

APR 16 2012

United States District Court  
District of New Jersey

MADELINE COX ARLEO  
U.S. MAG. JUDGE

UNITED STATES OF AMERICA : HON. MADELINE COX ARLEO

v. : Magistrate No. 12-8059

PETR MURMYLYUK : **CRIMINAL COMPLAINT**

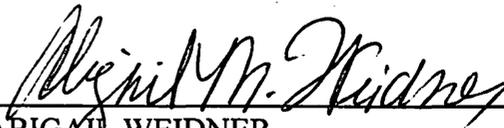
a/k/a "Dmitry Tokar," : **FILED UNDER SEAL**

I, Abigail Weidner, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

  
 \_\_\_\_\_  
 ABIGAIL WEIDNER  
 Special Agent  
 Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,

April 16, 2012 at  
 Date Madeline Cox Arleo  
 Honorable Madeline Cox Arleo  
 United States Magistrate Judge

Newark, New Jersey  
 City and State

## ATTACHMENT A

Between in or about August 2010 and on or about November 3, 2011, in Monmouth and Bergen Counties, in the District of New Jersey, and elsewhere, defendant

PETR MURMYLYUK,  
a/k/a "Dmitry Tokar,"

did knowingly and intentionally conspire and agree with CC1, Anton Mezentsev, Mikhail Shatov, Galina Korelina, M.Z., D.Z., and others to:

(1) devise and intend to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice to defraud to transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce certain writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343;

(2) knowingly and with intent to defraud access computers in interstate commerce and exceed authorized access to such computers, and by means of such conduct further the intended fraud and obtaining anything of value, namely United States currency, contrary to Title 18, United States Code, Section 1030(a)(4); and

(3) knowingly and willfully, directly and indirectly, by the use of the means and instrumentalities of interstate commerce, and of the mails and of the facilities of national securities exchanges, in connection with the purchase and sale of securities, use and employ manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section 240.10b-5, by (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, as more fully described below, in violation of Title 15, United States Code, Sections 78j(b) and 78ff; Title 17, Code of Federal Regulations, Section 240.10b-5.

### Overt Acts

In furtherance of the conspiracy and to effect its unlawful object, the following overt acts were committed in the District of New Jersey and elsewhere:

a. On or about September 6, 2011, defendant Murmylyuk impersonated Dmitry Tokar in a telephone call to Trade Station Securities.

b. On or about October 14, 2011, defendant Murmylyuk caused Trade Station Securities to send an e-mail regarding the account of Dmitry Tokar to [denisbofa@\[Provider1\].com](mailto:denisbofa@[Provider1].com).

c. On or about October 25, 2011, a coconspirator hacker gained unauthorized access to a victim's account at Scottrade using a computer in Bergen County, New Jersey.

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

## ATTACHMENT B

I, Abigail Weidner, am a Special Agent with the Federal Bureau of Investigation (“FBI”). Based upon my investigation and my discussions with other individuals involved in this investigation, I have knowledge of the facts below. I describe statements attributed herein to individuals in substance and in part.

1. At all times relevant to this Complaint:

### Defendant

- a. Defendant Petr Murmylyuk, a/k/a “Dmitry Tokar,” was a citizen of Russia and resided in or near Brooklyn, New York.

### Coconspirators

- b. CC1, a coconspirator who is not charged as a defendant herein, was a citizen of Russia and resided in or near Brooklyn, New York.

- c. Anton Mezentsev, Galina Korelina, and Mikhail Shatov, coconspirators who are not charged as defendants herein, were citizens of Russia and resided in or near Houston, Texas.

- d. D.Z., and M.Z., coconspirators who are not charged as defendants herein, were citizens of Kazakhstan and resided in or near Houston, Texas.

### Companies

- e. Fidelity Investments (“Fidelity”), Scottrade, E\*Trade, Charles Schwab, OptionsHouse, and Trade Station Securities (“TSS”) were companies that offered online brokerage accounts to their customers (collectively “the Online Brokerage Companies”).

- f. Comerica Bank (“Comerica”) and Wells Fargo Bank (“Wells Fargo”) were financial institutions whose deposits were insured by the Federal Deposit Insurance Corporation.

### The Investigation

2. The FBI, the United States Secret Service, and the Internal Revenue Service - Criminal Investigation have been investigating a fraudulent scheme to steal money from victims’ accounts at the Online Brokerage Companies.

3. Interviews with security officials at the Online Brokerage Companies revealed that the scheme worked as follows:

a. One or more coconspirators (“the Hackers”) gained unauthorized access to individual victims’ online brokerage accounts at Fidelity, Scottrade, and E\*Trade (“the Victim Accounts”).

b. Upon gaining access to the Victim Accounts, the Hackers changed telephone numbers or e-mail addresses on file to prevent notice of unauthorized trading activity from reaching victims.

c. The Hackers used their control of the Victim Accounts to cause the Victim Accounts to make unfavorable trades benefitting the Hackers as described below.

#### *The Options Fraud*

d. The Hackers sometimes used liquid assets in the Victim Accounts to purchase shares of thinly traded stocks and authorized the purchase and sale of options contracts in the Victim Accounts (i.e., the right to buy or sell a security at a designated price in future).

e. The Hackers then used their unauthorized access to the Victim Accounts to offer to sell options on the thinly traded stocks (“the Options”).

f. At the same time, the Hackers used stolen identities to establish trading accounts at OptionsHouse, TSS, and elsewhere (“the Profit Accounts”). The Hackers used the Profit Accounts to purchase the Options from the Victim Accounts at a relatively low price.

g. The Hackers then offered the same Options for sale at grossly inflated prices — typically up to nine times the price the Profit Accounts had paid for them moments minutes earlier.

h. The Hackers then stole money from the Victim Accounts by causing the Victim Accounts to re-purchase the Options from the Profit Accounts at the inflated prices.

#### *The Short Sale Fraud*

i. At other times, the Hackers used assets in the Victim Accounts to purchase shares of securities that the Hackers offered for sale (through the Profit Accounts) at grossly inflated prices (“the Short Sale Fraud”).

j. To accomplish this variation of the scheme, the Hackers used the Profit Accounts to offer a short sale<sup>1</sup> of a security at a price well over that day's market price for the security in question.

k. Within moments of offering the shares for short sale from the Hackers Accounts, the Hackers used their control over the Victim Accounts to force the Victim Accounts to purchase the shares at the inflated price, resulting in a profit to a Profit Account at the expense of a Victim Account.

l. The Hackers then covered their fraudulent short sale by re-purchasing the borrowed security at the lower market price.

m. The Hackers profited based on the difference between the falsely inflated price at which the Profit Accounts sold and the true (lower) market price at which the Hackers covered their short sale.

#### *Harvesting the Proceeds of the Fraud*

n. Defendant Murmylyuk and CC1 recruited foreign nationals visiting, studying, and living in the United States, including Anton Mezentsev, Galina Korelina, Mikhail Shatov, D.Z., M.Z., and others, to open bank accounts into which proceeds of the sham trades benefitting the Profit Accounts could be deposited ("the Mule Accounts").

o. Defendant Murmylyuk and CC1 caused the proceeds of the sham trades described above to be transferred from the Profit Accounts into the Mule Accounts, where Anton Mezentsev, Galina Korelina, Mikhail Shatov, M.Z., D.Z., and others withdrew the funds and returned them to CC1 and others.

p. Fidelity, Scottrade, E\*Trade, and Charles Schwab have reported losses to date of approximately \$1,000,000 from the Options Fraud and the Short Sale Fraud, including losses from the account of B.Z., a resident of Monmouth County, New Jersey.

---

<sup>1</sup>Based on my training and experience, I am aware that a short sale is a sale of stock that an investor does not own, but rather borrows from a stock lender and must eventually return. To close out a short position that results from borrowing a stock, an investor purchases replacement shares on the open market and returns those shares to the stock lender within an agreed upon amount of time. Investors who sell stock short are betting that the price of the stock will fall and that they will be able to profit by replacing the shares that they have borrowed and sold at one price with shares purchased at a lower price.

### The TSS Account

4. On or about August 30, 2011, a TSS Account in the name of Dmitry Tokar (“the Tokar Account”) was funded with a \$5,000 check drawn on a Wells Fargo account in the name of M.Z.

5. According to information provided by Wells Fargo officials, the physical check that funded the Tokar Account bore the name “Dmitry Tokar” in the upper-left hand corner despite the fact the check was drawn on M.Z.’s account. Based on my training and experience investigating financial crimes, the use of a fraudulent check to fund a securities account is one indication of fraudulent use of that account.

6. On or about September 6, 2011, defendant Murmylyuk placed a telephone call to TSS and identified himself as Dmitry Tokar.<sup>2</sup> On the call, which TSS recorded, defendant Murmylyuk asked whether the \$5,000 check deposited to open the Tokar Account had cleared. Defendant Murmylyuk also stated that the e-mail account associated with the Tokar Account was denisbofa@[provider].com.

7. On or about September 9, 2011, securities trading began in the Tokar Account. Over the next approximately two months, the Tokar Account was used to conduct approximately 55 trades. The vast majority of these trades were consistent with the Short Sale Fraud described above.

8. Interviews with officials from Scottrade revealed that the counterparties to the fraudulent trading in the Tokar Account in September and October 2011 were either customers of Scottrade whose accounts had been compromised through unauthorized access or were trading accounts opened in the names of identity theft victims.

9. For example, on or about October 14, 2011 at approximately 9:04 a.m. (Eastern Time), the TSS account was used to short sell approximately 3,000 shares of the security AROW at the offered price of \$23.97. Based on industry records, AROW traded no higher than \$23.08 on that day. Based on my training and experience investigating securities frauds, there is no reason for a legitimate customer to purchase shares at an offering price higher than the market price.

10. Minutes after selling these shares, at approximately 9:08 a.m. (Eastern Time), the TSS Account covered its short position by purchasing 3,000 shares at \$21.72, realizing a profit of

---

<sup>2</sup>The voice on the September 6, 2011 call to TSS, based on my training and experience and that of other Russian speaking law enforcement personnel who have listened to the call, is similar to defendant Murmylyuk’s voice on recorded calls, obtained during the investigation, known to have been placed by defendant Murmylyuk.

more than approximately \$6,000 on a proposed trade that, based on my training and experience, no rational investor would agree to.

11. On or after October 14, 2011, TSS, in the ordinary course of its business, addressed an e-mail to Dmitry Tokar at the e-mail address denisbofa@[provider1].com (“the Tokar E-Mail”). In the Tokar E-Mail, TSS confirmed trading activity on the Tokar Account on October 14, 2011.

12. Between on or about October 6, 2011 and on or about October 20, 2011, the TSS Account was used to attempt to wire approximately \$40,000 to accounts for the benefit of Dmitry Tokar at the Russian bank Alfa Bank.

13. On or about November 1, 2011, Scottrade officials learned that the Hackers had gained unauthorized access to the brokerage accounts of C.L., J.D., L.R., and that C.L.’s account was forced to execute unauthorized trades of the securities BIOD and ARNA with the Tokar Account. The trades followed the pattern of the Options Fraud — the illogical sale and immediate re-purchase of options contracts in thinly traded equities. Scottrade suffered an approximately \$143,000 loss due to the November 1 trades on the account of C.L. benefitting the Tokar Account, which Scottrade officials stated was nearly the entire cash balance of C.L.’s trading account.

#### Defendant Murmylyuk’s Arrest

14. On or about November 3, 2011, defendant Murmylyuk was arrested in Brooklyn, New York on state fraud charges.

15. At the time of his arrest, defendant Murmylyuk possessed a Toshiba laptop that law enforcement personnel had seen him purchase at a Best Buy in Brooklyn, New York on or about September 26, 2011 (“the Murmylyuk Laptop”).

16. Forensic review of the Murmylyuk Laptop revealed the following evidence that connects defendant Murmylyuk to the commission of the Short Sale Fraud and the Options Fraud:

a. the e-mail address for M.Z., whose bank account funded the Tokar Account with a fraudulent \$5,000 check;

b. the text of the Tokar E-Mail sent to denisbofa@[provider1].com confirming trading activity on the TSS Account, which from training and experience I know means that the Tokar E-Mail was reviewed on the Murmylyuk Laptop;

c. the names, addresses, Social Security Numbers, e-mail addresses, and telephone numbers of approximately three of the counterparties to the fraudulent securities trading in the Tokar Account in September and October 2011;

d. approximately 130 references to the e-mail address rsev777@open.by, which was the e-mail address associated with a Victim Account at Scottrade in the name J.D. ("the J.D. Scottrade Account"). The J.D. Scottrade Account traded the stock LKSN with the Tokar Account on or about September 20, 2011 in connection with the Short Sale Fraud resulting in losses of approximately \$4,500 to Scottrade.

e. evidence that the Murmylyuk Laptop had been used to connect to Alfa Bank, the destination for the October 2011 wire transfers out of the Tokar Account;

f. evidence that sometime between its purchase in late September 2011 and on or about November 3, 2011, the Murmylyuk Computer was used to visit Internet pages belonging to both OptionsHouse and TSS, including seven visits to TSS websites on or about October 17, 2011.

g. an e-mail address used by Galina Korelina, who had opened Mule Accounts at the direction of CC1;

h. bank account numbers, online usernames, and passwords that CC1 had e-mailed to D.Z., who had opened Mule Accounts at the direction of CC1, in or about August 2011;

i. approximately 10 references to the e-mail address Alex\_Alex@mail.by, which was used to: (1) send confirmation of a plane reservation for travel for D.Z. in or about August 2010.; (2) open three securities accounts at Schwab, one of which was registered to defendant Murmylyuk's apartment building, in or about April 2011; and (3) take over the Fidelity brokerage account of O.M. on or about June 2, 2011;

j. approximately 22 references to the e-mail address alltravel@open.by, which was used to open a securities Victim Account in the name of J.M. at Schwab in or about April 2011;

k. evidence that on or about October 25, 2011, in a span of approximately 30 seconds, the Murmylyuk Laptop had connected to the Internet domains mail.by, open.by, and gemius.pl ("the Suspect Domains"). The Hackers visited the same three Suspect Domains from a compromised computer in Texas in an attempt to open a Profit Account in the name of J.A. at Options House on or about May 12, 2011.

17. According to representatives at Bank of America interviewed during the course of the investigation, on or about September 18, 2011, a single computer connecting to Bank of

America's computer network accessed: (1) an online bank account in the true name of defendant Murmylyuk; (2) an online bank account with the username denisbofa — the same name associated with the TSS Account's registered e-mail; and (3) an account with the online user name that matched the first name of M.Z.