GSG/2011R01361

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 14-
	:	
ROBERT DUBUC	:	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 and the "Sharapka Cash Out Organization"

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 obtained 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. The "Massachusetts Cash Out Crew"

b. Defendant ROBERT DUBUC was a resident of Malden, Massachusetts, who managed a "cash out crew" for the Sharapka Cash Out Organization that cashed out Fraudulent Accounts in and around Massachusetts (the "Massachusetts Cash Out Crew").

c. Co-conspirator "L.T.," not named as a defendant herein, was a resident of Salem, Massachusetts, who worked under defendant DUBUC's supervision as a casher for the Massachusetts Cash Out Crew.

d. During the period of the conspiracy charged herein, the Massachusetts Cash Out Crew cashed out approximately $390,000 in illicit proceeds from Fraudulent Accounts.

C. Selected Victim Companies

e. 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. 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

ROBERT DUBUC

did knowingly and intentionally conspire and agree with co-conspirator OLEKSIY SHARAPKA, co-conspirator L.T., 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, co-conspirator L.T., defendant DUBUC, 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 DUBUC, 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 DUBUC, 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 a number of 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-conspirator SHARAPKA and others directed defendant DUBUC and others to cash out the Fraudulent Accounts, deduct a fee, and return the balance of the proceeds to them in Ukraine. Defendant DUBUC, in turn, solicited co-conspirator L.T. and others to assist him.

12. For example, on or about May 7, 2012, co-conspirator SHARAPKA e-mailed defendant DUBUC, and asked defendant DUBUC to send him account-related information for Fraudulent Accounts that could be used to receive money diverted from the Victim Companies' customers. In response, on or about May 10, 2012, defendant DUBUC e-mailed co-conspirator SHARAPKA the requested information, including information related to a pre-paid debit card ending in 3027, opened in the name of "N.C." (the "N.C. 3027 Card"), without N.C.'s knowledge or consent. Thereafter, co-conspirator SHARAPKA and others attempted to divert money from the bank account of ADP customer B&S to the N.C. 3027 Card.

B. Fraudulent Transfers from Fundtech Customers

13. From on or about November 23, 2012 through on or about December 12, 2012, hackers caused 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. For example, on or about December 4, 2012, co-conspirator SHARAPKA e-mailed defendant DUBUC instructions for withdrawing funds from a bank account ending in 6409 in the name of "M.L." (the "M.L. 6409 Account"), which was opened without M.L's knowledge or consent. Among other things, the instructions stated that there would be transfers into the M.L. 6409 Account from "Modern Payments." Thereafter, on or about December 12, 2012, at defendant DUBUC's direction, co-conspirator L.T. traveled to a bank located in and around Beverly, Massachusetts, accessed the M.L. 6409 Account, which had received fraudulent transfers from the City of Evans, using an ATM card in the name of M.L., and withdrew money from the account.

D. Fraudulent IRS Refunds

14. 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 refunds were 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. The majority of these fraudulent tax refunds were cashed out by crews in and around New York. Approximately $10,000 of these fraudulent tax refunds were directed to Fraudulent Accounts that were cashed out by defendant DUBUC and the Massachusetts Cash Out Crew.

E. The Proceeds of the Fraud

15. 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 DUBUC wired money directly to co-conspirator SHARAPKA in Ukraine, or directed others to do the same. For example, on or about June 26, 2012, defendant DUBUC wired approximately $2,000 from a convenience store in Malden, Massachusetts to co-conspirator SHARAPKA in Ukraine.

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

b. 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, on or about October 10, 2012, co-conspirator

SHARAPKA e-mailed defendant DUBUC the account information for the Mirku 0414 Account and the Kumir 0443 Account. Thereafter, defendant DUBUC and others made a number of cash deposits under $10,000 into the Mirku 0414 Account and the Kumir 0443 Account.

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 15 of Count One above are hereby repeated, realleged and incorporated as if set forth in full 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

ROBERT DUBUC

did knowingly and intentionally conspire and agree with co-conspirator OLEKSIY SHARAPKA, co-conspirator L.T., 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, co-conspirator L.T., defendant DUBUC, 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 May 10, 2012, defendant DUBUC e-mailed co-conspirator SHARAPKA information related to the N.C. 3027 Card.

c. On or about June 26, 2012, defendant DUBUC, sent $2,000 to co-conspirator SHARAPKA in Kiev, Ukraine, using Moneygram.

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.

PAUL J. FISHMAN
United States Attorney

CASE NUMBER: 14-

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

ROBERT DUBUC

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