

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED

Jul 12 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

ALIAKSANDR KLIMENKA,
a/k/a "Alexander Klimenka,"
a/k/a "Александр Клименко,"
a/k/a "Аляксандр Клименка"

DEFENDANT(S).

INDICTMENT

18 U.S.C. §§ 1960, 2 – Operation of an Unlicensed Money Services Business
18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering

A true bill.

/s/ Foreperson of the Grand Jury

Foreman

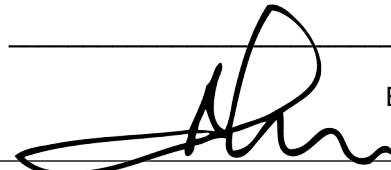
Filed in open court this 12th day of

July 2022.

Stephen Ybarra

Clerk

Bail, \$ Warrant



Hon. Alex G. Tse, United States Magistrate Judge

1 STEPHANIE M. HINDS (CABN 154284)
2 United States Attorney

FILED

Jul 12 2022

Mark B. Busby
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

3
4
5
6
7
8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 SAN FRANCISCO DIVISION

11 UNITED STATES OF AMERICA,) CASE NO. 3:22-cr-00256 MMC
12 Plaintiff,)
13 v.) VIOLATIONS: 18 U.S.C. §§ 1960, 2 – Operation of
14 ALIAKSANDR KLIMENKA,) an Unlicensed Money Services Business; 18 U.S.C.
15 a/k/a “Alexander Klimenka,”) § 1956(h) – Conspiracy to Commit Money
16 a/k/a “Александр Клименко,”) Laundering; 18 U.S.C. § 982(a)(1) – Criminal
17 a/k/a “Аляксандр Клименка,”) Forfeiture
18 Defendant.) SAN FRANCISCO VENUE

19 INDICTMENT

20 The Grand Jury charges:

21 Introductory Allegations

22 At all times relevant to this Indictment:

- 23 1. Defendant ALIAKSANDR KLIMENKA was a citizen of the Republic of Belarus.
24 2. SOFT-FX was a technology services company controlled by ALIAKSANDR
25 KLIMENKA.
26 3. FX OPEN was a financial company controlled by ALIAKSANDR KLIMENKA.
27 4. From in or around 2011 to in or around July 2017, BTC-e was a digital currency
28 exchange controlled by Alexander Vinnik, ALIAKSANR KLIMENKA, and others.

BTC-E BACKGROUND

1
2 5. From its inception in or around 2011 until it was shut down by law enforcement in or
3 around July 2017, BTC-e was one of the world’s largest digital currency exchanges. In the years it
4 operated, BTC-e processed several billion dollars’ worth of transactions and served over one million
5 users worldwide, including numerous customers in the United States and customers in the Northern
6 District of California.

7 6. BTC-e was one of the primary ways by which cyber criminals around the world
8 transferred, laundered, and stored the criminal proceeds of their illegal activities. BTC-e received
9 criminal proceeds of numerous computer intrusions and hacking incidents, ransomware events, identity
10 theft schemes, corrupt public officials, and narcotics distribution rings.

11 7. Because such a significant portion of BTC-e’s business was derived from criminal
12 activity, and given its global reach, the scope of the unlawful conduct was massive. During the relevant
13 timeframe from in or around 2011 to in or around 2017, BTC-e processed millions of bitcoin worth of
14 deposits and withdrawals.

15 8. Users could create BTC-e accounts with only a username, password, and email address.
16 A BTC-e user did not need to provide even the most basic identifying information such as name, date of
17 birth, address, or other identifiers. Unlike legitimate payment processors or digital currency exchanges,
18 BTC-e did not require its users to validate their identity information by providing official identification
19 documents.

20 9. Thus, a user could create a BTC-e account with nothing more than a username and email
21 address, which often bore no relationship to the identity of the actual user. Accounts were therefore
22 easily opened anonymously, including by customers in the United States within the Northern District of
23 California.

24 10. Once a user created an account, they could use it to send and receive bitcoin, or one of
25 several other digital currencies that BTC-e supported. BTC-e held funds on behalf of their customers in
26 digital currency wallets secured on BTC-e’s servers. BTC-e allowed users to purchase digital currencies
27 and fund their accounts through BTC-e’s affiliated financial “partners.” BTC-e also allowed users to
28 transfer funds from one BTC-e account to another through “BTC-e code” or “vouchers,” which

1 functioned like a transferable gift card. BTC-e’s business model obscured and anonymized transactions
2 and source of funds.

3 11. Despite doing substantial business in the United States, BTC-e was not registered as a
4 money services business with the United States Department of the Treasury’s Financial Crimes
5 Enforcement Network (“FinCEN”), as federal law requires. BTC-e had no anti-money laundering
6 and/or “Know-Your-Customer” (KYC) processes and policies in place, as federal law also requires.
7 Indeed, BTC-e collected virtually no customer data at all. As such, it was attractive to those who
8 desired to conceal criminal proceeds, as it made it more difficult for law enforcement to trace and
9 attribute funds.

10 12. BTC-e relied on shell companies and affiliate entities that were similarly unregistered
11 with FinCEN and lacked basic anti-money laundering and KYC policies. These entities catered to an
12 online and worldwide customer base, and electronically “muled” fiat currency in and out of BTC-e.

13 13. BTC-e maintained its servers in the United States. The servers were one of the primary
14 ways in which BTC-e and its operators effectuated their scheme. The servers were leased to and
15 maintained by SOFT FX and ALIAKSANDR KLIMENKA. BTC-e used other third-party companies,
16 including companies within the Northern District of California, to effectuate its operations.

17 BTC-E’S CRIMINAL DESIGN

18 14. As described above, BTC-e’s system was designed so that criminals could accomplish
19 financial transactions with anonymity and thereby avoid apprehension by law enforcement or seizure of
20 funds.

21 15. BTC-e was thus used extensively for illegal purposes and functioned as the exchange of
22 choice to convert digital currency like bitcoin to fiat currency for the criminal world.

23 16. The BTC-e operators were aware that BTC-e functioned as a money laundering
24 enterprise. Messages on BTC-e’s public message board openly and explicitly reflected some of the
25 criminal activity in which the users on the platform were engaged, and how they used BTC-e to launder
26 funds.

27 17. BTC-e users established accounts under monikers suggestive of criminality, including
28 monikers such as “ISIS,” “CocaineCowboys,” “blackhathackers,” “dzkillerhacker,” and “hacker4hire.”

1 18. Criminals used BTC-e to launder criminal proceeds and transfer funds among criminal
2 associates. In particular, BTC-e was used by hacking and computer intrusion rings operating around the
3 world to distribute criminal proceeds of their endeavors. It was also used by rings of identity thieves,
4 corrupt public officials, narcotics distribution networks, and other criminals.

5 19. Some of the earliest significant purveyors of ransomware used BTC-e as a means of
6 storing, distributing, and laundering their criminal proceeds. Ransomware is a practice in which cyber
7 criminals orchestrate the unwanted malicious download of encryption software on an unsuspecting
8 victim computer. It works as follows: once a victim is infected with the malicious software, often by
9 clicking on a malicious link or opening an infected email, the ransomware will encrypt multiple file
10 types on victim machines and hold those files for ransom, requiring the victim to pay the perpetrators of
11 the ransomware scheme in order to have their files decrypted. The only payment methods accepted by
12 purveyors of modern ransomware are bitcoin and other forms of digital currency.

13 20. One such ransomware scheme, CryptoWall, was distributed by methods including
14 phishing emails. CryptoWall was one of the most infamous varieties of ransomware and infected
15 countless computers across the world. During the timeframe relevant to this Indictment, the purveyors
16 of CryptoWall deposited and laundered many hundreds of thousands of dollars' worth of ransom
17 payments into BTC-e.

18 21. BTC-e also served as the receptacle and transmitter of criminal funds from a series of
19 well-publicized computer intrusions and resulting thefts.

20 STATUTORY ALLEGATIONS

21 COUNT ONE: (18 U.S.C. § 1960 – Operation of an Unlicensed Money Transmitting Business)

22 22. The factual allegations in paragraphs 1 through 21 are re-alleged and incorporated herein
23 as if set forth in full.

24 23. From in or around 2011, continuing through on or about July 25, 2017, both dates being
25 approximate and inclusive, in the Northern District of California and elsewhere, the defendant,

26 ALIAKSANDR KLIMENKA,

27 and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed,
28 supervised, directed, and owned all and part of a money transmitting business affecting interstate and

1 foreign commerce, to wit, “BTC-e,” and which:

- 2 a. failed to comply with the money transmitting business registration requirements
- 3 set forth in Title 31, United States Code, Section 5330, and the regulations
- 4 prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5)
- 5 and 1022.380(a)(2); and
- 6 b. otherwise involved the transportation and transmission of funds known to the
- 7 defendant to have been derived from a criminal offense and intended to be used to
- 8 promote and support unlawful activity.

9 and aided and abetted the same.

10 All in violation of Title 18, United States Code, Sections 1960 & 2.

11 COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

12 24. The factual allegations in paragraphs 1 through 21 are re-alleged and incorporated herein

13 as if set forth in full.

14 25. From in or around 2011, continuing through on or about July 25, 2017, both dates being

15 approximate and inclusive, within the Northern District of California, and elsewhere, the defendant,

16 ALIAKSANDR KLIMENKA,

17 willfully and knowingly did combine, conspire, confederate, and agree together and with individuals

18 known and unknown, to knowingly conduct and attempt to conduct financial transactions affecting

19 interstate and foreign commerce which involved the proceeds of a specified unlawful activity, to wit:

- 20 a. operation of an unregistered money transmitting business, in violation of Title 18,
- 21 United States Code, Section 1960
- 22 b. computer hacking and intrusions, in violation of Title 18, United States Code,
- 23 Section 1030;
- 24 c. identity theft, in violation of Title 18, United States Code, Section 1028
- 25 d. interstate transportation of stolen property, in violation of Title 18, United States
- 26 Code, Section 2314;
- 27 e. theft of government proceeds and extortion, in violation of Title 18, United States
- 28 Code, Sections 641 and 1951; and

1 f. narcotics trafficking, in violation of Title 21, United States Code, Section 841,
2 with the intent to promote the carrying on of the specified unlawful activity, and knowing that the
3 transaction was designed in whole and in part to conceal and disguise the nature, location, source,
4 ownership, and proceeds of said specified unlawful activity, and that while conducting and attempting to
5 conduct such financial transaction, knew that the property involved in the financial transaction
6 represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code,
7 Section 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

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

9 FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

10 26. All of the allegations contained in this Indictment are re-alleged and by this reference
11 fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18,
12 United States Code, Section 982(a)(1).

13 27. Upon a conviction for the offenses alleged in Counts 1 through 2 of this Indictment, the
14 defendant,

15 ALIAKSANDR KLIMENKA

16 shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal,
17 involved in those offenses or any property traceable to such offenses.

18 If any of the aforementioned property, as a result of any act or omission of the defendant

- 19 a. cannot be located upon the exercise of due diligence;
20 b. has been transferred or sold to, or deposited with, a third person;
21 c. has been placed beyond the jurisdiction of the Court;
22 d. has been substantially diminished in value; or
23 e. has been commingled with other property that cannot be divided without
24 difficulty;

25 any and all interest the defendant has in other property, up to the value of the property described above,
26 shall be vested in the United States and forfeited to the United States pursuant to 21 U.S.C. § 853(p), as
27 incorporated by 18 U.S.C. § 982(b)(1).

28 All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal

1 Rules of Criminal Procedure.

2

3 DATED: 7/12/2022

A TRUE BILL.

4

/s/

5

FOREPERSON

6

7 STEPHANIE M. HINDS
United States Attorney

8

9 /s/ Claudia Quiroz

10 CLAUDIA QUIROZ

Assistant United States Attorney

11

12 /s/ C. Alden Pelker

13 C. ALDEN PELKER

Trial Attorney

14 Computer Crime & Intellectual Property Section

United States Department of Justice

15

16

17

18

19

20

21

22

23

24

25

26

27

28