1540

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	) Criminal No. 15-198
	)
v.	) (18 U.S.C. §§ 371, 2,
	) 1030(a)(4), 1030(c)(3)(A),
ANDREY GHINKUL	) 1030(a)(5)(A), 1030(c)(4)(B),
a/k/a "Andrei Ghincul"	) 1343 and 1344)
a/k/a "Smilex"	) **(UNDER SEAL)**

INDICTMENT

The grand jury charges:

INTRODUCTION

At all times material to this Indictment, unless otherwise alleged:

1) Malicious software ("malware") is a software program designed to disrupt computer operations, gather sensitive information, gain access to private computer systems, or do other unauthorized action on a computer system. Common examples of malware include viruses, worms, Trojan horses, rootkits, keyloggers, spyware, and others.

2) Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware that uses keystroke logging often will provide the captured keystrokes to the individual who caused the malware to be installed or to a place designated by the individual. Through keystroke logging, individuals are able to

obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these individuals can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers,[1] to accounts that they control.

3) Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

[1] Electronic funds transfers ("EFT") are the exchange and transfer of money through computer-based systems using the Internet. ACH payments allow the electronic transferring of funds from one bank account to another bank account within the ACH network without any paper money changing hands. The ACH network is a network of participating depository financial institutions across the United States, and the network provides for interbank clearing of electronic payments. Because ACH payments require the network to clear the transaction, the funds are not immediately available. Wire transfers also allow electronic transferring of funds from one bank account to another bank account without any paper money changing hands; however, unlike ACH payments, wire transferred funds are immediately available.

4) "Bot," which is short for "robot," is a computer that has been infected by malware and does tasks at the malware's direction.

5) A "botnet" is a network of bots. It is a collection of bots that can communicate with a computer controlling the botnet or with each other through some network architecture.

6) Peer-to-peer networking is an advanced decentralized networking architecture. By comparison, in command and control networks, computers in the network are connected to a central server. When a computer wants to communicate with another device in the network, it communicates with the central server and the central server then communicates with the other device. In peer-to-peer networks, the computers are connected directly to other computers in the network. Computers can communicate with other computers in the network without the use of a centralized server.

7) Bugat is a multifunction malware package, which is specifically designed to automate the theft of confidential personal and financial information, such as online banking credentials, from infected computers through the use of keystroke logging and web injects.

8) Bugat malware is generally distributed through a process known as "phishing", where spam emails are distributed to victims. The emails appear legitimate and are carefully

crafted to entice the victim to click on a hyperlink or to open an attached file. In the event a user clicks on a hyperlink, the user is then usually redirected to an exploit kit, which is a web based software program that scans the victim's computer and operating systems for vulnerabilities and upon discovering one, forces the download of a malicious file upon the victim. In the event the victim opens an attached file, he is then directly infected either by the Bugat malware, or by a loader program, which then downloads the Bugat payload without the victim's consent or knowledge.

9) Bugat, like most modern malware families, is specifically crafted to defeat antivirus and other protective measures employed by victims. As the individuals behind Bugat improved the malware and added functionality, the name of the malware changed, at one point being called "Cridex," and later "Dridex." However, each version was based upon the same original code. Hereinafter a reference in this Indictment to Bugat is meant to refer to Cridex and Dridex as well.

10) A "mule" or "money mule" is a person who received stolen funds into their bank account, and then moved the money to other accounts, or withdrew the funds and transported the funds overseas as smuggled bulk cash.

11) First National Bank was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Pittsburgh, Pennsylvania. It offered online

banking services through computer servers located in the Western District of Pennsylvania.

12) First Commonwealth Bank was a financial institution insured by the Federal Deposit Insurance Corporation, and was headquartered in Indiana, Pennsylvania. It offered online banking services through computer servers located in the Western District of Pennsylvania.

13) The Sharon City School District was a public school district located in Sharon, Pennsylvania in the Western District of Pennsylvania.

14) Penneco Oil Company, Inc., Penneco Pipeline Corporation and Pennquest Oil Corporation (collectively Penneco Oil) were petroleum businesses located in Delmont, Pennsylvania in the Western District of Pennsylvania.

15) The defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," was a citizen and resident of Moldova. He was an administrator of the Bugat botnet. As an administrator, the Defendant managed part of the technical infrastructure of the botnet and played a major role in ensuring that victim computers were infected with the Bugat malware.

COUNT ONE
(Conspiracy)

The grand jury further charges:

16) Paragraphs 1 through 15 above are hereby realleged and incorporated by reference herein, as if fully stated.

THE CONSPIRACY AND ITS OBJECTS

17) From in and around November 2011, the exact date being unknown to the grand jury, and continuing to the present, in the Western District of Pennsylvania and elsewhere, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," knowingly and willfully did conspire, combine, confederate, and agree with other persons known and unknown to the grand jury, to commit the following offenses against the United States:

(a) to knowingly and with the intent to defraud, access a protected computer, without authorization, and by means of such conduct, further an intended fraud and obtain something of value, contrary to the provisions of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A), and Section 2;

(b) to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage, and attempt to cause damage, without authorization, to a protected computer, and the offense did cause and, if completed, caused loss to one or more

persons during any one-year period aggregating at least $5,000.00, contrary to the provisions of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B), and Section 2;

(c) to devise, and intend to devise, a scheme and artifice to defraud businesses and individuals, and to obtain money from these businesses' and individuals' bank accounts and property, that is, confidential personal and financial information, by means of material false and fraudulent pretenses, representations, and promises, and for purpose of executing such scheme and artifice, to transmit, and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures, contrary to the provisions of Title 18, United States Code, Section 1343 and Section 2; and

(d) to knowingly execute, and attempt to execute, a scheme and artifice to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution by means of material false or fraudulent pretenses, representations, and promises, contrary to the provisions of Title 18, United States Code, Section 1344 and Section 2.

18) The purpose of the conspiracy was to use the Bugat malware on infected computers to capture the user's confidential personal and financial information, such as online

banking credentials. The defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and his co-conspirators used the captured information without authorization to falsely represent to banks that the defendant and co-conspirators were the victims or employees of the victims with authority to access the victims' bank accounts. The defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and his co-conspirators subsequently caused or attempted to cause electronic funds transfers from the victims' bank accounts into the bank accounts of money mules. The money mules further transferred the stolen funds to the control of other members of the conspiracy.

MANNER AND MEANS OF THE CONSPIRACY

19) It was a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, sent phishing emails through the Internet that falsely represented themselves to be legitimate emails from legitimate companies, associations, and organizations.

20) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, created the phishing emails to fraudulently induce recipients to click on a hyperlink or attachment that falsely represented itself to be a legitimate link or attachment

containing business or personal information, when in truth and fact, it installed malware without the email recipients' consent or knowledge.

21) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, without authorization, installed and caused the installation of the Bugat malware on Internet-connected victim computers.

22) It was further a part of the conspiracy that the Bugat malware was designed to automate the theft of confidential personal and financial information, such as online banking credentials. The Bugat malware facilitated the theft of confidential personal and financial information by a number of methods. For example, the Bugat malware obtained such information through keystroke logging. Alternatively, the Bugat malware allowed computer intruders to hijack a computer session and use web injects to present a fake online banking webpage to trick a user into entering personal and financial information.

23) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, used the Bugat malware on infected computers to capture the user's confidential personal and financial information, such as online banking credentials, by keystroke logging or by

hijacking the computer session and presenting a web inject, i.e., fake online banking webpages.

24) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, used the captured information without authorization to falsely represent to banks that the Defendant and co-conspirators were victims or employees of victims who had authorization to access the victims' bank accounts and to make electronic funds transfers from the victims' bank accounts.

25) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, used the captured banking credentials to cause banks to make unauthorized wire transfers, ACH payments, or other electronic funds transfers from the victims' bank accounts, without the knowledge or consent of the account holders.

26) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, used money mules to receive the wire transfers, the ACH payments, or other electronic funds transfers from the victims' bank accounts.

27) It was further a part of the conspiracy that the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand

jury, used the money mules to further transfer the stolen funds to reach the control of other members of the conspiracy.

28) It was further a part of the conspiracy that, on or about November 8, 2011, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee of the Sharon City School District, which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to click on a graphic falsely represented to be a legitimate graphic.

29) It was further a part of the conspiracy that on or about November 10, 2011, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, caused the employee to click on the fraudulent graphic and, in so doing, unwittingly install the Bugat malware.

30) It was further a part of the conspiracy that, on or about December 16, 2011, in the Western District of Pennsylvania, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the electronic transfer of $999,000.00 from Sharon City School District's account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.

31) It was further a part of the conspiracy that, on or about August 31, 2012, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, engaged in interstate and foreign wire communications over the Internet by sending to an employee at Penneco Oil, which was located in the Western District of Pennsylvania, a phishing email to fraudulently induce the employee to unwittingly install the Bugat malware.

32) It was further a part of the conspiracy that on or about August 31, 2012, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, caused the employee to unwittingly install the Bugat malware onto a Penneco Oil computer.

33) It was further a part of the conspiracy that from on or about August 31, 2012, through on about September 4, 2012, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, used the Bugat malware to fraudulently obtain the banking credentials of Penneco Oil and to cause the transfer of funds out of Penneco Oil's bank accounts maintained with First Commonwealth Bank.

34) It was further a part of the conspiracy that, on or about August 31, 2012, in the Western District of Pennsylvania, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, fraudulently caused the international

electronic transfer of $2,158,600.00 from Penneco Oil's account X2948 at First Commonwealth Bank to an account in the name of G.S. at Krajinvestbank in Krasnodar, Russia. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for Krajinvestbank.

35) It was further a part of the conspiracy that, on or about September 4, 2012, in the Western District of Pennsylvania, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, fraudulently caused the international electronic transfer of $1,350,000.00 from Penneco Oil's account X1858 at First Commonwealth Bank to an account in the name of B.Y. at CJSC VTB Bank in Minsk, Belarus. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for CJSC VTB Bank.

36) It was further a part of the conspiracy that, on or about September 4, 2012, in the Western District of Pennsylvania, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators known and unknown to the grand jury, fraudulently attempted to cause the electronic transfer of $76,520.00 from Penneco Oil's account X0464 at First Commonwealth Bank to an account in the name of M.O.C. at Trumark Financial Credit Union, Philadelphia, Pennsylvania.

OVERT ACTS

37) In furtherance of the conspiracy, and to effect the objects of the conspiracy, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," and co-conspirators both known and unknown to the grand jury, did commit and cause to be committed, the following overt acts, among others, in the Western District of Pennsylvania and elsewhere:

(a) On or about November 8, 2011, the Defendant and co-conspirators sent to an employee at the Sharon City School District a phishing email, in order to cause the Bugat malware to be installed on an Internet-connected computer used by the Sharon City School District, without the employee's consent or knowledge.

(b) On or about November 10, 2011, the Defendant and co-conspirators caused the Bugat malware to be installed, without authorization, on the Sharon City School District's Internet-connected computer located in the Western District of Pennsylvania.

(c) On or about December 16, 2011, in the Western District of Pennsylvania, the Defendant and co-conspirators fraudulently attempted to cause the electronic transfer of $999,000.00 from Sharon City School District's account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.

(d) On or about August 31, 2012, the Defendant and co-conspirators sent to an employee at Penneco Oil a phishing email, in order to cause the Bugat malware to be installed on an Internet-connected computer used by Penneco Oil, without the employee's consent or knowledge.

(e) On or about August 31, 2012, the Defendant and co-conspirators caused the Bugat malware to be installed, without authorization, on Penneco Oil's Internet-connected computer located in the Western District of Pennsylvania.

(f) From on or about August 31, 2012 through on or about September 4, 2012, the Defendant and co-conspirators caused the transfer of funds out of Penneco Oil's bank accounts maintained with First Commonwealth Bank.

(g) On or about August 31, 2012, the Defendant and co-conspirators caused the international electronic transfer of $2,158,600.00 from Penneco Oil's account X2948 at First Commonwealth Bank to an account in the name of G.S. at Krajinvestbank in Krasnodar, Russia. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for Krajinvestbank.

(h) On or about September 4, 2012, in the Western District of Pennsylvania, the Defendant and co-conspirators caused the international electronic transfer of $1,350,000.00 from Penneco Oil's account X1858 at First Commonwealth Bank to

an account in the name of B.Y. at CJSC VTB Bank in Minsk, Belarus. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for CJSC VTB Bank.

(i) On or about March 12, 2014, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," engaged in a chat conversation over the Internet with a member of the conspiracy known to the grand jury in which the Defendant stated that he had a new theme for spam emails, namely, that the purported originator of the email was a medical institution and that the victim recipient had tested positive for cancer.

(j) On or about July 23, 2014, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," sent an email to himself from iavorscaia@gmail.com to iavorscaia@gmail.com containing a loader file designed to download Bugat malware into victim computers.

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

COUNT TWO
(Wire Fraud)

The grand jury further charges:

38) Paragraphs 1 through 15 and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

39) From on or about November 8, 2011, until on or about December 16, 2011, in the Western District of Pennsylvania and elsewhere, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," for the purpose of executing, and attempting to execute, a scheme and artifice to defraud the Sharon City School District, and to obtain money and property of the Sharon City School District, by means of material false and fraudulent pretenses, representations, and promises, well knowing at the time that the pretenses, representations, and promises were false and fraudulent when made, knowingly did transmit, and cause to be transmitted, in interstate and foreign commerce, certain writings, signs and signals, that is, an electronic phishing email for the purpose of fraudulently gaining access to a protected computer of an employee of the Sharon City School District for use in attempting the fraudulent electronic transfer of funds from the Sharon City School District bank account.

In violation of Title 18, United States Code, Section 1343 and Section 2.

COUNT THREE
(Unauthorized Computer Access with Intent to Defraud)

The grand jury further charges:

40) Paragraphs 1 through 15 and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

41) From on or about November 8, 2011 through on or about December 16, 2011, the exact date being unknown, in the Western District of Pennsylvania and elsewhere, the defendant, Andrey Ginkul, a/k/a "Andrei Ghincul, a/k/a Smilex, knowingly, and with intent to defraud, accessed a protected computer of the Sharon City School District, without authorization, and by means of such conduct furthered an intended fraud and obtained something of value, specifically, the banking credentials, including the username and password, of an employee of Sharon City School District for use in attempting the fraudulent electronic transfer of funds from the bank account of the Sharon City School District.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A), and Section 2.

COUNT FOUR
(Damaging a Computer)

The grand jury further charges:

42) Paragraphs 1 through 15 and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

43) From on or about November 8, 2011 through on or about December 16, 2011, the exact date being unknown, in the Western District of Pennsylvania and elsewhere, the defendant, Andrey Ginkul, a/k/a "Andrei Ghincul, a/k/a Smilex, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage, without authorization, to a protected computer belonging to the Sharon City School District, an offense which would, if completed, have caused a loss to a person during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i), and Section 2.

COUNT FIVE
(Unauthorized Computer Access with Intent to Defraud)

The grand jury further charges:

44) Paragraphs 1 through 15 and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

45) From on or about August 31, 2012, through on or about September 4, 2012, the exact dates being unknown, in the Western District of Pennsylvania and elsewhere, the defendant, Andrey Ginkul, a/k/a "Andrei Ghincul, a/k/a Smilex, knowingly, and with intent to defraud, accessed a protected computer of Penneco Oil, without authorization, and by means of such conduct furthered an intended fraud and obtained something of value, specifically, the banking credentials, including the username and password, of an employee of Penneco Oil for use in the fraudulent electronic transfer of funds totaling $3,508,600 from the bank accounts of Penneco Oil.

In violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A), and Section 2.

COUNT SIX
(Damaging a Computer)

The grand jury further charges:

46) Paragraphs 1 through 15 and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

47) From in and around August 31, 2012, and continuing thereafter to on or about September 4, 2012, in the Western District of Pennsylvania and elsewhere, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," did knowingly cause and attempt to cause the transmission of a program, information, code, and command, and, as a result of such conduct, did intentionally cause damage and attempt to cause damage, without authorization, to a protected computer belonging to Penneco Oil, which offense caused, and would, if completed, have caused, loss aggregating at least $5,000 in value to at least one person during a one-year period.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i), and Section 2.

COUNTS SEVEN THROUGH NINE
(Bank Fraud)

The grand jury further charges:

48) Paragraphs 1 through 15, and 19 through 37 above are hereby realleged and incorporated by reference herein, as if fully stated.

49) On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," having devised and intended to devise a scheme and artifice to defraud First Commonwealth Bank and First National Bank to obtain monies and funds owned by and under the custody and control of First Commonwealth Bank and First National Bank by means of material false and fraudulent pretenses, representations and promises, well knowing at the time that the pretenses, representations and promises would be and were false and fraudulent when made, did knowingly execute and attempt to execute the foregoing scheme and artifice, by causing, and attempting to cause, the transfer of funds, with each transfer, and attempted transfer, being a separate count of this indictment as described below:

Count	On or About Date	Description
7	December 16, 2011	The attempted wire transfer of $999,000.00 from Sharon City School District's account at First National Bank to an account in the name of S.M. at PJSC Bank Forum, Kiev, Ukraine.
8	August 31, 2012	The wire transfer of $2,158,600.00 out of First Commonwealth Bank account X2948 belonging to Penneco Oil to an account in the name of G.S. at Krajinvestbank in Krasnodar, Russia. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for Krajinvestbank.
9	September 4, 2012	The wire transfer of $1,350,000.00 out of First Commonwealth Bank account X1858 belonging to Penneco Oil to an account in the name of B.Y. at CJSC VTB Bank in Minsk, Belarus. The transaction was processed through Citibank, New York City, New York, as the correspondent bank for CJSC VTB Bank.

In violation of Title 18, United States Code, Section 1344 and Section 2.

FORFEITURE ALLEGATION I

50) The allegations contained in Count One and Counts Three through Six of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

51) Upon conviction of the offenses in violation of Title 18, United States Code, Sections 371, 2, 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A) and 1030(c)(4)(B)(i), set forth in Count One and Counts Three through Six of this Indictment, defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," shall forfeit to the United States of America:

a. pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense, such property includes but is not limited to a money judgment for a sum of money equal to the proceeds obtained as a result of the offense; and

b. pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

52) If through any acts or omission by the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," any or

all of the property described in paragraphs 50 to 51 above (hereinafter the "Subject Properties"):

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

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

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

d. has been substantially diminished in value; or

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

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B), 982(b) and 1030(i), Title 21, United States Code, Section 853, and Title 28 U.S.C. § 2461(c).

FORFEITURE ALLEGATION II

53) The allegations contained in Count Two and Counts Seven through Nine of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeitures pursuant to Title 18, United States Code, Section 981(a)(1)(C) and 28 United States Code, Section 2461(c).

54) Upon conviction of the offenses in violation of Title 18, United States Code, Sections 1343, 1344 and 2 set forth in Count Two and Counts Seven through Nine of this Indictment, the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes, and is derived from, proceeds traceable, directly and indirectly, to such violations. The property to be forfeited includes, but is not limited to, a money judgment for a sum of money equal to the proceeds obtained as a result of the offenses.

55) If through any acts or omission by the defendant, ANDREY GHINKUL a/k/a "Andrei Ghincul," a/k/a "Smilex," any or all of the property described in paragraphs 53 to 54 above (hereinafter the "Subject Properties"):

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 28, United States Code, Section 2461(c).

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

A True Bill,

FOREPERSON

DAVID J. HICKTON
United States Attorney
PA ID NO. 34524

STEPHEN R. KAUFMAN
FOR
DAVID J. HICKTON

CERTIFIED FROM THE RECORD
09/17/2015
ROBERT V. BARTH JR., CLERK
Keith Anderson
Deputy Clerk