

BØ11

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

UNITED STATES OF AMERICA

v.

NIKA NAZAROV

a/k/a Nika Utiashvili
a/k/a Mihail Atansov
a/k/a Stefan Trifonov Zhelyazkov

MARTINS IGNATJEVS

a/k/a Yordan Angelov Stoyanov
a/k/a Aleksander Tihomirov
a/k/a Svetlin Iliyanov Asenov

ALEKSANDRE KOBASHVILI

a/k/a Antonios Nastas
a/k/a Ognyan Krasimirov Trifonov

DMITRIJS KUZMINOV

a/k/a Parush Gospodinov Genchev

VALENTINS SEVECS

a/k/a Marek Jaswilko
a/k/a Rafal Szczytko

DMITRIJS SLAPINS

ARMENS VECELS

ARTIOM CAPACLI

ION CEBANU

TOMASS TRECINKAS

RUSLANS SARAPOVS

SILVESTRS TAMENIEKS

ABDELHAK HAMDAOUI

PETAR ILIEV

Criminal No. 20-295
(18 U.S.C. § 1956(h))
[UNDER SEAL]

FILED

SEP 29 2020

CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

The grand jury charges:

Introduction

At all times material to this Indictment:

1. From in and around 2016, and continuing thereafter to in and around October 2019, the Defendants, and co-conspirators known and unknown to the grand jury, were members of a transnational organized crime network known as “QQAAZZ.” QQAAZZ provided money laundering services to significant cybercriminal organizations that stole money from unwitting victims in the United States and abroad.

2. In order to launder stolen funds, the Defendants and their co-conspirators opened and maintained hundreds of bank accounts at financial institutions in numerous countries, including Portugal, Spain, Germany, Turkey, the United Kingdom, Belgium and the Netherlands. QQAAZZ used the bank accounts to receive funds stolen by cybercriminals from victims and their respective financial institutions, including in the Western District of Pennsylvania.

3. After receiving the stolen funds, QQAAZZ transferred the funds through a complex series of transactions. These transactions included traditional electronic funds transfers to other QQAAZZ-controlled bank accounts as well as the conversion of the stolen funds to cryptocurrency. After taking a fee of up to 40 to 50-percent, QQAAZZ returned the balance of the stolen funds to the cybercriminals. In total, cybercriminals attempted to transfer tens of millions of dollars to QQAAZZ-controlled accounts, and QQAAZZ successfully laundered millions of dollars stolen from victims around the world.

Members of the Conspiracy

4. The members of QQAAZZ were citizens of multiple countries, including Georgia, Latvia, Romania, Bulgaria, and Belgium.

5. QQAAZZ was organized into a hierarchy with three primary levels: leaders, mid-level managers, and money couriers, oftentimes known as “money mules” and described as such herein.

6. The leaders of QQAAZZ directed mid-level managers, developed strategies for opening bank accounts around the world, advertised “cash-out” services on cybercriminal internet forums, and coordinated to receive stolen funds from and return laundered funds to cybercriminals. The phrase “cash-out services” refers to the ability to withdraw funds in currency from a bank account.

7. Mid-level managers of QQAAZZ received direction from the organization’s leaders, recruited money mules to open bank accounts around the world, and arranged travel for the money mules. Sometimes mid-level members of the conspiracy also opened QQAAZZ-controlled bank accounts.

8. Money mules at times used aliases and false identification documents, and at other times used their true identities, to register shell companies¹ and open personal and corporate bank accounts controlled by QQAAZZ at international financial institutions. The primary purpose of the accounts was to receive and launder stolen funds. The money mules were complicit in the scheme, meaning that they were aware of the illegal source of victim funds.

¹ As used herein, a “shell company” is a corporate entity formed under the laws of a jurisdiction outside of the United States for the purpose of opening bank accounts. A shell company does not have an actual business function outside of being the named owner of these bank accounts.

The Defendants

9. NIKA NAZAROV, formerly Nika Utiashvili, a/k/a Mihail Atanasov, a/k/a Stefan Trifonov Zhelyazkov, was a citizen of Georgia. NAZAROV was a member of the conspiracy who managed co-conspirators in the opening of QQAAZZ-controlled bank accounts. NAZAROV used the alias Stefan Trifonov Zhelyazkov to register a shell company in Spain and open a QQAAZZ-controlled bank account, which was the intended recipient of funds attempted to be stolen from two United States victims.

10. MARTINS IGNATJEVS, a/k/a Yodan Angelov Stoyanov, a/k/a Aleksander Tihomirov Yanev, a/k/a Svetlin Iliyanov Asenov, was a citizen of Latvia, and he resided in the United Kingdom. IGNATJEVS was a member of the conspiracy who managed co-conspirators in the opening of QQAAZZ-controlled bank accounts.

11. ALEKSANDRE KOBIASHVILI, a/k/a Antonios Nastas, a/k/a Ognyan Krasimirov Trifonov, was a citizen of Georgia. KOBIASHVILI used the aliases Antonios Nastas and Ognyan Krasimirov Trifonov to register a shell company and open QQAAZZ-controlled bank accounts in Portugal. One of the QQAAZZ-controlled bank accounts opened by KOBIASHVILI was the intended recipient of funds attempted to be stolen from a United States victim.

12. DMITRIJS KUZMINOV, a/k/a Parush Gospodinov Genchev was a citizen of Latvia. KUZMINOV registered shell companies and opened QQAAZZ-controlled bank accounts in Portugal and Germany. One of the accounts opened in Portugal was the recipient of funds stolen from a United States victim.

13. VALENTINS SEVECS, a/k/a Marek Jaswilko, a/k/a Rafal Szczytko, was a citizen of Latvia. SEVECS used the alias Marek Jaswilko to register a shell company in Portugal and open at least 16 QQAAZZ-controlled bank accounts in that company's name. Two of these corporate

bank accounts were the intended recipients of funds attempted to be stolen from three United States victims.

14. DMITRIJS SLAPINS was a citizen of Latvia. SLAPINS's identification was used to register shell companies and QQAAZZ-controlled bank accounts in the United Kingdom and Germany. SLAPINS also opened a personal bank account in Germany that was the intended recipient of funds attempted to be stolen from a United States victim.

15. ARMENS VECELS was a citizen of Latvia. VECELS registered a shell company in Portugal and opened QQAAZZ-controlled bank accounts in Portugal, Spain, and the United Kingdom. The accounts VECELS opened in Portugal were the intended recipient accounts for funds attempted to be stolen from five United States victims.

16. ARTIOM CAPACLI was a citizen of Bulgaria. CAPACLI opened a QQAAZZ-controlled bank account in Spain, which received funds stolen from a United States victim.

17. ION CEBANU was a citizen of Romania. CEBANU opened a QQAAZZ-controlled bank account in Spain, which received funds stolen from a United States victim.

18. TOMASS TRESCINKAS was a citizen of Latvia. TRESCINKAS opened a QQAAZZ-controlled bank account in Spain, which received funds stolen from a United States victim.

19. RUSLANS SARAPOVS was a citizen of Latvia. SARAPOVS opened a QQAAZZ-controlled bank account in Spain, which received funds stolen from a United States victim.

20. SILVESTRS TAMENIEKS was a citizen of Latvia. TAMENIEKS opened a QQAAZZ-controlled bank account in Spain, which received funds stolen from a United States victim.

21. ABDELHAK HAMDAOUI was a citizen of Belgium. HAMDAOUI opened QQAazz-controlled bank accounts in Belgium and Germany. One of the accounts opened by HAMDAOUI received funds stolen from a United States victim.

22. PETAR ILIEV was a citizen of Bulgaria. ILIEV opened a QQAazz-controlled bank account in Portugal which was the intended recipient of funds attempted to be stolen from a United States victim.

**Co-Conspirators Charged
in Related Indictment at Criminal No. 19-304²**

23. Aleksejs Trofimovics, a/k/a Aleksejs Trofimovich, a/k/a Alexey Trofimovich, a/k/a Aleko Stoyanov Angelov, was a citizen of Latvia. Trofimovics registered shell companies and opened QQAazz-controlled bank accounts in Portugal that were the recipients, and intended recipients, of funds stolen and attempted to be stolen from United States victims.

24. Ruslans Nikitenko, a/k/a Krzysztof Wojciech Lewko, a/k/a Milen Nikolchev Nikolov, a/k/a Rafal Zimnoch, a/k/a Emil Raykov Yordanov, was from Latvia. Nikitenko was a member of the conspiracy who managed co-conspirators in the opening of QQAazz-controlled bank accounts. Nikitenko used the aliases Krzysztof Wojciech Lewko, Milen Nikolchev Nikolov, Rafal Zimnoch, and Emil Raykov Yordanov to register shell companies and open QQAazz-controlled bank accounts in Portugal, including accounts that were the recipients, and intended recipients, of funds stolen and attempted to be stolen from United States victims.

25. Arturs Zaharevics, a/k/a Piotr Ginelli, a/k/a Arkadiusz Szuberski, a/k/a Pawel Tomasz Blitek, a/k/a Marcin Ostapowicz, was a citizen of Latvia, and at times he resided in the

² On September 25, 2019, a federal grand jury in the Western District of Pennsylvania returned a one-count indictment at Criminal No. 19-304 charging QQAazz members Aleksejs Trofimovics, Ruslans Nikitenko, Arturs Zaharevics, Deniss Ruseckis, and Deinis Gorenko with conspiracy to commit money laundering, in violation of Title 18, United States Code, Section 1956(h), for their involvement in the same conspiratorial conduct charged herein.

United Kingdom. Zaharevics was a member of the conspiracy who recruited and managed co-conspirators in the opening of QQAazz-controlled bank accounts. Zaharevics used the aliases Piotr Ginelli and Arkadiusz Szuberski to register shell companies and open QQAazz-controlled bank accounts in Portugal.

26. Deniss Ruseckis, a/k/a Denis Rusetsky, a/k/a Sevdelin Sevdalinov Atanasov, was a citizen of Latvia. Ruseckis registered shell companies and opened QQAazz-controlled bank accounts in Portugal that were the recipients, and intended recipients, of funds stolen and attempted to be stolen from United States victims.

27. Deinis Gorenko was a citizen of Latvia. Gorenko opened QQAazz-controlled bank accounts in Portugal that were the recipients of funds stolen from United States victims.

The Victims

28. QQAazz laundered money stolen from victims in the United States and other countries, including the United Kingdom, Switzerland, and Italy. Victims included both businesses and individuals. Some of the victims in the United States held bank accounts at financial institutions headquartered in the Western District of Pennsylvania.

29. Bank 1 was a financial institution headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. Bank 1 was insured by the Federal Deposit Insurance Corporation or chartered by the United States.

30. Bank 2 was a financial institution headquartered in Pittsburgh, Pennsylvania, in the Western District of Pennsylvania. Bank 2 was insured by the Federal Deposit Insurance Corporation or chartered by the United States.

31. Examples of identified victims living or conducting business within the United States included:

- a. a technology company in Windsor, Connecticut;

- b. an Orthodox Jewish Synagogue in Brooklyn, New York;
- c. a medical device manufacturer in York, Pennsylvania;
- d. an individual in Montclair, New Jersey;
- e. an architecture firm in Miami, Florida;
- f. an individual in Acworth, Georgia;
- g. an automotive parts manufacturer in Livonia, Michigan;
- h. a homebuilder in Skokie, Illinois;
- i. an individual in Carrollton, Texas; and,
- j. an individual in Villa Park, California.

32. In total, dozens of United States victims have been identified. However, because QQAAZZ served numerous cybercriminal organizations, the total number of victims whose funds were stolen, or attempted to be stolen, through unauthorized electronic funds transfers is unknown.

COUNT ONE
Conspiracy to Commit Money Laundering
(18 U.S.C. § 1956(h))

The grand jury charges:

33. The allegations contained in Paragraphs 1 through 32 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

34. From in and around 2016, and continuing thereafter to in and around October 2019, in the Western District of Pennsylvania and elsewhere, the Defendants did knowingly and intentionally conspire and agree with each other and other persons known and unknown to the grand jury, to commit money laundering in violation of Title 18, United States Code, Section 1956, that is:

- a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, involving the proceeds of specified unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, wire fraud, in violation of Title 18, United States Code, Section 1343, and bank fraud, in violation of Title 18, United States Code, Section 1344, 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 that while conducting and attempting to conduct such financial transactions knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and

- b. to knowingly transport, transmit, transfer, and attempt to transport, transmit, and transfer monetary instruments and funds from a place in the United States to and through a place outside the United States, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represent the proceeds of some form of unlawful activity, and knowing that such transportation, transmission, and transfer was designed, in whole and in part, to conceal and disguise the nature, location, source, ownership and control of the proceeds of specified unlawful activity, namely, computer fraud, in violation of Title 18, United States Code, Section 1030, wire fraud, in violation of Title 18, United States Code, Section 1343, and bank fraud, in violation of Title 18, United States Code, Section 1344, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i).

Manner and Means of the Conspiracy

35. During all times relevant to the Indictment, the manner and means used to accomplish the conspiracy included the following:

Overview of the Conspiracy

36. QQAazz members at times used aliases and false identification documents, and at other times used their true identities, to register shell companies and open personal and corporate bank accounts controlled by QQAazz at foreign financial institutions.

37. The primary purpose of the bank accounts was to receive money stolen by cybercriminals from unwitting victims in the United States and abroad.

38. In order to attract business from cybercriminals, QQAazz members advertised the group's services on exclusive, underground cybercriminal online forums.

39. QQAazz members communicated with their criminal clients on these forums and over Jabber, a secure online instant message software.

40. QQAAZZ provided cybercriminals with account information for specific bank accounts controlled by QQAAZZ, which were designated to receive funds stolen by the cybercriminals.

41. After receiving account information from QQAAZZ, cybercriminals would attempt to initiate an electronic funds transfer from the victim's bank accounts to the recipient account provided by QQAAZZ.

42. If the electronic funds transfer was successful, QQAAZZ "cashed-out" (that is, withdrew) the funds and transferred the funds either to a different QQAAZZ-controlled bank account or to "tumbling" services where the funds were converted to cryptocurrency through a series of transactions designed to obfuscate the original source of the funds.

43. QQAAZZ returned a portion of the laundered funds to the cybercriminals and kept a portion for the group as a fee, which was typically between 40 to 50 percent of the total amount of the stolen funds.

Aliases and Fraudulent Identification Documents

44. In furtherance of the conspiracy, QQAAZZ members created and used alias names and fraudulent identification documents. Some QQAAZZ members used multiple fraudulent identification documents with different aliases.

45. The fraudulent identification documents included country identification cards and passports. These fraudulent identification documents were used to register shell companies and open bank accounts at foreign financial institutions. The defendants arranged for funds stolen from fraud victims to be deposited into these foreign financial institution accounts.

46. For example, VALENTINS SEVECS, a citizen of Latvia, used fraudulent Polish identification cards in the names Marek Jaswilko and Rafal Sczytiko as shown in **EXHIBIT A**.

47. NIKA NAZAROV, formerly Nika Utiashvili, a citizen of Georgia, used a fraudulent Bulgarian passport in the name of Stefan Trifonov Zhelyazkov as shown in **EXHIBIT B**.

48. The table below summarizes some of the aliases and fraudulent identification documents used by QQAazz members:

DEFENDANT	ALIASES	FRAUDULENT IDENTIFICATION DOCUMENTS
ALEKSANDRE KOBASHVILI	Antonios Nastas Ognyan Krasimirov Trifonov	Greek Passport Bulgarian Identity Card
DMITRIJS KUZMINOV	Parush Gospodinov Genchev	Bulgarian Passport
NIKA NAZAROV	Mihail Atansov Stefan Trifonov Zhelyazkov	Bulgarian Identity Card Bulgarian Passport
Ruslans Nikitenko	Milen Nikolchev Nikolov Krzysztof Wojciech Lewko Rafal Zimnoch	Bulgarian Passport & Polish Identification Cards
Deniss Ruseckis	Sevdelin Sevdalinov Atanasov	Bulgarian Passport
VALENTINS SEVECS	Marek Jaswilko Rafal Szczytko	Polish Identification Cards
Aleksejs Trofimovics	Aleko Stoyanov Angelov	Bulgarian Identification Card
Arturs Zaharevics	Piotr Ginelli Arkadiusz Szuberski Pawel Tomasz Blitek Marcin Ostapowicz	Polish Identification Cards

Beneficiary Accounts

49. In furtherance of the conspiracy, QQAazz members used aliases and true identities to register shell companies and to open QQAazz-controlled bank accounts at financial institutions in numerous countries, including in Portugal, Spain, Germany, Turkey, the United Kingdom, Belgium and the Netherlands.

50. The shell companies used to open the corporate bank accounts conducted no known legitimate business activity.

51. QQAAZZ members reserved and purchased travel arrangements for other members to travel to the many countries in which QQAAZZ members opened and maintained bank accounts.

52. For example, a QQAAZZ member arranged a flight from London, United Kingdom to Lisbon, Portugal for DMITRIJS KUZMINOV on December 6, 2018.

53. In total, QQAAZZ members opened hundreds of personal bank accounts and corporate bank accounts at numerous financial institutions for the purpose of using the accounts to receive stolen funds from victims.

54. QQAAZZ used corporate bank accounts to receive larger amounts of stolen funds without raising the suspicion of bank officials.

55. QQAAZZ used personal accounts in order to more easily convert stolen funds into cryptocurrency.

56. The following table identifies Defendants and charged conspirators who registered shell companies and opened corporate bank accounts in the names of those shell companies in furtherance of the conspiracy:

DEFENDANT	NAME USED TO OPEN ACCOUNT	SHELL COMPANY	COUNTRY	ACCOUNTS OPENED
Deinis Gorenko	Deinis Gorenko	Adding Chances Unipessoal LDA	Portugal	6
ALEKSANDRE KOBIASHVILI	Antonios Nastas	Nastas Construction Unipessoal LDA	Portugal	10
	Ognyan Krasimirov Trifonov	Robustroots Unipessoal LDA	Portugal	7
DMITRIJS KUZMINOV	Dmitrijs Kuzminvos	Pixelcategory Unipessoal LDA	Portugal	10
NIKA NAZAROV	Stefan Trifonov Zhelyazkov	Stefilaz S.L.	Spain	1

DEFENDANT	NAME USED TO OPEN ACCOUNT	SHELL COMPANY	COUNTRY	ACCOUNTS OPENED
Ruslans Nikitenko	Krzysztof Wojciech Lewko	Selbevulte Unipessoal LDA	Portugal	11
	Milen Nikolchev Nikolov	Privilegioasis Unipessoal LDA	Portugal	11
	Rafal Zimnoch	Colossal Devotion Unipessoal LDA	Portugal	9
	Emil Raykov Yordanov	Emil Raykov Yordanov Unipessoal LDA	Portugal	7
Deniss Ruseckis	Sevdalin Sevdalinov Atanasov	Sevdalin Sevdalinov Atanasov Unipessoal LDA	Portugal	Unknown
	Deniss Ruseckis	Flamingocloud Unipessoal LDA	Portugal	13
VALENTINS SEVECS	Marek Jaswilko	Sauvage Real Unipessoal LDA	Portugal	17
DMITRIJS SLAPINS	Dmitrijs Slapins	Slapincraft Ltd.	United Kingdom	Unknown
	Dmitrijs Slapins	Movers GmbH	Germany	Unknown
TOMASS TRESCINSKIS	Tomass Trescinskis	Golden Halk Heavey Transporte S.L.	Spain	Unknown
Aleksejs Trofimovics	Aleksejs Trofimovics	Aktrofi Services Unipessoal LDA	Portugal	13
	Aleko Stoyanov Angelov	Solidenigma Unipessoal LDA	Portugal	5
	Aleksejs Trofimovics	Atrofi Design Ltd.	United Kingdom	Unknown
	Aleksejs Trofimovics	Atrofi Design Services Ltd.	United Kingdom	Unknown
ARMENS VECELS	Armen Vecels	Build4Less Unipessoal LDA	Portugal	11
Arturs Zaharevics	Piotr Ginelli	Cardinal Gradual Real Estate Unipessoal LDA	Portugal	10
	Arkadiusz Szuberski	PT XMiners Unipessoal LDA	Portugal	7

Receipt of Stolen Funds

57. In furtherance of the conspiracy, QQAazz used the foreign bank accounts as the beneficiary account intended to receive unauthorized electronic transfer of funds that had been stolen, or attempted to be stolen, by cybercriminals.

58. The table below illustrates a sample of the hundreds of attempted and successful unauthorized electronic transfers to QQAazz-controlled bank accounts of funds stolen and attempted to be stolen from United States victims:

DATE	VICTIM	AMOUNT	BENEFICIARY BANK ACCOUNT	DEFENDANT
4/7/16	Medical Device Manufacturer*	\$176,500	Yaromu Gida Ltd. Acct: x5197 (Turkey)	Unknown
10/7/16	Technology Company	\$198,435	Stefilaz S.L. Acct: x2172 (Spain)	NIKA NAZAROV I
11/22/16	PK & SK	\$47,432	Dmitrijs Slapins Acct: x7345 (Germany)	DMITRIJS SLAPINS
9/20/17	JK	\$84,900	Aktrofi Services LDA Acct: x4628 (Portugal)	Aleksejs Trofimovics
11/9/17	Residential Homebuilder	\$98,700	Sauvage Real LDA Acct: x6079 (Portugal)	VALENTINS SEVECS
11/29/17	Architectural Firm	\$121,360	Selbevulte LDA Acct: x3596 (Portugal)	Ruslans Nikitenko
3/8/18	LC	\$29,500	Flamingcloud LDA Acct: x3197 (Portugal)	Deniss Ruseckis
3/12/18	RV	\$150,000	Sauvage Real LDA Acct: x6079 (Portugal)	VALENTINS SEVECS
3/21/18	Landscaping Equipment Manufacturer	\$300,000	Seculo Grandioso Acct: x3004 (Portugal)	Unknown
4/10/18	Electrical Services Contractor	\$59,426	Cardinal Gradual LDA Acct: x3078 (Portugal)	Arturs Zaharevics
8/30/18	Automotive Components Manufacturer*	\$99,693	Selbevulte LDA Acct: x0175 (Portugal)	Ruslans Nikitenko

DATE	VICTIM	AMOUNT	BENEFICIARY BANK ACCOUNT	DEFENDANT
8/30/18	Automotive Components Manufacturer*	\$498,536	Sauvage Real LDA Acct: x0006 (Portugal)	VALENTINS SEVECS
11/14/18	Automotive Parts Manufacturer	\$112,921	Deinis Gorenko Acct: x9194 (Portugal)	Deinis Gorenko
12/6/18	Freight Forwarding Company	\$99,528	Pixelcategory LDA Acct: x0725 (Portugal)	DMITRIJS KUZMINOV
12/12/18	Charity Services	\$299,000	Build4Less LDA Acct: x0103 (Portugal)	ARMENS VECELS
12/12/18	Charity Services	\$150,327	Build4Less LDA Acct: x0103 (Portugal)	ARMENS VECELS
12/12/18	Automobile Parts Supplier	\$149,610	Petar Valentinov Iliev Acct: x2194 (Portugal)	PETAR ILIEV
12/12/18	Equipment Company	\$266,960	Nastas Construction Acct: x0126 (Portugal)	ALEKSANDRE KOBIASHVILI
1/22/19	Baked Goods Manufacturer	\$49,188	Artiom Capacli Acct: x7136 (Spain)	ARTIOM CAPACLI
1/22/19	Baked Goods Manufacturer	\$293,831	Golden Halk Heavey Transporte Acct: x9440 (Spain)	TOMASS TRESCINSKIS
1/22/19	Baked Goods Manufacturer	\$49,182	Ion Cebanu Acct: x5434 (Spain)	ION CEBANU
2/7/19	Farming & Agricultural Retailer	\$78,123	Ruslans Sarapovs Acct: x0217 (Spain)	RUSLANS SARAPOVS
2/7/19	Farming & Agricultural Retailer	\$73,441	Silvestrs Tamenieks Acct: x9561 (Spain)	SILVESTRS TAMENIEKS
3/27/19	Freight and Logistics Service Provider	\$28,263	Abdelhak Hamdaoui Acct: x4350 (Belgium)	ABDELHAK HAMDAOUI

* Indicates victim bank headquartered in the Western District of Pennsylvania

59. In total, QQAazz-controlled bank accounts received tens of millions of dollars stolen from victims worldwide, while millions more dollars were attempted to be transferred to those accounts but were stopped before the transactions were completed.

Cybercriminal Forum Advertisements

60. In furtherance of the conspiracy, QQAAZZ advertised cash-out and money laundering services on exclusive, underground, Russian-speaking, online cybercriminal forums.

61. These forums provided virtual meeting places where vetted cybercriminals sought and offered specialized technical skills, services, or products needed to engage in a variety of cybercriminal activities.

62. One specialized service critical to the cybercriminal underground was the cash-out and money laundering service provided by criminal groups including QQAAZZ.

63. In order to facilitate the sale and receipt of services, the underground forums rented advertisement space to individuals or groups wanting to draw attention to their particular service. These advertisements could cost as much as \$10,000 per year.

64. QQAAZZ advertised its cash-out and money laundering services on the underground forums. For example, QQAAZZ advertised on one such forum that it provided “a global, complicit bank drops service,” indicating the availability of bank accounts in numerous countries throughout the world with “drops” (*i.e.*, money mules) who were complicit in, and knowledgeable of, the criminal scheme.

65. Through these underground forums, QQAAZZ developed numerous cybercriminal clients. Among QQAAZZ’s cybercriminal clientele were several nefarious malware organizations, including GozNym, Dridex, and Trickbot.

Jabber Communications with Cybercriminal Clientele

66. In furtherance of the conspiracy, QQAAZZ communicated, usually in Russian, with its cybercriminal clients using Jabber, a secure online instant message software.

67. QQAAZZ members used several online monikers, including “qqaazz,” “globalqqaazz,” “markdevido,” “richrich,” “donaldtrump55,” “manuel,” “krakadil,” “kalilinux,” “ritchie,” “totala,” and “totala22.” These online monikers were often used by multiple members of QQAAZZ at different times.

68. QQAAZZ used these online monikers to pass account information of QQAAZZ-controlled accounts to the cybercriminal clients.

69. For example, on February 18, 2016, QQAAZZ used the moniker “richrich” to pass account information to a member of GozNym Malware Crime Group. During the chats, “richrich” stated that he was the “drop handler” for the United Kingdom and Europe and that he had access to corporate and personal bank accounts. The GozNym member requested “drop” accounts, and “richrich” provided the GozNym member with corporate bank accounts in the name “Yaromu Gida” at a bank in Turkey. As referenced in the table in Paragraph 58, on April 7, 2016, Yaromu Gida Acct. x5197 received \$176,500 in funds stolen from a medical device manufacturer utilizing a bank headquartered in the Western District of Pennsylvania.

70. As another example, on November 21, 2017, QQAAZZ used the online moniker “donaldtrump55” to pass account information to a known cybercriminal client. During the chats, the cybercriminal client asked for a “drop” in Portugal. “donaldtrump55” provided details for Selbevulte LDA, Account x3596, opened in Portugal by Ruslans Nikitenko using a fraudulent Polish identification card with the alias Krzysztof Wojciech Lewko. As referenced in the table in Paragraph 58, on November 29, 2017, Selbevulte LDA Acct. 3596 was the intended recipient of a \$121,360 transfer from a United States victim.

Cash-Out and Laundering Services

71. In furtherance of the conspiracy, QQAAZZ members would transfer funds received from cybercriminals to other QQAAZZ-controlled bank accounts or to “tumbling” services where

the funds were converted to cryptocurrency through a series of transactions designed to obfuscate the original source of the funds.

72. QQAAZZ used personal bank accounts opened by money mules to receive funds transferred from original accounts in order to more easily convert the funds into cryptocurrency.

Return of Laundered Funds

73. In furtherance of the conspiracy, QQAAZZ charged around 40- to 50-percent of the stolen funds it received as a fee for laundering the money.

74. For example, as part of the Jabber chats between QQAAZZ using the online moniker “richrich” and the member of GozNym described in Paragraph 69 above, “richrich” stated that he would take “55%” of the stolen funds.

75. As a result of the significant amount of stolen funds received into QQAAZZ-controlled accounts, QQAAZZ made millions of dollars providing its cash-out services to cybercriminals.

All in violation of Title 18, United States Code, Section 1956(h).

Forfeiture Allegations

1. The allegations within this Indictment are re-alleged and by this reference fully incorporated herein for the purpose of alleging criminal forfeiture to the United States of America of certain property in which the Defendants have an interest.

2. As a result of committing the money laundering offense alleged in Count One of this Indictment, the Defendants shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in the offense, or any property traceable to such property.

Money Judgment

3. The United States will seek a forfeiture money judgment for a sum of money equal to the value of any property, real or personal, involved in this offense, and any property traceable to such property.

Substitute Assets

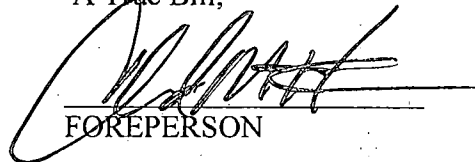
4. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:


- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- 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 subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

All pursuant to Title 18, United States Code, Section 982(a)(1).

A True Bill,


FOREPERSON


SCOTT W. BRADY
United States Attorney
PA ID No. 88352


DEBORAH CONNOR
Chief, Money Laundering and
Asset Recovery Section
Criminal Division

Exhibit A – Fraudulent Polish Identification Cards Used By VALENTINS SEVECS

