UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	
	:	Hon. Cathy L. Waldor
v.	:	
	:	Mag. No. 13-6089
OLEKSIY SHARAPKA,	:	
LEONID YANOVITSKY,	:	AMENDED CRIMINAL COMPLAINT
a/k/a "Lenny,"	:	
ROBERT DUBUC,	:	
LAMAR TAYLOR, and	:	
ANDREY YARMOLITSKIY	:	

I, Jeremiah Reppert, 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 United States Secret Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Jeremiah Reppert, Special Agent
United States Secret Service

Sworn to before me, and
subscribed in my presence

June 13, 2013 at
Newark, New Jersey

HONORABLE CATHY L. WALDOR
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

Count One
(Wire Fraud Conspiracy)

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, defendants

OLEKSIY SHARAPKA,
LEONID YANOVITSKY,
a/k/a "Lenny,"
RICHARD GUNDERSEN,
ROBERT DUBUC,
LAMAR TAYLOR, and
ANDREY YARMOLITSKIY

did knowingly and intentionally conspire and agree with each other, and with others known and unknown, to devise a scheme and artifice to defraud ADP, Inc., Fundtech, Inc., J.P. Morgan Chase Bank, and their customers, as well as others, and to obtain money and property from ADP, Inc., Fundtech, Inc., J.P. Morgan Chase Bank, and their customers, as well as others, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing this scheme and artifice to defraud, 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.

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

Count Two
(Money Laundering Conspiracy)

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, defendants

OLEKSIY SHARAPKA,
LEONID YANOVITSKY,
a/k/a "Lenny,"
RICHARD GUNDERSEN,
ROBERT DUBUC,
LAMAR TAYLOR, and
ANDREY YARMOLITSKIY

willfully and knowingly conspired and agreed with each other, and with others known and unknown, to commit certain offenses under Title 18, United States Code, Section 1956, in that they conducted and attempted to conduct financial transactions affecting interstate commerce,

which transactions involved the proceeds of specified unlawful activity, that is, conspiracy to commit wire fraud in violation of Title 18, United States Code, Section 1349, and wire fraud in violation of Title 18, United States Code, Section 1343: (1) with the intent to promote the carrying on of such specified unlawful activity; and (2) knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership,

and control of the proceeds of said specified unlawful activity, and while conducting and attempting to conduct such financial transactions knew the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Section 1956(h), and Title 18, United States Code, Section 2.

Count Three
(Conspiracy to Commit Identity Theft)

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, defendants

OLEKSIY SHARAPKA,
LEONID YANOVITSKY,
a/k/a "Lenny,"
RICHARD GUNDERSEN,
ROBERT DUBUC,
LAMAR TAYLOR, and
ANDREY YARMOLITSKIY

did knowingly and intentionally conspire and agree with each other, and with others known and unknown, to transfer, possess and use means of identification of other persons without lawful authority, in a manner affecting interstate and foreign commerce, with the intent to commit, and in connection with, unlawful activity constituting a violation of Federal law, namely, Title18, United States Code, Section 1349, contrary to Title 18, United States Code, Section 1028(a)(7).

In violation of Title 18, United States Code, Sections 1028(f) and 1028(b).

ATTACHMENT B

I, Jeremiah Reppert, a Special Agent with the United States Secret Service ("USSS"), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. In addition, a number of e-mails discussed herein were in Russian and/or Ukranian; to the extent translations are used in this affidavit, they are based on preliminary drafts.

Overview of the Scheme

1. The USSS, Department of Homeland Security – Homeland Security Investigations, Internal Revenue Service – Criminal Investigation, and the Department of Defense – Defense Criminal Investigative Service, are investigating an international computer hacking and identity theft scheme that has targeted over a dozen government agencies, payroll processing companies and financial institutions (collectively, the "Victim Companies") located throughout the United States. Pursuant to the scheme, hackers first compromise account credentials of the Victim Companies' customers through various means. They then gain unauthorized access to the accounts of the Victim Companies' customers. Next, the hackers divert money from those accounts to bank accounts and pre-paid debit cards opened in the names of identity theft victims, many of which were controlled by defendant OLEKSIY SHARAPKA. Defendant SHARAPKA, in turn, directs managers in the United States, who run local "cashing" crews of individuals (known as "cashers" or "cashiers"), to "cash out" the fraudulently funded bank accounts and pre-paid debit cards by, among other things, conducting Automated Teller Machines ("ATM") withdrawals and fraudulent purchases. In addition to the Victim Companies, SHARAPKA and his co-conspirators submitted fraudulent tax returns to the Internal Revenue Service ("IRS") claiming refunds, and directed those refunds to accounts they controlled, and cashed out those accounts in the same manner. The majority of the proceeds of these cash out operations flow up from the cashers to their managers, and then to the higher levels of the operation; the cashers often transfer the funds via international wire transfer services as Western Union and MoneyGram, among other methods. To date, defendant SHARAPKA and his co-conspirators have attempted to defraud the Victim Companies and their customers of in excess of approximately $15 million.

Relevant Parties and Individuals

2. At all times relevant to this Complaint:

a. Defendant OLEKSIY SHARAPKA was a resident of Kiev, Ukraine, and the head of the "Sharapka Cash Out Organization" described herein. From in or about November 2004 through in or about March 2012, defendant SHARAPKA was in federal custody in the District of Massachusetts, serving a 102-month federal sentence based upon his guilty plea to mail fraud, access device fraud, and aggravated identity theft charges. Those charges related to defendant SHARAPKA's participation in a scheme pursuant to which defendant SHARAPKA

and his co-conspirators used stolen bank account numbers and identity information to create bank cards, and then withdrew money from those stolen bank accounts using ATMs. In or about March 2012, defendant SHARAPKA was deported from the United States to Ukraine upon completion of his federal sentence.

b. Defendant LEONID YANOVITSKY, a/k/a "Lenny," was a resident of Kiev, Ukraine, and assisted defendant SHARAPKA in managing the Sharapka Cash Out Organization by, among other things, tracking bank accounts and pre-paid debit cards used by the organization and receiving overseas wires from managers of cash out crews in the United States.

c. Defendant OLEG PIDTERGERYA was a resident of Brooklyn, New York, who managed a cash out crew in the New York area for the Sharapka Cash Out Organization.

d. Defendant RICHARD GUNDERSEN was a resident of Brooklyn, New York, who worked as a casher under defendant PIDTERGERYA's supervision.

e. Defendant ROBERT DUBUC was a resident of Malden, Massachusetts, who managed a cash out crew in Massachusetts for the Sharapka Cash Out Organization.

f. Defendant LAMAR TAYLOR was a resident of Salem, Massachusetts, who worked as a casher under defendant DUBUC's supervision.

g. Defendant ANDREY YARMOLITSKIY was a resident of Atlanta, Georgia, who operated a cash out crew in Georgia for the Sharapka Cash Out Organization.

h. Defendant ILYA OSTAPYUK was a resident of Brooklyn, New York, who facilitated the movement of fraud proceeds for the Sharapka Cash Out Organization.

i. Co-conspirator "A.S.," not named as a defendant herein, was a resident of the Ukraine, who assisted defendant SHARAPKA in managing the Sharapka Cash Out Organization by, among other things, tracking bank accounts and pre-paid debit cards used by the organization.

j. Co-conspirator "V.K.," not named as a defendant herein, was a resident of Ukraine, who facilitated the movement of fraud proceeds for the Sharapka Cash Out Organization.

k. From at least as early as in or about March 2012 through in or about June 2013, the Sharapka Cash Out Organization targeted the IRS, and over a dozen banks, retail brokerage firms, financial service companies, accounting firms, and payroll processing companies, including the following entities and their customers, among others:

i. Aon Hewitt;

ii. Automatic Data Processing, Inc. ("ADP");

iii. Citibank, N.A.;

iv. E-Trade;

v. Electronic Payments, Inc.;

vi. Fundtech Holdings LLC ("Fundtech");

vii. iPayment, Inc.;

viii. JP Morgan Chase Bank, N.A. ("Chase");

ix. Nordstrom Bank;

x. PayPal;

xi. TD Ameritrade;

xii. The United States Department of Defense, Defense Finance and Accounting Service;

xiii. TIAA-CREF;

xiv. USAA; and

xv. Veracity Payment Solutions, Inc.

3. At all times relevant to this Complaint:

a. ADP was headquartered in New Jersey, and was one of the world's largest providers of outsourcing solutions for human resources, payroll, and tax administration services. ADP offered 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 a legitimate username and password, 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 employees could receive payroll through ADP was by transferring their payroll onto pre-paid debit cards.

b. Fundtech was headquartered in New Jersey, and offered, among other things, an online bill payment system called "Modern Payments." Modern Payments not only enabled its users to collect bill payments online, it also handled the issuance of refunds or rebates to customers. Municipalities such as the City of Evans, Colorado (the "City of Evans") used the Modern Payments platform to collect utilities payments, and to handle refunds for utilities overpayments, as well as to issue rebates to customers.

c. Chase Bank was a financial institution headquartered in New York that, among other things, provided personal banking services to its customers. One of the features that Chase Bank provided its customers was online access to their personal banking accounts.

Probable Cause

A. Fraudulent Transfers from the Payroll Accounts of ADP Clients

4. From in or about October 2011 through in or about June 2013, hackers first obtained the account log-in credentials (*e.g.*, usernames and passwords) of ADP customers from the customers themselves using a variety of unlawful means. Next, the hackers used those fraudulently obtained account log-in credentials to access the customers' accounts, which were hosted on ADP computer servers, located in New Jersey, Georgia and South Dakota. Using this method, the hackers gained control of the accounts of over 130 ADP customers. Thereafter, the hackers attempted to divert approximately $4 million from those accounts by attempting to transfer money from those accounts to accounts they controlled, including numerous transfers from in or about March 2012 through in or about April 2012 to pre-paid debit cards held in the name of defendant SHARAPKA (the "Sharapka Debit Cards").

5. Defendant SHARAPKA listed the following e-mail address on several applications for the Sharapka Debit Cards: artistaga@gmail.com (the "Artistaga Gmail Account"), registered to "Oleksiy Sharapka" and "Sharapka Internet Services, Inc." at an address on Ocean Parkway in Brooklyn, New York (the "Ocean Parkway Address"). The Ocean Parkway Address is defendant PIDTERGERYA's apartment. On or about December 18, 2012, United States Magistrate Judge Cathy L. Waldor authorized the issuance of a search warrant for the Artistaga Gmail Account based upon evidence indicating that the owner of these email accounts used them in furtherance of conspiracy described herein.

6. A review of the contents of the Aristaga Gmail Account revealed that it was being used by defendant SHARAPKA to direct the conspiracy described herein, and that it contained hundreds of e-mail messages between defendant SHARAPKA and co-conspirators PIDTERGERYA, YANOVITSKY, and DUBUC, discussing, among other things, access device fraud, bank fraud, wire fraud, identity theft, and money laundering. Among others, I reviewed an e-mail from defendant SHARAPKA to defendant YANOVITSKY dated on or about September 6, 2012 forwarding a Microsoft Excel spreadsheet containing a list of over 300 pre-paid debit cards in the names of other individuals, including known identity theft victims, being used by the Sharapka Cash Out Organization to receive fraudulent transfers from the Victim Companies. The name "oleg," which I believe to be a reference to defendant PIDTERGERYA appeared next to approximately 60 of these cards, including a pre-paid debit card ending in 2123 in the name of "A.S." (the "A.S. 2123 Card"). The name "bob," which I believe to be a reference to defendant ROBERT DUBUC appeared next to approximately 28 of these cards, including a pre-paid debit card ending in 3027 in the name of "N.C.," a known identity theft victim (the "N.C. 3027 Card"), without his authorization and consent.

The A.S. 2123 Card and the Attempted Fraudulent Transfer from ADP Customer B&S

7. For example, in or about June 2012, defendant SHARAPKA and his co-conspirators attempted to transfer funds belonging to ADP customer "B&S" to the A.S. 2123 Card. Although ADP was able to prevent this fraudulent transfer, defendant SHARAPKA and his co-conspirators were able to fraudulently transfer funds to that card on or about July 6, 2012 and on or about July 7, 2012, from other Victim Companies. Subsequently, according to bank

and ATM surveillance footage that I reviewed, 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.

The N.C. 3027 Card and the Attempted Fraudulent Transfer from ADP Customer B&S

8. In addition, in or about June 2012, defendant SHARAPKA and his co-conspirators attempted to transfer funds belonging to ADP customer B&S to the N.C. 3027 Card, by adding the information for the N.C. 3027 Card to B&S's payroll account with ADP. ADP was also able to prevent this fraudulent transfer. Prior to the attempted transfer, however, on or about May 7, 2012, defendant SHARAPKA e-mailed defendant DUBUC, and stated: "You can do the same thing with the rest of the regular cards, so I can activate them and start giving them to guys to put money on, because we are losing time again... Just write me the following: 1. Brand (like: readydebit, rushcard, bank freedom, *etc.*), name on the card, card number, exp, cvv2 code, phone for activation. thanks." In response, on or about May 10, 2012, defendant DUBUC e-mailed defendant SHARAPKA the requested information, including information related to the N.C. 3027 Card. While the fraudulent transfer from ADP customer B&S was stopped, the N.C. 3027 Card received a fraudulent electronic funds transfer from another Victim Company on or about July 6, 2012, which was reversed by the Victim Company on or about July 10, 2012.

The A.S. 5731 Card and Fraudulent Transfers from ADP Customer H.A.C.

9. From between in or about April 18, 2012 and in or about April 20, 2012, the Sharapka Cash Out Organization attempted to fraudulently transfer money from the account of ADP customer "H.A.C." On or about April 20, 2012, an American Express pre-paid debit card in the name of defendant SHARAPKA received a fraudulent funds transfer from ADP customer H.A.C. Defendant SHARAPKA and his co-conspirators also attempted to transfer funds from H.A.C. to a pre-paid debit card ending in 5731 opened in the name of "A.S." (the "A.S. 5731 Card"). ADP, however, was able to prevent that fraudulent transfer.

10. The A.S. 5731 Card, however, has been used by the Sharapka Cash Out Organization on several other occasions to receive fraudulent transfers from Victim Companies. For example, on or about June 27, 2012, defendant SHARAPKA e-mailed defendant PIDTERGERYA information concerning the A.S. 5731 Card. On or about June 27, 2012, the 5731 Card received a fraudulent IRS tax refund in the name of an identity theft victim.

11. According to bank and ATM surveillance footage that I reviewed, on or about June 27, 2012, defendants PIDTERGERYA and GUNDERSEN used the A.S. 5731 Card at a bank in Brooklyn, New York to withdraw money fraudulently received from an IRS tax refund.

B. Fraudulent Transfers from Fundtech Customers

12. 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 bank accounts and pre-paid debit cards 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") by defendant GUNDERSEN using a fraudulent Ohio driver's license in the name of "S.C." In fact, on or about May 15, 2012, defendant SHARAPKA received an e-mail with the subject "Ritchie" – a reference to defendant GUNDERSEN's first name, and containing the same photograph of defendant GUNDERSEN used in the fraudulent Ohio S.C. driver's license.

13. On or about November 6, 2012, defendant SHARAPKA e-mailed defendant PIDTERGERYA the information for the A.C.C. 8175 Account, including the full account number. Subsequently, on or about December 9, 2012, defendant PIDTERGERYA conducted an ATM transaction in Mount Pocono, Pennsylvania using the A.C.C. 8175 Account and withdrawing money fraudulently transferred to the account from the City of Evans, a Fundtech customer.

14. Thereafter, on or about December 4, 2012, defendant 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"). Among other things, the instructions stated that there would be transfers into the M.L. 6409 Account from "Modern Payments." I have reviewed ATM and bank surveillance photos of defendant TAYLOR attempting to access the M.L. 6409 Account, which had received fraudulent transfers from the City of Evans, on multiple occasions, including at a bank in Beverly, Massachusetts on or about December 12, 2012.

15. In addition, I have reviewed ATM and bank surveillance photos of defendant TAYLOR from on or about December 13, 2012 making and attempting to make cash withdrawals using a pre-paid debit card ending in 9415 in the name of "S.B." (the "S.B. 9415 Card") and a pre-paid debit card ending in 2445 in the name of "J.M." (the "J.M. 2445 Card") from an ATM in Malden, Massachusetts. Both the S.B 9415 Card and the J.M. 2445 Card received fraudulent electronic rebates from the City of Evans through Fundtech's Modern Payments platform. In addition, both the S.B 9415 Card and the J.M. 2445 Card were listed in the spreadsheet defendant YANOVITSKY e-mailed defendant SHARAPKA on or about September 6, 2012, which is described in paragraph 6 above.

C. Fraudulent Transfers from Chase Bank Accounts

16. Between in or about October 2012 and in or about April 2013, law enforcement learned that hackers had first obtained the account log-in credentials (*e.g.*, usernames and passwords) of Chase Bank customers using a variety of unlawful means. Next, the hackers used those fraudulently obtained account log-in credentials to gain unauthorized access to personal bank accounts of numerous Chase Bank customers. After gaining access, hackers transferred funds from these accounts to multiple pre-paid American Express debit cards controlled by the Sharapka Cash Out Organization. To date, Chase Bank has identified approximately 40 customer accounts that were compromised in this fashion, and that the Sharapka Cash Out Organization attempted to steal approximately $60,000 from Chase customers' accounts in this manner.

17. I have reviewed multiple e-mails between defendant SHARAPKA and defendant PIDTERGERYA in which they exchanged, among other things, information related to pre-paid American Express 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"). For example, on or about February 18, 2013, defendant SHARAPKA e-mailed defendant PIDTERGERYA information related to approximately 11 Fraudulent AMEX Pre-paid Cards, including one in the name of "R.M." (the "R.M. Amex Card"). I have reviewed ATM surveillance photos of defendant PIDTERGERYA from on or about February 20, 2013, making 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.

18. On or about October 18, 2012, defendant YANOVITSKY forwarded defendant SHARAPKA an email from co-conspirator A.S., not named as a defendant herein, in which co-conspirator A.S. wrote, in sum and substance, that his cousin was worried about sending money via Moneygram, and included the Suspicious Activity Reporting instructions used by money transfer services. Based on the investigation to date, I believe that the cousin referenced in this e-mail is defendant YARMOLITSKIY.

19. Thereafter, on or about November 29, 2012, defendant YANOVITSKY e-mailed defendant SHARAPKA a photograph of defendant YARMOLITSKIY; the subject of the e-mail was "picture for id." Based on my investigation, I know that members of the Sharapka Cash Out Organization exchanged such photographs to prepare fraudulent identification to be used to facilitate the cash outs of fraudulent pre-paid debit cards in the names of others, such as the Fraudulent AMEX Pre-paid Cards discussed above.

20. I have reviewed multiple e-mails sent by defendant YANOVITSKY to an e-mail address believed to be controlled by co-conspirator A.S., including a spreadsheet similar to the one described in paragraph 6, containing, among other things, information related to pre-paid American Express debit cards opened in the names of others, including confirmed identity theft victims, that were used to receive fraudulent electronic funds transfers from Chase Bank victims. I have also reviewed ATM surveillance photographs of defendant YARMOLITSKIY making and attempting to make multiple cash withdrawals using these fraudulently funded pre-paid American Express debit cards in the names of others, on at least the following dates at the below locations:

a. On or about November 19, 2012, at an ATM located in Chamblee, Georgia;

b. On or about December 17, 2012, at an ATM located in Norcross, Georgia;

c. On or about December 19, 2012, at an ATM located in Chamblee, Georgia; and

d. On or about January 17, 2013, at an ATM located in Duluth, Georgia.

D. Fraudulent IRS Refunds

21. From between in or about March 2012 through in or about September 2012, defendant SHARAPKA and his co-conspirators caused fraudulent tax returns claiming refunds to be submitted to the IRS in the names of identity theft victims. The tax refunds were directed to bank accounts and pre-paid debit cards controlled by the Sharapka Cash Out Organization.

22. For example, the spreadsheet that defendant YANOVITSKY e-mailed to defendant SHARAPKA on or about September 6, 2012 (discussed above in paragraph 6) contained pre-paid debit card information related to cards that, among other things, received fraudulent IRS tax refunds. For example, a pre-paid debit card ending in 7786 in the name of "S.T.," a pre-paid debit card ending in 7505 in the name of "N.C.," and a pre-paid debit card ending in 9410 in the name of "S.B." all received fraudulent IRS tax refunds between in or about June 2012 and in or about August 2012.

23. As another example, on or about May 30, 2012, defendant GUNDERSEN 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 defendant GUNDERSEN's photo. 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.

24. I have reviewed bank and ATM surveillance photographs of defendants PIDTERGERYA and GUNDERSEN making and attempting to make multiple cash withdrawals from the R.M. 3889 Account on the following dates at the below locations, among others:

a. Defendant PIDTERGERYA: on or about June 6, 2012, at a bank located in Brooklyn, New York;

b. Defendant PIDTERGERYA: on or about June 6, 2012, at an ATM located in Brooklyn, New York;

c. Defendant GUNDERSEN: on or about June 7, 2012, at a bank located in Brooklyn, New York;

d. Defendant PIDTERGERYA: on or about June 8, 2012, at an ATM located in Brooklyn, New York; and,

e. Defendant GUNDERSEN: on or about June 27, 2012, at a bank branch located in Brooklyn, New York, at or about the same time of the event described in paragraph 11 above.

25. In addition, I have reviewed e-mails between defendants SHARAPKA and PIDTERGERYA discussing, among other things, fraudulent accounts opened in the name of R.M. For example, on or about July 5, 2012, defendant SHARAPKA e-mailed defendant PIDTERGERYA a list of bank accounts that included the R.M. 3889 Account.

E. The Proceeds of the Fraud

26. The Sharapka Cash Out Organization has used a variety of means to launder the proceeds of the fraudulent activity described above, and transfer the proceeds of the fraud overseas.

Direct Overseas Transfers

27. For example, I have reviewed financial records showing that on multiple occasions throughout 2012, defendants PIDTERGERYA, DUBUC, and TAYLOR wired money directly to defendant SHARAPKA in the Ukraine, or directed others to do the same. For example:

a. On or about May 5, 2012, defendant PIDTERGERYA, using his own name, sent approximately $740 from a Duane Reade in Brooklyn, New York to defendant SHARAPKA in Kiev, Ukraine using Moneygram.

b. On or about June 26, 2012, defendant DUBUC, using his own name, sent approximately $2,000 from a convenience store in Malden, Massachusetts to defendant SHARAPKA in Kiev, Ukraine using Moneygram.

c. On or about August 13, 2012, defendant TAYLOR, using the name "N.C.," sent approximately $2,000 from a convenience store in Salem, Massachusetts to defendant SHARAPKA in Kiev, Ukraine using Moneygram.

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

28. In addition, defendant SHARAPKA directed members of the Sharapka Cash Out Organization to move the fraud proceeds through bank accounts controlled by defendant ILYA OSTAPYUK and co-conspirator V.K. and held in the names of Mirku Inc. and Kumir Inc.: the "Mirku 0414 Account" and the "Kumir 0443 Account."

29. Specifically, on or about October 4, 2012, defendant SHARAPKA e-mailed defendant PIDTERGERYA the account information for the Mirku 0414 Account and the Kumir 0443 Account, and wrote: "Here is one more account... As you know, I can't use my HSBC anymore. Therefore, we need to use their transfer routes as much as we can, since it is still possible. Because after that we will need to sit and wait for another [chance]." The e-mail also contained an excerpt from an online chat between defendant SHARAPKA and co-conspirator V.K., in which defendant SHARAPKA informed V.K. that "Oleg" would make $9,900 deposits into the Mirku 0414 Account and the Kumir 0443 Account.

30. Subsequently, on or about October 9, 2012, defendant SHARAPKA e-mailed defendant PIDTERGERYA a screenshot containing details of the Kumir 0443 Account. In the body of the e-mail, defendant SHARAPKA wrote: "That V[] sent me screenshot of his account.... this is a business account and you may deposit there as much as you want without any problem. We had to open a full-fledged corporation for our needs a long time ago, and won't be bound up with it, deposited money there and wired it." On or about October 10, 2012, defendant SHARAPKA e-mailed defendant DUBUC the same screenshot.

31. In another e-mail dated on or about December 17, 2012, defendant SHARAPKA gave defendant PIDTERGERYA a record confirming deposits – each slightly under $10,000 – that had been made over the previous weeks into the Mirku 0414 Account and the Kumir 0443 Account. For example, based on a review of bank records and bank surveillance photographs, I have learned the following:

a. 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 (as discussed in paragraphs 12 through 15 above).

b. Thereafter, defendant PIDTERGERYA and others made a number of cash deposits into the Mirku 0414 Account and the Kumir 0443 Account matching the dates and amounts listed in defendant SHARAPKA's December 17th e-mail. Indeed, I have reviewed bank surveillance photographs showing defendant PIDTERGERYA's girlfriend depositing approximately $9,990 in cash and money orders on or about December 12, 2012, into the Mirku 0414 Account at a bank located in Brooklyn, New York.

c. I have also reviewed bank surveillance photographs showing defendant PIDTERGERYA depositing approximately $9,900 in cash and money orders into the Kumir 0443 Account at bank in Brooklyn, New York – exactly as recorded by defendant SHARAPKA in his e-mail.

32. In summary, I have learned the following concerning the Mirku 0414 Account and the Kumir 0443 Accounts:

a. 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. Bank surveillance photographs confirm that defendants PIDTERGERYA, DUBUC, and YARMOLITSKIY made a number of the cash deposits into the Mirku 0414 Account. After being deposited in the account, the funds were moved or wired to other accounts.

b. Between in or about June 2012 and in or about March 2013, 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. Bank surveillance photographs confirm that defendants PIDTERGERYA, DUBUC, and YARMOLITSKIY made a number of the cash deposits into Kumir 0443 Account. After being deposited in the account, the funds were moved or wired to other accounts.