UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	
	)	**Civil Action No. 25-cv-**
ALL VIRTUAL CURRENCY HELD IN THE BTC-E OPERATING WALLETS AS OF JULY 25, 2017, AND OTHER ASSETS FURTHER DESCRIBED HEREIN	)	
	)	

Defendants *in rem*.

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

The United States of America, by its attorneys and in accordance with Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions, brings this complaint for forfeiture *in rem* and alleges the following:

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit Defendant Properties involved in: (a) transactions involving the operation of an unlicensed money transmitting business in violation of 18 U.S.C. § 1960; and (b) transactions that are part of a money laundering conspiracy in violation of 18 U.S.C. § 1956(h), both of which grounds render the Defendant Properties forfeitable under 18 U.S.C. § 981(a)(1)(A).

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1345, and 1355.

3. Venue lies in this district pursuant to 28 U.S.C. §§ 1355(b) because acts and omissions giving rise to the forfeiture occurred in this district, and some of the Defendant Properties are located abroad.

NATURE OF THE ACTION AND STATUTORY BASIS FOR FORFEITURE

4. The United States files this *in rem* forfeiture action to seek forfeiture of the Defendant Properties involved in, and traceable to, violations of money laundering conspiracy and unlicensed money transmitting, in violation of 18 U.S.C. §§ 1956(h) and 1960.

5. Procedures for this action are mandated by Rule G of the Supplemental Rules for Admiralty or Maritime Claims and Asset Forfeiture Actions and, to the extent applicable, 18 U.S.C. §§ 981 and 983 and the Federal Rules of Civil Procedure.

6. Title 18, United States Code Section 981(a)(1)(A) mandates forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956, 1957, or 1960, or any property traceable to such property.

7. Title 18, United States Code Section 1956(a)(1)(A)(i) provides, in relevant part, that "[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity— . . . knowing that the transaction is designed in whole or in part . . . to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity" is guilty of concealment money laundering.

8. Title 18, United States Code Section 1956(h) provides that any person who conspires to commit any offense of under Section 1956 is subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.

9. Title 18, United States Code Section 1960 provides that "[w]hoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business" is guilty of illegal money transmitting. An unlicensed money transmitting business is "a money transmitting business which affects interstate or foreign commerce in any manner or degree" and which, *inter alia,* "(B) fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section; or (C) otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."

PARTIES TO THE CASE

10. The Plaintiff is the United States of America.

11. The Defendant Properties comprise the following groups of assets, (A) through (F):

(A) All virtual currency held in the BTC-e operating wallets as of July 25, 2017, including but not limited to: (i) Approximately 925.93922019 bitcoin seized between August 2, 2017, and August 17, 2017; (ii) Approximately 4036.91817168321 ether seized on August 5, 2017; (iii) Approximately 2249.25 litecoin seized between August 7, 2017 and August 11, 2017; (iv) Approximately 284553.52143074 namecoin seized on August 10, 2017; (v) Approximately 1946.609 novacoin seized on August 7, 2017; (vi) Approximately 279.05 peercoin seized on August 11, 2017; (vii) Approximately 33.03682558 dash seized between August 7, 2017 and August 11, 2017; (viii) Approximately 929.5 BTC transferred to 1FFs5hv6JBScJq63aFZvBaNsP6FwnhVgre on or about July 31, 2017; (ix) Approximately 485,705.4599 ETH held in 0x8eb3fa7907ad2Ef4c7E3BA4B1d2F2aAc6f4B5ae6 as of July 30, 2017.

(B) Approximately USD $89,683,590.51, AUD $ 5,471,132.02, RUB 9,339,457.71, and GBP 35,459.32 in funds consolidated and previously held in the name of or for the benefit of Canton Business Corporation at FXOpen and/or

XP Solutions Limited, account number X60FXPNXXF9776910001, and related trading accounts, including any interest earned thereon;

(C) Approximately USD $72,574.48 and RUB 453,361.66 in funds consolidated and previously held in the name of Alexander Vinnik at FXOpen and/or XP Solutions Limited, account number XX20FXPNXXF3396510002, and related trading accounts, including any interest earned thereon;

(D) Approximately USD $5,491.509.67 in funds consolidated and previously held in the name of or for the benefit of Canton Business Corporation and/or Stanislav Golovanov at FXOpen AU Pty Ltd., account number XX46FXPNXXG3750310001, and related trading accounts, including any interest earned thereon;

(E) All funds on deposit in account numbers (i) CZ6903000000000273635458, (ii) CZ6703000000000273635300, and (iii) CZ7803000000000273636266, held in the name of NANO ABC LP at Československá obchodní banka.

(F) All funds on deposit in account number CZ0080000000000001939292223 held in the name of NANO ABC LP at Česká spořitelna banka.

FACTUAL ALLEGATIONS

12. The Defendant Properties were all assets involved in the operation of BTC-e, an unlicensed cryptocurrency exchange that laundered money for criminals from 2011 until it was shut down by U.S. law enforcement in 2017.

13. BTC-e was one of the primary ways by which cyber criminals around the world transferred, laundered, and stored the criminal proceeds of their illegal activities.

14. BTC-e allowed users to set up and fund accounts anonymously, attracting a significant criminal clientele.

15. BTC-e received criminal proceeds of numerous computer intrusions, hacking incidents, ransomware events, identity theft schemes, corrupt public officials, and darknet narcotics distribution rings.

16. To facilitate the movement of funds on behalf of customers without detection or apprehension, BTC-e held numerous cryptocurrency wallets and financial accounts opened in the name of shell and front companies across the globe.

17. The Defendant Properties are all linked to BTC-e's operation, as set forth in detail below.

A. Bitcoin and Digital Currency

18. Digital currency is a digital form of value that is circulated over the Internet.

19. Digital currency includes virtual currency, which refers to digital currency that is typically not denominated in a government-backed currency. Notwithstanding the technical definitions, the terms "digital currency" and "virtual currency" are often used interchangeably. Cryptocurrency refers to digital currency that relies on principles of cryptography to secure and transmit funds in a peer-to-peer network.

20. One of the most popular forms of virtual currency is the cryptocurrency Bitcoin.

21. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network.

22. Bitcoin is just one of many forms of virtual currency. There are thousands of others, including litecoin, ether, and dogecoin.

23. Bitcoin has the largest market capitalization of any present form of decentralized virtual currency.

24. To send and receive bitcoin, the parties involved in a transaction use Bitcoin "addresses."

25. A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers.

26. Each Bitcoin address is controlled through the use of a unique private key.

27. This key is the equivalent of a password or PIN and is necessary to access the funds associated with an address.

28. Only the holder of an address' private key can authorize transfers of bitcoin from that address to other addresses.

29. Users can operate multiple Bitcoin addresses at any given time.

30. All Bitcoin transactions are recorded on the Bitcoin blockchain.

31. The blockchain is a distributed public ledger that maintains all Bitcoin transactions, incoming and outgoing.

32. The blockchain records every Bitcoin address that has ever received a bitcoin and maintains records of every transaction for each Bitcoin address.

33. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner chooses to make information about the owner's Bitcoin address publicly available), investigators can often use the blockchain to help identify the owner of a particular Bitcoin address.

34. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can trace transactions to and among other recipients.

35. The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account.

36. Wallets are used to store and transact in virtual currency.

37. Wallets can interface with blockchains and generate and/or store addresses and private keys.

38. One wallet can hold the private keys for thousands of addresses.

39. To acquire bitcoin, a typical user will purchase them from a virtual currency "exchange."

40. A virtual currency exchange is a platform used to buy and sell virtual currencies. Exchanges allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa.

41. Many exchanges will also store their customers' virtual currency.

B. BTC-e Generally

42. BTC-e was an online digital currency exchange that allowed users to anonymously buy, sell, and store bitcoin and other digital currencies.

43. BTC-e was in operation from 2011 until 2017.

44. Over the course of its operation, BTC-e processed over $9 billion worth of transactions and served over one million users worldwide, including customers in the United States.

45. BTC-e allowed users to easily and quickly set up accounts through the BTC-e website, BTC-e.com.

46. Once an account was established, the user could buy and sell different forms of digital currency through BTC-e.

47. Users could also store money in their BTC-e accounts and could transfer funds to other BTC-e users through "BTC-e codes" or "vouchers," which functioned like digitally transferable gift cards.

48. BTC-e's business model obscured and anonymized transactions.

49. To create a BTC-e account, a user did not need to provide even the most basic identifying information such as a name, date of birth, address, or other identifiers.

50. All BTC-e required to create a user account was a self-created username, password, and email address.

51. Unlike legitimate payment processors or digital currency exchanges, BTC-e did not require its users to validate their identity by providing official identification documents.

52. BTC-e at times requested identifying documentation, such as a driver's license or passport, when a customer attempted to use bank wires, but such documentation was not always requested or required, and was not required to engage in most transactions through BTC-e.

53. Thus, a user could create a BTC-e account with nothing more than a username and email address, which often bore no relationship to the identity of the actual user. Accounts were easily opened anonymously, including by customers in the United States.

54. BTC-e allowed users to buy and sell numerous forms of cryptocurrency, including bitcoin, ether, litecoin, namecoin, novacoin, peercoin, and dash.

55. BTC-e held wallets for each of these cryptocurrencies to enable users' purchases and sales, and to assist in processing user transactions.

56. BTC-e secured its cryptocurrency wallets on BTC-e's servers.

C. BTC-e's Operation as an Illegal Money Transmitting Business

57. BTC-e's core business model was money transmitting—accepting funds from users and transferring those funds to other people or accounts.

58. BTC-e openly described its money transmitting business model on its public website, explaining, "BTC-e provides an online tool that allows users to freely trade Bitcoins for a number of different currencies worldwide."

59. A review of the BTC-e servers seized by U.S. law enforcement in 2017 confirmed that BTC-e had over one million customers and processed over $9 billion worth of transactions, including customer deposits, transfers within BTC-e to other users and accounts, and withdrawals.

60. The trading activity on BTC-e included swaps across numerous types of cryptocurrencies, as well as converting cryptocurrency to fiat currency, particularly U.S. Dollars and Russian Rubles.

61. Money transmitters doing business in the United States have numerous obligations under U.S. laws designed to safeguard the financial system and prevent money laundering; variations of these laws are replicated in other jurisdictions worldwide.

62. However, BTC-e failed to comply with these laws, despite BTC-e's substantial business footprint in the United States, including a U.S. client base as well as U.S.-located servers that were essential to the site's operation.

63. In particular, BTC-e was not registered as a money services business with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), as federal law requires.

64. BTC-e had no meaningful anti-money laundering and/or "Know-Your-Customer" ("KYC") processes and policies in place, as federal law also requires.

65. This made BTC-e particularly attractive to those who desired to conceal criminal proceeds, as it made it more difficult for law enforcement to trace and attribute funds.

66. FinCEN is based in Washington, D.C.

67. A failure to register with FinCEN is an omission occurring in Washington, D.C., giving this District jurisdiction over cases involving violations of 18 U.S.C. § 1960 based on a failure to register with FinCEN.

D. Criminal Use of BTC-e

68. BTC-e was utilized by cybercriminals worldwide and was one of the principal entities used to launder and liquidate criminal proceeds.

69. Analysis of data housed on BTC-e's servers, the Bitcoin blockchain, communications, and financial account records showed that a sizable amount of BTC-e's business was derived from criminal activity.

70. BTC-e processed transactions involving the proceeds of specified unlawful activity, including:

a. operation of an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960;

b. computer hacking and intrusions, in violation of 18 U.S.C. § 1030;

c. identity theft, in violation of 18 U.S.C. § 1028;

d. interstate transportation of stolen property, in violation of 18 U.S.C. § 2314;

e. theft of government proceeds and extortion, in violation of 18 U.S.C. §§ 641 and 1951; and

f. narcotics trafficking, in violation of 21 U.S.C. § 841.

71. BTC-e received and transferred cryptocurrency valued at at least $68.3 million from darknet marketplaces; at least $14.0 million from fraud shops; at least $10.3 million from ransomware perpetrators; at least $20.0 million from virtual currency mixers; and at least $8.25 million from the hack of Mt. Gox.

72. Messages on BTC-e's own message platform openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged, and how they used BTC-e to launder funds.

73. The owners and administrators of BTC-e were aware that BTC-e functioned as a money laundering enterprise.

74. Specific illustrative examples of BTC-e's role as a forum for money laundering are provided in the paragraphs immediately below:

i. Narcotics Trafficking

75. BTC-e's launch in 2011 aligned with the launch and growing popularity of Silk Road.

76. Silk Road was the first darknet drug market which allowed users to buy and sell illegal narcotics and other criminal goods using bitcoin.

77. Silk Road was shuttered by law enforcement in 2013.

78. After Silk Road closed, it was soon replaced by other similar sites and services, such as Silk Road 2.0, Evolution, Agora, and AlphaBay.

79. These darknet markets openly advertised and promoted the sale of drugs, featuring colorful home pages with photographs of different pills, crystals, and powders offered by vendors boasting 5-star ratings and glowing customer reviews.

80. While the marketplaces allowed the dealers—known as "vendors"—to transact with buyers anonymously within the site, the dealers needed to be able cash out their bitcoin at an exchange that would not ask questions about the source of funds, verify the dealer's identity, freeze their accounts as suspicious, or report the activity to law enforcement.

81. BTC-e thus became a sought-after platform for dealers to cash out their bitcoin from their darknet drug sales.

82. After selling fentanyl, methamphetamine, cocaine, and opiates, the drug dealers would take their earned bitcoin and transfer it to BTC-e to convert it to U.S. dollars.

83. Over the course of the service's operation, BTC-e received at least $68.3 million from darknet marketplaces.

ii. Ransomware Attacks

84. Some of the largest purveyors of ransomware at the time used BTC-e as a means of storing, distributing, and laundering their criminal proceeds.

85. Ransomware is a type of criminal scheme in which cyber criminals orchestrate the unwanted encryption of a victim computer or computer network and demand payment in order for the victim to regain computer access.

86. In a ransomware attack, a victim is infected with malicious software, often by clicking on a fraudulent email.

87. From there, the ransomware will encrypt files on victim machines and hold those files for ransom, meaning the victim must pay the administrators of the ransomware scheme in order to regain access to the contents of their files.

88. Victims that pay the ransom are able to decrypt their files by using a decryption key provided by the ransomware perpetrators.

89. Modern purveyors of ransomware demand and accept ransom payments exclusively in cryptocurrency.

90. The method of encryption implemented by the ransomware typically renders it impossible for victims to decrypt their encrypted files without paying the ransom.

91. CryptoWall was one of the most infamous early varieties of ransomware, which infected thousands of computers across the globe, including many victims in the United States.

92. The perpetrators of CryptoWall deposited and laundered hundreds of thousands of dollars' worth of ransom payments at BTC-e.

93. Other ransomware perpetrators similarly used BTC-e to launder and cash out victim payments.

iii. *Hacks and Thefts: Mt. Gox*

94. BTC-e was a popular repository for cyber criminals who hacked into victim computers and stole their cryptocurrency.

95. One example involved funds taken from the digital currency exchange Mt. Gox, which operated between 2011 and 2014.

96. In 2014, Mt. Gox declared bankruptcy after it was impacted by a series of widely-reported intrusions that resulted in thefts totaling hundreds of thousands of bitcoin.

97. Approximately 300,000 of the bitcoin stolen from Mt. Gox were sent to three accounts at BTC-e.

98. BTC-e was used to conceal the stolen funds and obscure their ultimate destination, allowing the perpetrator(s) to profit from their crimes.

E. Alexander VINNIK

99. Alexander Vinnik ("VINNIK"), a Russian national, was one of the primary operators of BTC-e.

100. VINNIK was charged by indictment in the Northern District of California in May 2016 and in a superseding indictment in the same district in January 2017. *United States v. BTC-e et al.*, No. 3:16-cr-00227-SI, ECF Nos. 1, 6 (N.D. Cal.).

101. On May 3, 2024, VINNIK pled guilty in the U.S. District Court for the Northern District of California to money laundering conspiracy in violation of 18 U.S.C. § 1956(h) for his role in operating BTC-e. *See United States v. BTC-e et al.*, No. 3:16-cr-00227-SI, ECF No. 123 (N.D. Cal. May 3, 2024).

102. In this plea agreement, VINNIK admitted that "BTC-e was one of the primary ways by which cyber criminals around the world transferred, laundered, and stored the criminal proceeds of their illegal activities. BTC-e received criminal proceeds of numerous computer intrusions and hacking incidents, ransomware attacks, identity theft schemes, corrupt public officials, and narcotics distribution rings." *Id.* at 3.

103. VINNIK further identified many of the above-listed Defendant Properties and accounts holding the Defendant Properties as assets that were forfeitable as a result of VINNIK's guilty plea. *Id.* at 12-13.

104. On February 11, 2025, the criminal case against VINNIK was dismissed prior to a sentence being imposed.

105. The dismissal was not a result of any evidentiary infirmity.

F. Defendant Property A

106. Defendant Property A reflects the cryptocurrency held in BTC-e's operating wallets at the time the site was seized on July 25, 2017, including the specific cryptocurrency assets that were successfully seized by the U.S. government as part of that takedown.

107. For much of its operation, BTC-e maintained its servers in the United States.

108. The servers were one of the primary ways in which BTC-e and its operators effectuated their scheme.

109. On July 25, 2017, Alexander VINNIK was arrested, and the United States seized the BTC-e servers, which at the time were located at a server hosting facility in the District of New Jersey.

110. The servers contained BTC-e's cryptocurrency wallets, which held BTC-e's operating assets, customer deposits, and reserves.

111. The wallet files included numerous cryptocurrency asset types, including Bitcoin, ether, litecoin, namecoin, novacoin, peercoin, and dash.

112. BTC-e's security protections and infrastructure set-up resulted in some delays in law enforcement locating and gaining access to the private keys associated with BTC-e.

113. During that time, remaining BTC-e operators still at large gained access to back-up copies of the wallets and transferred out the bulk of the funds.

114. Law enforcement successfully seized (i) approximately 925.93922019 bitcoin seized between August 2, 2017, and August 17, 2017; (ii) approximately 4036.91817168321 ether seized on August 5, 2017; (iii) approximately 2249.25 litecoin seized between August 7, 2017 and August 11, 2017; (iv) approximately 284553.52143074 namecoin seized on August 10, 2017; (v) approximately 1946.609 novacoin seized on August 7, 2017; (vi) approximately 279.05 peercoin seized on August 11, 2017; and (vii) approximately 33.03682558 dash seized between August 7, 2017 and August 11, 2017.

115. BTC-e co-conspirators were able to access and move remaining cryptocurrency from BTC-e's wallets.

116. Specifically, ether was transferred out of BTC-e's wallet as follows:

a. On or about July 29, a test transaction of 0.0001 ETH was sent from BTC-e's wallet to address 0x8eb3fa7907ad2Ef4c7E3BA4B1d2F2aAc6f4B5ae6.

b. Shortly thereafter, approximately 485,705.4598 ETH—valued at just under $91 million USD at the time—was sent to the same address.

117. As of July 30, 2017, the balance of address 0x8eb3fa7907ad2Ef4c7E3BA4B1d2F2aAc6f4B5ae6 was 485,705.4599 ETH, which constituted

funds directly transferred out of BTC-e's wallet before the funds could be seized by the U.S. government.

118. Bitcoin was transferred out of BTC-e's wallets in multiple transactions.

119. Those transfers included approximately 929.5 BTC transferred to 1FFs5hv6JBScJq63aFZvBaNsP6FwnhVgre on or about July 31, 2017 in the following transactions:

a. 522 BTC transferred in transaction hash 254a9a13c09f6064d546a720c1b9a0c98c1262bd258eb83b46adb9d1852a6079;

b. 100 BTC transferred in transaction hash 3f06b0242428b1df0744cd2a6e1aa0296d672b7b83fc41da11076789520b4cb1;

c. 100 BTC transferred in transaction hash 9c3d0af222fde5d843972dbae105dd4242b9ef2e3854b86b862355ec0db0c36e;

d. 50 BTC transferred in transaction hash 97e1ce2d17a14a092ecd9accaf41c0d7a05a116cc4f07461e3be3c8f863d38dd;

e. 50 BTC transferred in transaction hash aa272a634d74e26fa07cca5c6cb5d55595882f266d37da395c60402c4c18a3c9;

f. 50 BTC transferred in transaction hash 18a6be164e79b94d02b35ebbdf8a6d1502ce8826496951efc43d5ff2bc4889b9;

g. 10 BTC transferred in transaction hash 32b910aca744c8d6451f78b46625a97a25f2f412ccb0102d8c4f709242cf215d;

h. 20 BTC transferred in transaction hash 559de7cc75b88f718aa04c6410d6677369d3635410bb85d65c64e6cf521c6dfd;

i. 20 BTC transferred in transaction hash 93688423262ad72229a1f4827ffec9475c4e006debd71fbcea18b68283912193;

j. 5 BTC transferred in transaction hash 971cacb0d81a7a8eaa6d6a086cee399488e332af7cb23a0df862d09106addd46; and

k. 2.5 BTC transferred in transaction hash 3a0c3bdd7d1e5e7560990b359391ab906cabccefed1adc044bc4683388cd84fe.

120. The 929.5 bitcoin involved in the transactions detailed above constituted funds directly transferred out of BTC-e's wallets before the funds could be seized by the U.S. government.

121. The unseized bitcoin and ether were subsequently transferred to new addresses, including those associated with the exchange Wex.

122. Wex was an effort to continue BTC-e's criminal operation under a new name, despite the U.S. criminal case.

123. The unseized funds were subsequently further laundered and remain at large.

G. Shell Companies & Accounts

124. While BTC-e was operating, VINNIK and the other BTC-e operators went to considerable lengths to conceal their identities and BTC-e's corporate location.

125. The BTC-e website did not list executives' or employees' names and provided conflicting information about the country from which the company operated.

126. The website did not provide a valid physical address for BTC-e.

127. Even when issues arose with the exchange in 2013 and the operators needed to reassure their users, they refused to provide reporters with their full names. *See* BTC-e: Our Recent

Issues Were Caused By a Surge In Users, Coindesk, https://www.coindesk.com/markets/2013/12/11/btc-e-our-recent-issues-were-caused-by-a-surge-in-users (Dec. 11, 2013), *accessed on* March 8, 2025.

128. BTC-e offered users many different ways to deposit and withdraw funds.

129. The supported platforms changed over time but included various electronic payment methods as well as bank transfers.

130. To process these payments successfully, BTC-e needed to have accounts at different payment platforms.

131. For example, in order for BTC-e to allow its users to buy cryptocurrency in exchange for Liberty Reserve Dollars, BTC-e needed to have an account set up at Liberty Reserve where it could receive and store Liberty Reserve Dollars.

132. Liberty Reserve was a Costa Rica-based digital currency exchange service that allowed users to register and transfer money to other users with only a name, e-mail address, and birth date.

133. Deposits could be made through third parties using a credit card or bank wire, among other deposit options.

134. Deposited funds were then "converted" into Liberty Reserve Dollars (LRUSD) or Liberty Reserve Euros (LREUR), which were tied to the value of the U.S. dollar and the euro, respectively.

135. Liberty Reserve was shut down by U.S. law enforcement in May 2013 after the founder was charged in the United States with money laundering and operation of an unlicensed money service business.

136. For BTC-e to accept payment in bank wires, BTC-e needed to have access to bank accounts.

137. In order to avoid detection, BTC-e relied on a network of shell and front companies across the globe.

138. Accounts were opened in the name of the shell companies rather than in BTC-e's true name.

139. Canton Business Corp. (Canton) was one of the primary shell companies used as a "front" for BTC-e's operations.

140. Canton Business Corp. was incorporated in the Seychelles in August 2011.

141. Canton Business Corp.'s business paperwork listed "Mr. Golovanov Stanislav," discussed further below, as the company's director.

142. Other BTC-e shell companies included Nano ABC, Always Efficient LLP, Eurostyle Advisor Ltd., Donald Communications Corporation, Pantera Capital S.A., Gem Invest, Big Computers, and TIM Solutions.

143. The shell companies generally used nominee directors to further conceal the connections to the BTC-e administrators.

144. The BTC-e operators, including VINNIK, used aliases and appropriated other individuals' identities to set up accounts.

145. One of the most prolific nominee aliases used for BTC-e shell companies and financial accounts was "Stanislav Golovanov."

146. The real Stanislav Golovanov was a corporate nominee who lived in Russia.

147. Email correspondence dated September 2011 between VINNIK and the real Golovanov captured VINNIK's retention of Golovanov's services to set up an account at a foreign bank. Golovanov provided VINNIK with a quoted price per trip to the bank.

148. Subsequent to the email exchange, VINNIK sent an application with Golovanov's information to open an account at Rietmu Bank in Latvia.

149. VINNIK subsequently re-used Golovanov's identity and contact information to open numerous accounts at other financial institutions.

150. Golovanov was listed as the beneficiary of Canton Business Corporation and its accounts.

151. This gave the appearance that Golovanov was controlling the various shell company financial accounts, when in reality VINNIK and his BTC-e administrator co-conspirators were ultimately responsible.

152. VINNIK established an email account in Golovanov's name, golovanov.stas@gmail.com, and used it to communicate with other companies, such as financial institutions, while pretending to be Golovanov.

153. When VINNIK was arrested in Greece in 2017, Greek authorities found numerous credit cards in VINNIK's procession, including a corporate bank card in the name of Stanislav Golovanov.

154. BTC-e customers attempting to send money to BTC-e by bank wire were typically instructed to send funds to accounts held in the name of one of BTC-e's shell companies.

155. On several occasions, financial institutions flagged the account activity, asked follow-up questions, and/or shut down the accounts.

156. For example, Baltikums Bank raised concerns about an account in the name of Canton Business Corp., which the bank realized appeared to be primarily used for deposits related to the operation of a bitcoin exchange.

157. In an email to VINNIK's alias "Golovanov," a Baltikums Bank representative noted that the activity appeared contrary to the stated purpose of the bank account.

158. When confronted, VINNIK (as Golovanov) admitted that these deposits were tied to the operation of BTC-e.

159. Baltikums subsequently closed the Canton Business Corp. bank account, forcing VINNIK to move his operation to another financial institution.

160. After Baltikums closed the Canton account, VINNIK utilized an account at Hermes Bank, which is located in St. Lucia in the Caribbean.

161. The new account at Hermes Bank was soon also closed, due to a reported "compliance reason."

162. To ensure continued access to banking services and expanded trading connectivity to different markets, BTC-e needed to establish relationships with larger financial firms within which BTC-e could "nest" its operations without arousing suspicion.

163. BTC-e could open accounts at these firms and then send and receive funds through the larger firms' vetted accounts without arousing the suspicions of the bank compliance departments.

164. Generally, these sorts of nested relationships depend on the larger firms' ignorance of or complicity in the smaller company's activities.

165. One of the primary firms that BTC-e used was Mayzus Financial Services, which also offered services through its related service, MoneyPolo.

166. BTC-e shell companies Always Efficient and Canton Business Corp. had accounts at Mayzus Financial Services, which in turn had accounts at multiple international banks.

167. BTC-e customers could wire funds to Mayzus Financial Services with a wire reference indicating that the deposit was for the credit of, e.g., the Canton Business Corp. account.

168. Once the funds were received in Mayzus's bank account, Mayzus would credit the corresponding amount to Canton's account at Mayzus.

169. BTC-e would then update the individual customer's BTC-e account balance accordingly.

170. BTC-e relied on its accounts at Mayzus to be able to accept and transmit customer funds.

171. One of the other primary services that BTC-e used to facilitate its financial activity was FXOpen, described further below in relation to Defendant Properties B, C, and D.

H. FXOpen and XP Solutions

172. FXOpen is a financial services firm offering online trading services, primarily focusing on Forex markets as well as cryptocurrency.

173. The company allows individual and institutional customers to open accounts, deposit and transfer funds, and trade.

174. FXOpen operates numerous divisions worldwide, including FXOpen New Zealand and FXOpen Australia (FXOpen AU), which are each incorporated as their own corporate entities.

175. FXOpen companies operate in Australia, New Zealand, Russia, Saint Kitts and Nevis, and the United Kingdom and have representatives in a host of other countries.

176. FXOpen was operated by Belarussian-Cypriot national Aliaksandr KLIMENKA.

177. KLIMENKA was a friend and business associate of VINNIK's when VINNIK was residing in Moscow.

178. In July 2022, KLIMENKA was indicted in the Northern District of California with money laundering conspiracy and operating an unlicensed money transmitting business in connection with his work on BTC-e. *United States v. Aliaksandr Klimenka,* 22-cr-256, ECF No. 1 (N.D. Cal.).

179. KLIMENKA was arrested in Latvia in December 2023, and appeared in the United States in January 2024.

180. As of June 10, 2025, KLIMENKA is pending trial in the Northern District of California.

181. FXOpen user transactions were processed using eWallet Account Software from XP Solutions Limited (XPS).

182. XPS was a New Zealand limited company whose ownership and control overlapped with that of FXOpen.

183. FXOpen used XPS eWallet Account Software for FXOpen user deposits, withdrawals, and funds transfers to and from trading accounts held with FXOpen.

184. The XPS eWallet Account Software facilitated instant electronic funds transfers between various accounts, or eWallets, with support for multiple currencies.

185. Automated account messages pertaining to account activity sometimes referenced FXOpen and sometimes referenced XPS.

186. BTC-e opened accounts at FXOpen/XPS, including accounts in the name of Canton Business Corp. at both FXOpen New Zealand and FXOpen Australia.

187. The New Zealand and Australian accounts included:

a. Defendant Property B: Account X60FXPNXXF9776910001 at FXOpen New Zealand, in the name of Canton Business Corporation and Stanislav Golovanov;

b. Defendant Property C: Account XX20FXPNXXF3396510002 at FXOpen New Zealand, in the name of Alexander Vinnik;

c. Defendant Property D: Account XX46FXPNXXG3750310001 at FXOpen Australia, in the name of Canton Business Corporation and Stanislav Golovanov;

d. Account XX31FXPNXXG3750610001 at FXOpen Australia, in the name of Alexander Vinnik. (This account was emptied in 2016 and is therefore not sought for forfeiture.)

188. As described further below, the FXOpen accounts described in the previous paragraph were used to hold and transmit funds tied to the operation of BTC-e.

189. The balances of each of the above FXOpen accounts constituted criminally tainted property which was acquired as a result of, and/or otherwise derived from, BTC-e's criminal activity.

190. A search warrant executed on another alias email address controlled by VINNIK, vasiliy.sidorov.msk@gmail.com, revealed a May 2017 conversation between VINNIK and MoneyPolo.

191. MoneyPolo was a Mayzus-linked a payment processor.

192. In the May 2017 conversation, MoneyPolo inquired about transfers from the Always Efficient MoneyPolo account—a BTC-e shell company account—to the Canton Business Corp. account and then to XP Solutions.

193. VINNIK, using a pseudonym, stated that all transfers into the account were "topping up the btc-e trading account" (translated from Russian), and all outgoing transfers from the account were withdrawals from BTC-e.

194. BTC-e received or used "invoices" from FXOpen to legitimize BTC-e's financial activities on multiple occasions.

195. These invoices were often in large, round-dollar amounts, including just below $100,000, and for purported services that did not reflect real business activity.

196. For example, in May 2013, Baltikums Bank reached out to "Stanislav Golovanov" regarding activity in the Canton Business Corporation account at Baltikums.

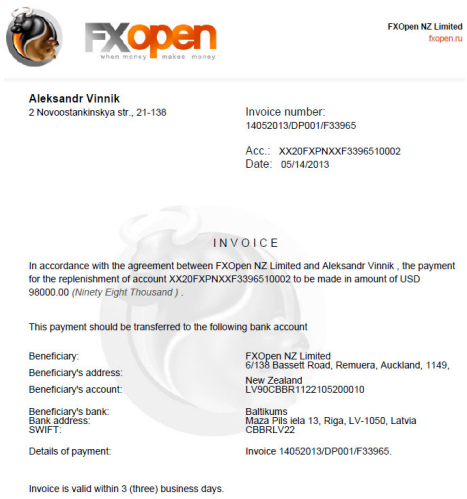
197. VINNIK, using the email address golovanov.stas@gmail.com, attached an invoice from FXOpen to verify the transaction.

198. The original invoice was made out to Aleksandr VINNIK and listed FXOpen Account Number XX20FXPNXXF3396510002 (the Defendant Property C account).

199. A Baltikums Bank representative noted that the invoice did not name Canton Business Corporation.

200. "Golovanov" promptly responded that this was a "glitch" and furnished a new invoice—with the same date and for the same amount of $98,000—naming Canton Business Corporation, Account XX60FXPNXXF9776910001 (the Defendant Property B account).

201. Copies of the two invoices described in the previous paragraph appear as follows:



FXOpen NZ Limited
fxopen.ru

Aleksandr Vinnik
2 Novoostankinskya str., 21-138

Invoice number:
14052013/DP001/F33965

Acc.: XX20FXPNXXF3396510002
Date: 05/14/2013

INVOICE

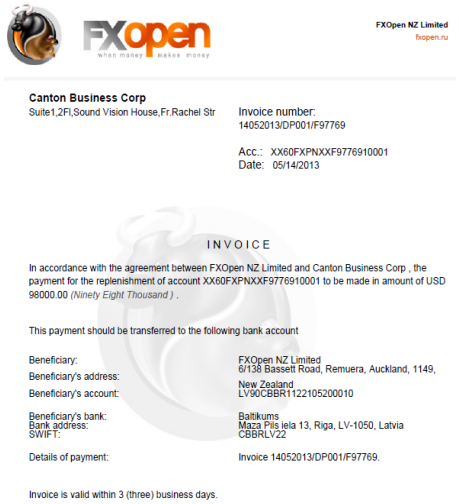
In accordance with the agreement between FXOpen NZ Limited and Aleksandr Vinnik , the payment for the replenishment of account XX20FXPNXXF3396510002 to be made in amount of USD 98000.00 *(Ninety Eight Thousand)* .

This payment should be transferred to the following bank account

Beneficiary:	FXOpen NZ Limited
Beneficiary's address:	6/138 Bassett Road, Remuera, Auckland, 1149, New Zealand
Beneficiary's account:	LV90CBBR1122105200010
Beneficiary's bank:	Baltikums
Bank address:	Maza Pils iela 13, Riga, LV-1050, Latvia
SWIFT:	CBBRLV22
Details of payment:	Invoice 14052013/DP001/F33965.

Invoice is valid within 3 (three) business days.

a)



FXOpen NZ Limited
fxopen.ru

Canton Business Corp
Suite1,2Fl,Sound Vision House,Fr.Rachel Str

Invoice number:
14052013/DP001/F97769

Acc.: XX60FXPNXXF9776910001
Date: 05/14/2013

INVOICE

In accordance with the agreement between FXOpen NZ Limited and Canton Business Corp , the payment for the replenishment of account XX60FXPNXXF9776910001 to be made in amount of USD 98000.00 *(Ninety Eight Thousand)* .

This payment should be transferred to the following bank account

Beneficiary:	FXOpen NZ Limited
Beneficiary's address:	6/138 Bassett Road, Remuera, Auckland, 1149, New Zealand
Beneficiary's account:	LV90CBBR1122105200010
Beneficiary's bank:	Baltikums
Bank address:	Maza Pils iela 13, Riga, LV-1050, Latvia
SWIFT:	CBBRLV22
Details of payment:	Invoice 14052013/DP001/F97769.

Invoice is valid within 3 (three) business days.

b)

202. In February 2012, Klimenka, using the account CEO <alexander.klimenka@fxopen.org>, emailed VINNIK at info@wme.cc.

203. Klimenka's February 2012 email included an attached invoice to Canton Business Corporation from FXOpen for $99,100, purportedly for "Advance payment for marketing and advertisement."

204. In many instances, the BTC-e-associated FXOpen accounts above were funded by transfers from other BTC-e accounts, including other FXOpen accounts and accounts at Mayzus and Mayzus-associated entities.

205. For example, according to Mayzus financial documentation of Euro transfers, from December 2015 through July 2017, Canton Business Corp. transferred approximately $27.57 million EUR to XPS/FXOpen through Mayzus.

206. Additional detail regarding Mayzus-associated wires into and out of the Defendant Property D account is described below.

I. Defendant Property B

207. Defendant Property B reflects the funds held in the Canton Business Corp. account at FXOpen New Zealand/XPS.

208. This includes funds that were previously held in the related trading accounts and which were consolidated in X60FXPNXXF9776910001.

209. Following the public disruption of BTC-e, the Defendant Property B account was frozen, and associated trading funds and sub-accounts were consolidated.

210. On December 18, 2019, the United States District Court for the Northern District of California issued a seizure warrant for the contents of Defendant Property B on the grounds that the contents were subject to forfeiture as property involved in and proceeds of money laundering and illegal money transmission. N.D. Cal. Case No. 3:19-72060.

211. As of March 17, 2025, the balance of Defendant Property B is approximately USD $89,683,590.51, AUD $ 5,471,132.02, RUB 9,339,457.71, and GBP 35,459.32.

212. Defendant Property B included transfers in U.S. Dollars (USD), Euros (EUR), British Pounds (GBP), and Russian Rubles (RUB).

213. Numerous outgoing payments from the Defendant Property B account include comments referencing “MT4 license” or variations thereof.

214. MT4 refers to MetaTrader, a trading platform used in the operation of BTC-e.

215. These MT4 transfers indicate that Defendant Property B was used to pay for operating expenses of BTC-e and/or to make payments to individuals involved in the operation of BTC-e.

216. On April 1, 2015, the Defendant Property B account received a transfer of approximately $5.5 million USD and a second transfer of approximately 10 million RUB.

217. A significant amount of money (approximately $9.57 million USD and $5.387 AUD) was transferred to Defendant Property B from Defendant Property D (the Canton Business Corp. account at FXOpen Australia).

218. As described further below, the funds in Defendant Property D were also tied to the operation of BTC-e.

219. The AUD balance was funded from a single transfer on December 28, 2015, from Defendant Property D, the Canton Business Corp. FXOpen/XPS Australia account, in the amount of approximately 5.4 million AUD.

220. There was some subsequent trading activity, leading to a final balance as of May 2017 of AUD $ 5,471,132.02.

221. The entirety of the AUD funds in Defendant Property B were sourced from Defendant Property D.

222. In December 2015, the Defendant Property B account also received a $9.57 million USD deposit from Defendant Property D.

223. The account received multiple EUR wire transfers from unidentified sources.

224. The GBP balance was from a single bank wire of 35,459.32 from an unidentified source, and there was no further GBP activity.

225. The funds transferred into and through Defendant Property B were all tied to and derived from the criminal operation of BTC-e.

226. Defendant Property B thus constitutes criminally tainted property, by virtue of its use to enable the operation of BTC-e.

J. Defendant Property C

227. Defendant Property C reflects the funds held in VINNIK's account at FXOpen New Zealand/XPS.

228. Following the public disruption of BTC-e, the Defendant Property C account was frozen, and associated trading funds and sub-accounts were consolidated.

229. Defendant Property C includes funds that were previously held in related trading accounts and which were consolidated in XX20FXPNXXF3396510002.

230. As of March 17, 2025, the balance of Defendant Property C is approximately USD $72,574.48 and RUB 453,361.66.

231. The Defendant Property C account includes funds in both USD and RUB.

232. Defendant Property C was funded in part from another BTC-e operating account, the Defendant Property B account (the Canton Business Corp. account at FXOpen New Zealand).

233. In April 2016, the Defendant Property C account received a 3 million RUB deposit from the Defendant Property B account.

234. A significant portion of the transactions through the Defendant Property C account appear to be using the account as a pass-through, in which funds are deposited and then transferred on to another account shortly thereafter. This includes pass-throughs for apparent trading activity tied to the account.

235. For example, on multiple instances in January 2016, the account received a deposit from WebMoney in the amount of 1 million RUB; the same day, the account transferred 1 million RUB to another FXOpen trading account.

236. On April 28, 2016, the account received a 3 million RUB deposit from Defendant Property B, the Canton Business Corp. account at FXOpen/XPS New Zealand. On the same day, the funds were transferred out.

237. The Defendant Property C account received approximately 45.3 million RUB deposits from June 2014 to August 2017.

238. The majority of the RUB inflows—totaling just under 30 million RUB—came from WebMoney.

239. WebMoney was one of the primary deposit methods for BTC-e customers.

240. WebMoney is an electronic payment system that was extremely popular in Russia, including among Russian cyber criminals.

241. Many of the deposits were large, round-figure deposits, including multiple 1 million and 990 million RUB deposits.

242. On numerous occasions, the large transfers were split into multiple smaller transactions sent on the same day within hours or even minutes of each other.

243. These sorts of transactions are indicative of money laundering or structuring in an attempt to mule funds into an account without triggering additional screening or red flags.

244. In addition to the WebMoney deposits, there were sizable inflows totaling approximately 8.2 million RUB across over 80 transactions from Yandex Money, another Russian-based payment platform.

245. There were also inflows from wire transfers.

246. The account activity is consistent with the account receiving transfers related to BTC-e.

247. VINNIK also used the business alias "WME" and the email address wmewme@gmail.com.

248. VINNIK operated as an exchanger under the alias "WME" prior to joining BTC-e.

249. "WME" was a reference to WebMoney exchange.

250. Following the launch of BTC-e, VINNIK integrated his WME business into the BTC-e platform.

251. A review of the email account wmewme@gmail.com revealed the account received many emails from accounts associated with FXOpen.

252. This included numerous emails from "noreply@fxopen.com" related to transactions and account statements, as well as email from FXopen-support@fxopen.com regarding trading inquiries.

253. Several emails specifically referenced account number XX20FXPNXXF3396510002 (the Defendant Property C account).

254. Funds transferred into Defendant Property C were tied to, and thus tainted by, VINNIK's criminal activities, namely the operation of BTC-e.

K. Defendant Property D

255. Defendant Property D reflects the funds that were held in BTC-e's accounts at FXOpen Australia. This includes funds that were previously held in the related trading accounts and which were consolidated at XX46FXPNXXG3750310001.

256. FXOpen AU Account Number XX46FXPNXXG3750310001 (Defendant Property D) was opened in the name of Stanislav Golovanov, with the company name listed as Canton Business Corporation.

257. The email on the account was golovanov.stas@gmail.com.

258. Golovanov.stas@gmail.com is the email address used by VINNIK to pose as Golovanov.

259. From November 2013 through at least December 2015, the golovanov.stas@gmail.com account received several emails per month from noreply@fxopen.com.au.

260. The majority of the emails contained account statements and withdrawal and transfer confirmations related to FXOpen AU Account Number XX46FXPNXXG3750310001 (Defendant Property D).

261. Between approximately December 2013 and April 2017, the Defendant Property D account received approximately $81,614,145.04 USD and $5,487,464.33 AUD, and sent out approximately $76,122,635.37 USD and $5,487,464.33 AUD.

262. Much of this activity was from high-six or seven-figure wire transfers to and from BTC-e-associated accounts at Mayzus Financial Services.

263. For example, on December 6, 2013, Defendant Property D account received a $3 million wire transfer from a Mayzus Financial Services account in Prague.

264. That wire was followed by another wire, on or about January 9, 2014, in the amount of $2.981 million from the Mayzus Prague account.

265. On May 27, 2014, the Defendant Property D account wired $3 million to a Mayzus Financial Services account.

266. A significant amount of money was also transferred from the Defendant Property D account (which was a Canton Business Corp. account at FXOpen Australia) to the Defendant Property B account (a Canton Business Corp. account at FXOpen New Zealand).

267. In total, approximately $9.57 million USD and $5.387 AUD was transferred from the Defendant Property D account to the Defendant Property B account.

268. As of August 2024, the balance of the Defendant Property D account was approximately $5,491.509.67.

L. Defendant Properties E and F

269. VINNIK successfully established bank accounts in Czechia, also known as the Czech Republic, in the name of Nano ABC, a dedicated BTC-e shell company.

270. The Nano ABC accounts included accounts denominated in USD, Euro, and Czech Koruna (CZK), though the bulk of the activity occurred through the USD accounts.

271. The accounts were used specifically to facilitate BTC-e's operation.

272. The most heavily used Nano ABC account was Account No. CZ6903000000000273635458 (Defendant Property E(i)), a USD account at the Československá obchodní banka, one of the largest commercial banks operating in Czechia.

273. A review of transaction records of the account from March 2016 to July 2017 revealed that the majority of the funds deposited into CZ6903000000000273635458 originated from Payeer LLC.

274. Payeer LLC is a digital wallet and payment platform that was one of the ways users could make deposits to BTC-e.

275. The transaction memos for the account indicated that many of the incoming payments listed invoice numbers with the reference, "For computer parts."

276. BTC-e and Nano did not sell computer parts; rather, the memos appeared intended to conceal the true nature of the activity.

277. About half of the funds transferred out of the Defendant Property E(i) account were directed to "Premium Silver," with memos referencing computer parts and invoice numbers.

278. The account also sent regular payments of $6,000 USD with references for programmer salary payments.

279. The Nano USD account was also used to fund the CZK account (CZ7803000000000273636266) (Defendant Property E(ii)) and the Euro account (CZ6703000000000273635300) (Defendant Property E(iii)).

280. The Czech and Euro accounts had minimal activity other than the transactions with the USD account.

281. On September 14, 2021, the United States District Court for the Northern District of California issued seizure warrants for funds in Defendant Properties E(i), E(ii), and E(iii) on the grounds that the funds were subject to forfeiture as property involved in and proceeds of money laundering and illegal money transmission. N.D. Cal. Case No. 3:21-mj-71476.

282. VINNIK also set up a trio of accounts under the name Nano ABC at Ceska Sporitelna, another Czech bank headquartered in Prague.

283. Similar to the Defendant Property E accounts at Československá obchodní banka, the accounts at Ceska Sporitelna included a USD account (Defendant Property F, Account No. CZ0080000000000001939292223), a Euro account, and a CZK account.

284. The Euro and CZK accounts had minimal activity and are not sought in this forfeiture order, though the deposit funding the CZK account included the name "VINNIK" in the memo field—further confirming the accounts' ties to VINNIK and BTC-e.

285. Like Defendant Property E, Defendant Property F was used to process payments tied to BTC-e's operation.

286. Memos on various payments found in Defendant Property F reference invoices, including for computer parts, as well as an explicit reference of "withdrawal from cryptocurrency."

287. Recurring $6,000 withdrawals from the account were made for the "salary of a programmer" and sent to the same bank receiving the similar wires from the Defendant Property E account.

288. These transactions indicate that Defendant Properties E and F were being used to process payments on behalf of BTC-e and to handle BTC-e operating expenses.

M. The Defendant Properties Are Criminally Tainted and are Property Involved in (or Traceable to Property Involved In) an Unlicensed Money Transmitting Business and Money Laundering Conspiracy

289. As detailed above, BTC-e was an unlicensed money transmitting business.

290. BTC-e was also a platform for pervasive money laundering.

291. BTC-e operated as a whole as a criminal enterprise, and all of its financial accounts served to further that criminal enterprise.

292. Even transactions in non-criminal proceeds on BTC-e's platform facilitated money laundering by helping to conceal or disguise criminal transactions.

293. The Defendant Properties are all criminally tainted property which were acquired as a direct result of, and/or otherwise derived from, BTC-e's criminal activity. That criminal activity included the operation of an unlicensed money transmitting business, in violation of 18 U.S.C. § 1960, and money laundering conspiracy, in violation of 18 U.S.C. § 1956.

294. In particular, with regard to the money laundering conspiracy, BTC-e as an enterprise was tainted by funds from computer hacking and intrusions, in violation of 18 U.S.C. § 1030; identity theft, in violation of 18 U.S.C. § 1028; interstate transportation of stolen property,

in violation of 18 U.S.C. § 2314; theft of government proceeds and extortion, in violation of 18 U.S.C. §§ 641 and 1951; and narcotics trafficking, in violation of 21 U.S.C. § 841.

295. Defendant Property A (see ¶ 11 above) comprise cryptocurrency in BTC-e wallets, and therefore all the funds in Defendant Property A is property that was involved in or is traceable to transactions on the BTC-e platform. As such, Defendant Property A is forfeitable as property involved in or traceable to an unlicensed money transmitting business and money laundering conspiracy. Defendant Properties A(i)-(vii) are in the custody and control of the U.S. Marshals Service. Defendant Properties A(viii)-(ix) remain at large.

296. Defendant Property B (*see* ¶ 11 above) comprise funds in accounts that were part of the BTC-e platform, and therefore all the currency in Defendant Property B is property that was involved in or is traceable to transactions on the BTC-e platform. As such, Defendant Property B is forfeitable as property involved in or traceable to an unlicensed money transmitting business and money laundering conspiracy. Defendant Property B is located in New Zealand.

297. Defendant Property C (*see* ¶ 11 above) comprise currency in VINNIK's accounts, which were used in furtherance of BTC-e's operation and which is the property that VINNIK harvested from the BTC-e platform or traceable to that property. As such, Defendant Property C is forfeitable as property involved in or traceable to property involved in an unlicensed money transmitting business and money laundering conspiracy. Defendant Property C is located in New Zealand.

298. Defendant Property D (*see* ¶ 11 above) comprise currency in accounts that were part of the BTC-e platform, and therefore all the currency in Defendant Property D is property that was involved in or is traceable to transactions on the BTC-e platform. As such, Defendant Property

D is forfeitable as property involved in or traceable to an unlicensed money transmitting business and money laundering conspiracy. Defendant Property D is located in Australia.

299. Defendant Properties E and F (*see* ¶ 11 above) comprise currency in bank accounts that were held by BTC-e and used in furtherance of BTC-e's core operations, and therefore all the currency in Defendant Properties E and F is property that was involved in or is traceable to transactions on the BTC-e platform. As such, Defendant Properties E and F are forfeitable as property involved in or traceable to an unlicensed money transmitting business and money laundering conspiracy. Defendant Properties E and F are located in Czechia (the Czech Republic).

FIRST CLAIM FOR RELIEF

18 U.S.C. § 981(a)(1)(A)

300. Paragraphs 1 through 299 above are incorporated by reference as if fully set forth herein.

301. The Defendant Properties are property that was involved in one or more transactions in violation of 18 U.S.C. § 1960 (operating an unlicensed money transmitting business), or are traceable to such property. Therefore, the Defendant Properties are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

SECOND CLAIM FOR RELIEF

18 U.S.C. § 981(a)(1)(A)

302. Paragraphs 1 through 299 above are incorporated by reference as if fully set forth herein.

303. The Defendant Properties are property that was involved in one or more transactions in violation of 18 U.S.C. § 1956(h) (money laundering conspiracy), or are traceable

to such property. Therefore, the Defendant Properties are subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, the United States of America, requests:

1. The Defendant Properties be proceeded against according to the law and the rules of this Court, and that due notice be given to all the interested parties to appear and show cause why forfeiture should not be decreed; and

2. The Court, for the reasons set forth herein, adjudge and decree that the Defendant Properties be forfeited to the United States of America and disposed of in accordance with existing laws, together with costs, and for such other relief as this Court deems proper and just.

Respectfully submitted,

DATED: June 30, 2025

MARGARET A. MOESER
CHIEF
MONEY LAUNDERING &
ASSET RECOVERY SECTION

/s/ Joshua L. Sohn
JOSHUA L. SOHN
Trial Attorney
Money Laundering and Asset Recovery Section
Criminal Division
United States Department of Justice
1400 New York Avenue NW
Washington, DC 20005
Telephone: (202) 353-2223
joshua.sohn@usdoj.gov

/s/ C. Alden Pelker
CATHERINE ALDEN PELKER
JONAS LERMAN
CLAUDIA QUIROZ
Trial Attorneys
Computer Crime and Intellectual Property Section
Criminal Division
United States Department of Justice
1301 New York Avenue NW
Washington, DC 20530
Telephone: (202) 514-1062
catherine.pelker@usdoj.gov
jonas.lerman@usdoj.gov
claudia.quiroz2@usdoj.gov

VERIFICATION

I, Leo Rovensky, a Special Agent with the Internal Revenue Service—Criminal Investigation, declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the foregoing Verified Complaint for Forfeiture *in rem* is based upon reports and information known to me and/or furnished to me by other law enforcement representatives and that everything represented herein is true and correct.

Executed on this 30th day of June 2025.

Leo Rovensky
Special Agent
Internal Revenue Service