GSG/2011R01361

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 13-
	:	
OLEG PIDTERGERYA	:	18 U.S.C. §§ 1349 and 371

I N F O R M A T I O N

The defendant having waived in open court prosecution by Indictment, the United States Attorney for the District of New Jersey charges:

Count One
(Wire Fraud Conspiracy)

Relevant Entities and Individuals

1. At all times relevant to this Information:

a. Co-conspirator OLEKSIY SHARAPKA was a resident of Kiev, Ukraine, and the leader of the "Sharapka Cash Out Organization," a criminal enterprise that operated a large-scale computer hacking and identity theft scheme from at least as early as in or about March 2012 through in or about June 2013. Pursuant to the scheme, co-conspirator SHARAPKA and his co-conspirators opened up bank accounts and pre-paid debit cards in the names of identity theft victims (the "Fraudulent Accounts"), which they funded by, among other means, fraudulently diverting funds from victims' bank accounts through computer hacking, or with the proceeds of fraudulent tax returns they caused to be filed with the Internal Revenue Service ("IRS") in the names of identity theft victims. Thereafter, co-conspirator SHARAPKA and his co-conspirators "cashed out" the Fraudulent Accounts and shared the illicit proceeds.

b. Co-conspirator LEONID YANOVITSKY, a/k/a "Lenny," not named as a defendant herein, was a resident of Kiev, Ukraine, and assisted co-conspirator SHARAPKA in

b. Co-conspirator LEONID YANOVITSKY, a/k/a "Lenny," not named as a defendant herein, was a resident of Kiev, Ukraine, and assisted co-conspirator SHARAPKA in managing the Sharapka Cash Out Organization by, among other things, tracking the Fraudulent Accounts used by the organization and receiving overseas wires from co-conspirators in the United States.

c. Defendant OLEG PIDTERGERYA was a resident of Brooklyn, New York, who managed a "cash out crew" for the Sharapka Cash Out Organization that cashed out Fraudulent Accounts in and around the New York City area (the "New York Cash Out Crew").

d. Co-conspirator "R.G.," not named as a defendant herein, was a resident of Brooklyn, New York, who worked as a "casher" under defendant PIDTERGERYA's supervision for the New York Cash Out Crew from in or about May 2012 through in or about October 2012.

e. Co-conspirator "R.D.," not named as a defendant herein, was a resident of Malden, Massachusetts, who managed a cash out crew in Massachusetts for the Sharapka Cash Out Organization.

f. During the course of the conspiracy, co-conspirator SHARAPKA and others targeted the customers of over a dozen financial institutions, retail brokerage firms, financial services companies, accounting firms, and payroll processing companies (collectively, the "Victim Companies"), including the following:

i. Automatic Data Processing, Inc. ("ADP") was a victim company headquartered in New Jersey, and was one of the world's largest providers of outsourcing solutions for human resources, payroll, and tax administration services. Among other services, ADP offered its customers the ability to manage their payroll accounts over the Internet. ADP customers could, for example, access ADP's website and, through the use of account log-in credentials, add employees to their payroll. Similarly, ADP customers could use ADP's website

to direct that money (*i.e.*, salary) be directly transferred from their bank accounts to their employees, or from their bank accounts to ADP and then to their employees, depending on how their accounts with ADP were set up. One of the ways in which an ADP customer's employee could receive payroll was by directing their payroll onto pre-paid debit cards.

ii. JP Morgan Chase Bank, N.A. ("Chase") was a victim company headquartered in New York that, among other things, provided personal banking services to its customers. One of the features that Chase offered its customers was online access to their personal banking accounts.

iii. Fundtech Holdings LLC ("Fundtech") was a victim company headquartered in New Jersey that offered its clients, among other things, an online bill payment system called "Modern Payments." Modern Payments enabled Fundtech's clients to both collect bill payments and issue refunds to their customers online. Municipalities such as the city of Evans, Colorado (the "City of Evans") used the Modern Payments platform to collect utilities payments and to issue refunds for utilities overpayments to its customers.

2. From at least as early as in or about March 2012 through in or about June 2013, in the District of New Jersey and elsewhere, defendant

OLEG PIDTERGERYA

did knowingly and intentionally conspire and agree with co-conspirator OLEKSIY SHARAPKA, and others known and unknown, to devise a scheme and artifice to defraud the Victim Companies and their customers, as well as the IRS, and to obtain money and property from the Victim Companies and their customers, as well as the IRS, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communications in

interstate and foreign commerce, certain signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

Object of the Conspiracy

3. The object of the conspiracy was for co-conspirator SHARAPKA, defendant PIDTERGERYA, and others to enrich themselves by: (1) compromising the account and personal identifying information of individuals through various means; (2) diverting money from victims' bank accounts to the Fraudulent Accounts, which they subsequently cashed out; and (3) filing fraudulent tax returns claiming refunds in the names of identity theft victims and directing those refunds to the Fraudulent Accounts, which they subsequently cashed out.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that international computer hackers working for the Sharapka Cash Out Organization first compromised the log-in credentials (*e.g.*, usernames and passwords) of customers of the Victim Companies, using hacking methods directed primarily at the Victim Companies' customers.

5. It was further part of the conspiracy that the computer hackers used the compromised log-in credentials to gain unauthorized access to the customers' accounts at the Victim Companies.

6. It was further part of the conspiracy that the computer hackers diverted money from the compromised accounts to Fraudulent Accounts controlled by the Sharapka Cash Out Organization.

7. It was further part of the conspiracy that after the funds had been diverted, co-conspirator SHARAPKA directed individuals in the United States, including defendant PIDTERGERYA, to cash out the Fraudulent Accounts by, among other things, conducting Automated Teller Machine ("ATM") withdrawals and fraudulent purchases.

8. It was further part of the conspiracy that from at least as early as in or about October 2011 through in or about June 2013, co-conspirator SHARAPKA and others compromised the personal identifying information of individuals, and used the compromised information to file fraudulent tax returns claiming refunds with the IRS. Those refunds were also directed to the Fraudulent Accounts and cashed out in the manner described above.

9. It was further part of the conspiracy that the majority of the illicit proceeds generated by the Sharapka Cash Out Organization's operations flowed up from the cashers to their managers, and then to the higher levels of the operation. The cashers often transferred funds from the United States to co-conspirator SHARAPKA and other co-conspirators overseas using international wire transfer services, among other methods.

Fraudulent Activity

10. In furtherance of the conspiracy and to effect the unlawful objects thereof, co-conspirator SHARAPKA, defendant PIDTERGERYA, and others committed and caused to be committed the following acts, among others:

A. Fraudulent Transfers from the Payroll Accounts of ADP Customers

11. From in or about October 2011 through in or about June 2013, hackers obtained the account log-in credentials of ADP customers from the customers themselves (not through ADP) using a variety of unlawful means. Next, the hackers used the fraudulently obtained log-in credentials to access the customers' accounts, which were hosted on ADP computer servers, located in New Jersey, Georgia and South Dakota. Using these methods, the hackers gained control of the accounts of over 130 ADP customers. Thereafter, they attempted to divert millions of dollars from those accounts by transferring and attempting to transfer money from the compromised customer accounts at ADP to the Fraudulent Accounts. After funds had been successfully diverted to the Fraudulent Accounts, co-conspirators SHARAPKA and

YANOVITSKY directed defendant PIDTERGERYA, co-conspirator R.D., and others to cash out the Fraudulent Accounts, deduct a fee, and return the balance of the proceeds to them in Ukraine. In total, co-conspirator SHARAPKA and others transferred approximately $700,000 to the Fraudulent Accounts, which they subsequently cashed out.

12. For example, in or about June 2012, co-conspirator SHARAPKA and others attempted to transfer funds belonging to ADP customer "B&S" to a pre-paid debit card ending in 2123 in the name of "A.S." (the "A.S. 2123 Card"), which was opened without A.S.'s knowledge or consent. Although ADP was able to prevent this fraudulent transfer, co-conspirator SHARAPKA and others were able to fraudulently transfer funds to that card on or about July 6, 2012 and on or about July 7, 2012, from the accounts of other Victim Customers. Subsequently, on or about July 9, 2012, and on or about July 10, 2012, defendant PIDTERGERYA used the A.S. 2123 Card at a bank in Queens, New York to withdraw the fraudulently transferred funds.

B. Fraudulent Transfers from Chase Bank Accounts

13. Between in or about October 2012 and in or about April 2013, hackers transferred funds from the accounts of Chase customers to multiple pre-paid American Express debit cards controlled by the Sharapka Cash Out Organization. For example, on or about February 18, 2013, co-conspirator SHARAPKA e-mailed defendant PIDTERGERYA information related to approximately 11 debit cards opened in the names of others that were used to receive fraudulent electronic funds transfers from Chase Bank victims (the "Fraudulent AMEX Pre-paid Cards"), including one in the name of "R.M." (the "R.M. Amex Card"). In total, co-conspirator SHARAPKA and others transferred approximately $60,000 from the accounts of Chase customers to the Fraudulent Accounts, which they subsequently cashed out.

14. On or about February 20, 2013, defendant PIDTERGERYA made a cash withdrawal using the R.M. Amex Card, which received fraudulent electronic funds transfers from Chase Bank victims, at an ATM located in Brooklyn, New York.

C. Fraudulent Transfers from Fundtech Customers

15. From on or about November 23, 2012 through on or about December 12, 2012, hackers caused approximately $330,000 in unauthorized rebates to be issued through the Fundtech Modern Payments platform by compromising third-party credentials. Many of these unauthorized rebates were sent to Fraudulent Accounts controlled by the Sharapka Cash Out Organization, including to a business bank account ending in 8175 in the name of "A.C.C." opened at a bank in Brooklyn, New York (the "A.C.C. 8175 Account"). The A.C.C. 8175 Account was opened at defendant PIDTERGERYA's direction by co-conspirator R.G. using a fraudulent Ohio driver's license in the name of "S.C."

16. Thereafter, defendant PIDTERGERYA and others, including co-conspirator R.G. cashed out Fraudulent Accounts that had received money from Fundtech customers. For example, on or about December 9, 2012, defendant PIDTERGERYA withdrew approximately $480.00 in cash from an ATM in Mt. Pocono, Pennsylvania, from the A.C.C. 8175 Account, which was used to receive money fraudulently diverted from a Fundtech customer.

D. Fraudulent IRS Refunds

17. From between in or about March 2012 through in or about September 2012, co-conspirator SHARAPKA and others caused fraudulent tax returns claiming refunds in the names of identity theft victims to be submitted to the IRS. The fraudulent tax refunds were also directed to Fraudulent Accounts controlled by the Sharapka Cash Out Organization. In total, co-conspirator SHARAPKA and others attempted to obtain approximately $500,000 in fraudulent tax refunds in this manner, and successfully directed approximately $200,000 in fraudulent

refunds to the Fraudulent Accounts, which they subsequently cashed out, primarily using defendant PIDTERGERYA's New York Cash Out Crew.

18. For example, on or about May 30, 2012, at defendant PIDTERGERYA's direction, co-conspirator R.G. opened a fraudulent Chase Bank account ending in 3889 in the name of identity theft victim "R.M." (the "R.M. 3889 Account"), using a fraudulent Florida driver's license with co-conspirator R.G.'s photo and R.M.'s name. Thereafter, the Sharapka Cash Out Organization transferred money from approximately 20 fraudulent IRS tax refunds to the R.M. 3889 Account, including approximately $20,000 in fraudulent IRS tax refunds between in or about June 2012 and in or about July 2012. Following these transfers, defendant PIDTERGERYA and co-conspirator R.G. cashed out the account by making a series of ATM withdrawals in and around Brooklyn, New York.

E. The Proceeds of the Fraud

19. The Sharapka Cash Out Organization used a variety of means to transfer the proceeds of their fraud overseas.

Direct Overseas Transfers

a. On multiple occasions throughout 2012, defendant PIDTERGERYA and others wired the illicit proceeds of the scheme directly to co-conspirator SHARAPKA in Ukraine, or directed others to do the same. For example, on or about May 5, 2012, defendant PIDTERGERYA sent approximately $740 from a store in Brooklyn, New York to co-conspirator SHARAPKA in Ukraine, using Moneygram.

b. On or about June 26, 2012, co-conspirator R.D. sent approximately $2,000 from a convenience store in Malden, Massachusetts to co-conspirator SHARAPKA in Ukraine, using Moneygram.

The "Mirku 0414 Account" and the "Kumir 0443 Account"

c. In addition, co-conspirator SHARAPKA directed members of the Sharapka Cash Out Organization to move the fraud proceeds through bank accounts they controlled in the names of Mirku, Inc. ("the "Mirku 0414 Account") and Kumir, Inc. (the "Kumir 0443 Account"). Specifically, in or about October 2012, co-conspirator SHARAPKA e-mailed defendant PIDTERGERYA and co-conspirator R.D. the account information for the Mirku 0414 Account and the Kumir 0443 Account, and directed them to make cash deposits under $10,000 into those accounts. Thereafter, defendant PIDTERGERYA and co-conspirator R.D., and others made a number of cash deposits under $10,000 into the Mirku 0414 Account and the Kumir 0443 Account.

d. For example, between in or about June 2012 and in or about March 2013, the Sharapka Cash Out Organization made approximately 50 cash and money order deposits – each slightly under $10,000 – into the Mirku 0414 Account for a total of approximately $450,000. After being deposited in the Mirku 0414 Account, the funds were moved or wired to other accounts. During that same period, the Sharapka Cash Out Organization made approximately 75 cash and money order deposits – each slightly under $10,000 – into the Kumir 0443 Account for a total of approximately $700,000. After being deposited in the Kumir 0443 Account, the funds were moved or wired to other accounts.

In violation of Title 18, United States Code, Section 1349.

Count Two
(Conspiracy to Commit Access Device Fraud and Identity Theft)

1. The allegations set forth in Paragraphs 1 and 4 through 19 of Count One above are hereby repeated, realleged and incorporated as if full set forth herein.

2. From at least as early as in or about March 2012 through in or about June 2013, in the District of New Jersey and elsewhere, defendant

OLEG PIDTERGERYA

did knowingly and intentionally conspire and agree with co-conspirator OLEKSIY SHARAPKA, and others known and unknown to commit offenses against the United States, namely, to:

(a) knowingly, and with intent to defraud, traffic in and use one or more unauthorized access devices during a one-year period, and by such conduct obtain anything of value aggregating $1,000 or more during that period in violation of Title 18, United States Code, Section 1029(a)(2); and

(b) knowingly transfer, possess, and use without lawful authority, a means of identification of another person with the intent to commit, and aid and abet, access device fraud and wire fraud, in violation of Title 18, United States Code, Section 1028(a)(7).

Object of the Conspiracy

3. The object of the conspiracy was for co-conspirator SHARAPKA, defendant PIDTERGERYA, and others to enrich themselves by: (1) compromising the account and personal identifying information of individuals through various means; (2) diverting money from victims' bank accounts to the Fraudulent Accounts, which they subsequently cashed out; and (3) filing fraudulent tax returns claiming refunds in the names of identity theft victims and directing those refunds to the Fraudulent Accounts, which they subsequently cashed out.

Overt Acts

4. In furtherance of the conspiracy and to effect the unlawful objects thereof, the following overt acts, among others, were committed in the District of New Jersey and elsewhere:

a. From in or about October 2011 through in or about June 2013, co-conspirators used log-in credentials stolen directly from ADP customers to unlawfully access those customers' ADP accounts, which were hosted on ADP computer servers located in, among other places, New Jersey.

b. On or about December 9, 2012, defendant PIDTERGERYA withdrew approximately $480.00 in cash from an ATM in Mt. Pocono, Pennsylvania, from the A.C.C. 8175 Account, which was fraudulently opened and used to receive money fraudulently diverted from a Fundtech customer.

c. On or about February 20, 2013, defendant PIDTERGERYA made a cash withdrawal using the R.M. Amex Card at an ATM located in Brooklyn, New York.

d. From on or about November 23, 2012 through on or about December 12, 2012, co-conspirators compromised the Fundtech Modern Payments platform.

In violation of Title 18, United States Code, Section 371.

Forfeiture Allegation

1. The allegations contained in this Information are hereby realleged and incorporated by reference for the purpose of noticing forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(B) and Title 28, United States Code, Section 2461(c).

2. The United States hereby gives notice to the defendant, that upon his conviction of the offenses charged in this Information, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(B) and Title 28, United States Code, Section 2461(c), which requires any person convicted of such offenses to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offenses.

3. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

(a) cannot be located upon the exercise of due diligence;

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

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) to seek forfeiture of any other property of such defendant up to the value of the forfeitable property described above.

Paul J. Fishman

PAUL J. FISHMAN
United States Attorney

CASE NUMBER: 14-_____

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

OLEG PIDTERGERYA

INFORMATION FOR

18 U.S.C. §§ 1349 and 371

PAUL J. FISHMAN
UNITED STATES ATTORNEY, NEWARK, NEW JERSEY

GURBIR S. GREWAL
ASSISTANT U.S. ATTORNEY
NEWARK, NEW JERSEY
(973) 645-2931