18, United States Code, that is, a group of individuals associated in fact that engaged in, and the activities of which affected, interstate and foreign commerce. The enterprise constituted an ongoing organization whose members functioned as a continuing unit for the common purpose of achieving the objectives of the enterprise.

Purposes of the Enterprise

3. The purposes of the enterprise included the following:

a. Infecting computers used by various businesses and other entities,

including small businesses, governmental entities, and non-profit organizations, with malicious software;

b. Obtaining bank account numbers, passwords, PIN numbers, RSA SecureID token codes, and similar information necessary to log into online bank accounts;

c. Initiating electronic funds transfers from those bank accounts to the bank accounts of "money mules";

d. Transferring funds from money mules to overseas;

e. Obtaining the use of computer servers necessary to obtain banking credentials and provide real-time communications among enterprise members;

f. Assigning different members the tasks of writing malicious software, administering computer servers, recruiting money mules, infecting computers, accessing bank accounts to make unauthorized transfers, and receiving transferred funds outside the United States; and

g. Avoiding detection of criminal activity.

The Racketeering Conspiracy

4. From in or about May 2009, the exact date being unknown to the Grand Jury, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter "DEFENDANTS"), each being a person employed by and associated with the Jabber

Zeus Crew, an enterprise engaged in, and the activities of which affected, interstate and foreign commerce, together with others known and unknown, did knowingly and intentionally conspire to violate 18 U.S.C. § 1962(c), that is, 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 indictable under 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1029 (fraud in connection with access devices), and 18 U.S.C. § 1028 (identity theft).

5. It was part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

Manner and Means of the Conspiracy

6. It was part of the conspiracy that DEFENDANTS used computer intrusion, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere.

7. It was further part of the conspiracy that DEFENDANTS installed, without authorization, malicious software known as "Zeus" or "Zbot" on Internet-connected computers without those computers' owners' authorization, thereby causing damage to those computers.

8. It was further part of the conspiracy that DEFENDANTS used that malicious software to capture bank account numbers, passwords, and other information necessary to log into online banking accounts.

9. It was further part of the conspiracy that DEFENDANTS used that captured information without authorization to falsely represent to banks that DEFENDANTS were employees of the victims authorized to make transfers of funds from the victims' bank accounts.

10. It was further part of the conspiracy that DEFENDANTS used that captured information to cause banks to make unauthorized transfers of funds from the victims' bank accounts.

11. It was further part of the conspiracy that DEFENDANTS used as "money mules" residents of the United States who received funds transferred over the Automated Clearing House ("ACH") network or through other interstate wire systems from victims' bank accounts into the money mules' own bank accounts, and then withdrew some of those funds and wired the funds overseas to conspirators.

12. It was further part of the conspiracy that DEFENDANTS maintained Internet-connected computer servers, in the United States and elsewhere, to facilitate communication.

13. It was further part of the conspiracy that DEFENDANTS knowingly falsely registered a domain name and knowingly used that domain name in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

Overt Acts

14. In furtherance of the conspiracy and to achieve the objectives thereof, the conspirators performed or caused to be performed, the following overt acts, among others, in the District of Nebraska and elsewhere:

a. On or about June 22, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by BULLITT COUNTY FISCAL COURT.

b. On or about June 22, 2009, DEFENDANTS used stolen access information to cause FIRST FEDERAL SAVINGS BANK to transfer funds out of a bank account belonging to BULLITT COUNTY

FISCAL COURT and into one or more bank accounts designated by DEFENDANTS.

c. On July 7, 2009, KLEPIKOV received a chat message from an alert messaging system which notifies members of the enterprise once a bank account has been compromised.

d. On July 8, 2009, BRON received a chat message from PENCHUKOV which included details of bank account. The message contained information concerning a victim bank account, user credentials and bank account numbers.

e. On July 8, 2009, JOHN DOE #1 sent a chat message to PENCHUKOV which included details of a bank account. The message contained account and company identification information.

f. On July 8, 2009, JOHN DOE #1 sent a chat message to PENCHUKOV which included details of a bank account. The message contained account and company identification information.

g. On or about July 8, 2009, PENCHUKOV transmitted login credentials for an employee of TOWN OF EGREMONT to JOHN DOE #3.

h. On or about July 8, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by ODAT LLC.

i. On or about July 8, 2009, KULIBABA sent PENCHUKOV online messages identifying bank accounts of victims and providing bank account information for money mules to receive funds stolen from victims.

j. On or about July 8, 2009, DEFENDANTS used stolen access information to attempt to cause UNION BANKSHARES CORPORATION to transfer funds out of a bank account belonging to ODAT LLC and into one or more bank accounts designated by DEFENDANTS.

k. On July 9, 2009, KULIBABA received a chat message from PENCHUKOV which included details of a transfer from a victim bank account belonging to ODAT LLC. The message included the amount to be transferred and the money mule name and account to

which the money was deposited.

l. On July 9, 2009, KULIBABA received a chat message from PENCHUKOV which included details of a transfer from a bank account. The message included the amount to be transferred and the money mule names and account to which the money was deposited.

m. On or about July 12 and 13, 2009, PENCHUKOV, JOHN DOE #2, and another individual exchanged online messages about unauthorized withdrawals they had made from accounts owned by BULLITT COUNTY FISCAL COURT.

n. On or about July 28, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by DOLL DISTRIBUTING.

o. On or about July 29, 2009, DEFENDANTS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to DOLL DISTRIBUTING and into one or more bank accounts designated by DEFENDANTS.

p. On or about July 29, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by TOWN OF EGREMONT.

q. On or about July 29, 2009, DEFENDANTS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANTS.

r. On or about July 30, 2009, JOHN DOE #3 sent JOHN DOE #2 an online message about the TOWN OF EGREMONT bank account.

s. On or about July 30, 2009, DEFENDANTS used stolen access information to cause SALISBURY BANK & TRUST to transfer funds out of a bank account belonging to TOWN OF EGREMONT and into one or more bank accounts designated by DEFENDANTS.

t. On or about August 12, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by FRANCISCAN SISTERS OF CHICAGO.

u. On or about August 12, 2009, DEFENDANTS used stolen access

information to cause BANK OF AMERICA to transfer funds out of a bank account belonging to FRANCISCAN SISTERS OF CHICAGO and into one or more bank accounts designated by DEFENDANTS.

v. On or about August 13, 2009, PENCHUKOV sent an online message to JOHN DOE #2 listing recipients and amounts of funds transferred from a bank account belonging to FRANCISCAN SISTERS OF CHICAGO.

w. On or about August 25, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by UNITED DAIRY, INC.

x. On or about August 26, 2009, DEFENDANTS used stolen access information to cause KEY BANK to transfer funds out of a bank account belonging to UNITED DAIRY, INC. and into one or more bank accounts designated by DEFENDANTS.

y. On or about August 28, 2009, PENCHUKOV and JOHN DOE #3 each received an online message containing login credentials for an employee of UNITED DAIRY, INC.

z. On August 28, 2009, JOHN DOE #2 sent a chat message to PENCHUKOV which included details of five victim bank accounts. The message contained victim names, bank account and routing information.

aa. On September 1, 2009, JOHN DOE #2 received a chat message from PENCHUKOV which included details of multiple transfers from a bank account. The message included the names, bank account details and deposit amounts of nine money mules.

bb. On September 23, 2009, KLEPIKOV received a chat message from PENCHUKOV which included details of a bank account. The message contained client banking login information.

cc. On September 23, 2009, BRON received a chat message from PENCHUKOV which included bank account numbers and other information concerning a bank account.

dd. On or about September 28, 2009, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by

PARAGO, INC.

ee. On or about September 28, 2009, DEFENDANTS used stolen access information to attempt to cause FIRST NATIONAL BANK OF OMAHA to transfer funds out of a bank account belonging to PARAGO, INC. and into one or more bank accounts designated by DEFENDANTS.

ff. On or about September 28, 2009, PENCHUKOV transmitted login credentials for an employee of PARAGO, INC. to JOHN DOE #3.

gg. On November 25, 2009, TIKONOV received a chat message from PENCHUKOV which included banking credentials and other information concerning a bank account.

hh. On December 3, 2009, KONOVALENKO sent a chat message to KULIBABA which included the details of eight bank accounts. The message included the bank website URL (uniform resource locator), name associated with the accounts and login credentials to access each account.

ii. On February 4, 2010, TIKONOV received a chat message from PENCHUKOV which included banking credentials and other information concerning a bank account.

jj. On or about March 3, 2010, DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by HUSKER AG, LLC.

kk. On or about March 3, 2010, DEFENDANTS used stolen access information to attempt to cause UNION BANK AND TRUST to transfer funds out of a bank account belonging to HUSKER AG, LLC and into one or more bank accounts designated by DEFENDANTS.

ll. On or about March 3, 2010, PENCHUKOV, TIKONOV, and JOHN DOE #3 received a message containing stolen access credentials for an employee of HUSKER AG, LLC.

mm. On or about March 8, 2010, KONOVALENKO sent KULIBABA an online message regarding how much money he was making operating money mules for PENCHUKOV.

In violation of Section 1962(d) of Title 18 of the United States Code.

COUNT II
(Bank Fraud, 18 U.S.C. §§ 1344, 1349)

15. The Grand Jury hereby repeats and realleges each and every allegation contained in Paragraphs 1 through 3 and 6 through 14 of this Superseding Indictment.

16. From in or about May 2009, the exact date being unknown to the Grand Jury, and continuing to the present, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter "DEFENDANTS") devised and executed a scheme and artifice to defraud BANK OF AMERICA, FIRST FEDERAL SAVINGS BANK, FIRST NATIONAL BANK OF OMAHA, KEY BANK, SALISBURY BANK & TRUST, UNION BANK AND TRUST, and UNITED BANKSHARES CORPORATION, all of which were depository institutions insured by the Federal Deposit Insurance Corporation.

17. It was part of the scheme that DEFENDANTS used computer intrusion, malicious software, and fraud to steal or attempt to steal millions of dollars from several bank accounts in the United States, and elsewhere. Defendants and their co-conspirators infected thousands of business computers with software that captured passwords, account numbers, and other information necessary to log into online banking accounts, and then used the captured information to steal millions of dollars from account-holding victims' bank accounts. Account holding victims included BULLITT COUNTY FISCAL COURT, DOLL DISTRIBUTING, FRANCISCAN SISTERS OF CHICAGO, HUSKER AG, LLC, PARAGO, INC., TOWN OF EGREMONT, and UNITED DAIRY, INC..

18. DEFENDANTS intended and foresaw that their conduct would defraud banks

in the District of Nebraska.

19. On or about July 19, 2009, in the District of Nebraska and elsewhere, DEFENDANTS executed and attempted to execute and conspired to execute the scheme and artifice set forth above, in that the DEFENDANTS caused the malicious software described above to be installed, without authorization, on a computer used by DOLL DISTRIBUTING, and in that DEFENDANTS falsely represented to FIRST NATIONAL BANK OF OMAHA that DEFENDANTS were entitled to authorize transfers of funds out of a bank account maintained with FIRST NATIONAL BANK OF OMAHA and belonging to DOLL DISTRIBUTING.

In violation of Sections 1344 and 1349 of Title 18 of the United States Code.

COUNT III
(Bank Fraud, 18 U.S.C. §§ 1344, 1349)

20. The Grand Jury hereby repeats and realleges each and every allegation contained in Paragraphs 1 through 3, 6 through 14, and 16 through 18 of this Superseding Indictment.

21. On or about September 28, 2009, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter "DEFENDANTS") executed and attempted to execute and conspired to execute the scheme and artifice set forth in Paragraphs 16 and 17 above, in that the DEFENDANTS caused malicious software to be installed, without authorization, on a computer used by PARAGO, INC., and in that DEFENDANTS falsely represented to FIRST NATIONAL BANK OF OMAHA that DEFENDANTS were entitled to authorize transfers of funds out of a bank account maintained with FIRST NATIONAL BANK OF

OMAHA and belonging to PARAGO, INC.

In violation of Sections 1344 and 1349 of Title 18 of the United States Code.

COUNT IV
(Bank Fraud, 18 U.S.C. §§ 1344, 1349)

22. The Grand Jury hereby repeats and realleges each and every allegation contained in Paragraphs 1 through 3, 6 through 14, and 16 through 18 of this Superseding Indictment.

23. On or about March 3, 2010, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter "DEFENDANTS") executed and attempted to execute and conspired to execute the scheme and artifice set forth in Paragraphs 16 and 17 above, in that the DEFENDANTS caused malicious software described above to be installed, without authorization, on a computer used by HUSKER AG, LLC, and in that DEFENDANTS falsely represented to UNION BANK AND TRUST that DEFENDANTS were entitled to authorize transfers of funds out of a bank account maintained with UNION BANK AND TRUST and belonging to HUSKER AG, LLC.

In violation of Sections 1344 and 1349 of Title 18 of the United States Code.

COUNT V
(Aggravated Identity Theft, 18 U.S.C. § 1028A)

24. The Grand Jury hereby repeats and realleges each and every allegation contained in Paragraphs 1 through 3 and 6 through 14 of this Superseding Indictment.

25. On or about July 19, 2009, September 28, 2009, and March 3, 2010, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter

"DEFENDANTS") did knowingly transfer and possess and use, without lawful authority, a means of identification of another person during and in relation to the violations of Title 18, United States Code, Sections 1344 and 1349 charged in Count Two, Count Three, and Count Four above.

In violation of in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT VI
(Conspiracy, 18 U.S.C. § 371,
to violate Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2), (a)(5)(A),
and Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028(a)(7))

26. The Grand Jury hereby repeats and realleges each and every allegation contained in Paragraphs 1 through 3 and 6 through 14 of this Superseding Indictment.

The Conspiracy and Its Objects

27. From in or about May 2009, the exact date being unknown to the Grand Jury, and continuing to the present, in the District of Nebraska and elsewhere, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3 (hereinafter "DEFENDANTS") did knowingly conspire, combine, confederate, and agree, together and with other individuals, both known and unknown to the Grand Jury, to commit offenses against the United States, that is:

a. 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, thus causing damage affecting 10 or more protected computers during a 1-year period, all in violation of 18 U.S.C. § 1030(a)(5)(A), (c)(4)(A)(i)(VI), and (c)(4)(B);

b. to intentionally access a computer without authorization, and exceed

authorized access, and thereby obtain information from a protected computer, for purposes of commercial advantage and private financial gain, all in violation of in violation of 18 U.S.C. § 1030(a)(2), and (c)(2)(B)(i); and

c. to knowingly transfer and possess and use, in or affecting interstate or foreign commerce, without lawful authority, a means of identification of another person, to wit, a bank account number and a password and a PIN number and a token code, with the intent to commit, and in connection with, any unlawful activity that constitutes a violation of Federal law, to wit, violations of Sections 1344 and 1349 of Title 18 of the United States Code, and the offense involved the transfer of more than five identification documents, authentication features, and false identification documents; and as a result of the offense, the defendant and another individual committing the offense, obtained anything of value aggregating $1,000 or more during any 1-year period, all in violation of 18 U.S.C. § 1028(a)(7), (b)(1)(B), (b)(1)(D), and (f).

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

NOTICE OF FORFEITURE

28. The allegations contained in all prior paragraphs of this Superseding Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections Section 981(a)(1)(C), 982(a)(2)(A), and 1963, and Title 28, United States Code, Section 2461(c).

29. The Grand Jury hereby finds that there is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

30. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States of

America gives notice to all defendants that, in the event of a conviction by any defendant of any of the offenses charged in Counts One, Two, Three, Four, or Six of this Superseding Indictment, the United States intends to forfeit the property of that defendant as is further described in this Notice of Forfeiture.

31. Pursuant to Title 18, United States Code, Section 1963, upon conviction of an offense in violation of Title 18, United States Code, Section 1962 as charged in Count One, the defendants, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3, shall forfeit to the United States of America:

a. any interest acquired or maintained in violation of section 1962;

b. any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over, any enterprise which the defendants established, operated, controlled, conducted, or participated in the conduct of, in violation of section 1962; and

c. any property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity or unlawful debt collection in violation of section 1962.

32. Upon conviction any of the offenses in violation of Title 18, United States Code, Sections 1344 and 1349 set forth in Counts Two through Four of this Superseding Indictment, the defendants, VYACHESLAV IGOREVICH PENCHUKOV, IVAN VIKTORVICH KLEPIKOV, ALEXEY DMITRIEVICH BRON, ALEXEY TIKONOV, YEVHEN KULIBABA, YURIY KONOVALENKO, and JOHN DOEs #1 through #3, shall forfeit to the United States of America,

pursuant to Title 18, United States Code, Section 982(a)(2)(A), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violations.

33. Pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), upon conviction of a conspiracy to violate Title 18, United States Code, Sections 1028(a)(7), 1030(a)(2), and 1030(a)(5)(A), in violation of Title 18, United States Code, Section 371, as set forth in Count Six of this Superseding Indictment, DEFENDANTS shall forfeit to the United States of America any property, real or personal, which constitutes or is derived from proceeds traceable to said violations.

34. The United States of America gives notice to all defendants, that upon conviction of any defendant, a money judgment may be imposed on that defendant equal to the total value of the property subject to forfeiture, which is at least $70,000,000.00.

35. If any of the property described above, as a result of any act or omission of the defendants:

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

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

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

d. has been substantially diminished in value; or

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

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Section 1963(m).

36. The above-named defendants, and each of them, are jointly and severally liable for the forfeiture obligations as alleged above.

All pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(A), 1963 and 28 U.S.C. § 2461©).

A TRUE BILL.

[redacted]

FOREPERSON

DEBORAH R. GILG
United States Attorney

The United States of America requests that trial of this case be held at Lincoln, Nebraska, pursuant to the rules of this Court.

DEBORAH R. GILG
United States Attorney

By:
STEVEN A. RUSSELL
Assistant United States Attorney

LANNY A. BREUER
Assistant Attorney General, Criminal Division

JOHN T. LYNCH
Chief, Computer Crime & Intellectual Property Section

By:
JOSH A. GOLDFOOT
Senior Counsel
Computer Crime & Intellectual Property Section
United States Department of Justice