

UNITED STATES OF AMERICA  
FINANCIAL CRIMES ENFORCEMENT NETWORK  
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	Number 2022-03
<b>Bittrex, Inc.</b>	)	
	)	

**CONSENT ORDER IMPOSING CIVIL MONEY PENALTY**

The Financial Crimes Enforcement Network (FinCEN) has conducted a civil enforcement investigation and determined that grounds exist to impose a Civil Money Penalty against Bittrex, Inc. (Bittrex) for violations of the Bank Secrecy Act (BSA) and its implementing regulations.<sup>1</sup> Bittrex admits to the Statement of Facts and Violations set forth below and consents to the issuance of this Consent Order.

**I. JURISDICTION**

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director may impose civil penalties for violations of the BSA and its implementing regulations.<sup>2</sup> At all times relevant to this Consent Order, Bittrex was a “domestic financial institution,” specifically, a “money services business” (MSB) as defined by the BSA and its implementing regulations.<sup>3</sup> As such, Bittrex was required to comply with applicable BSA regulations.

---

1 The BSA is codified at 31 U.S.C. §§ 5311-5314, 5316-5336 and 12 U.S.C. §§ 1829b, 1951-1959. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

2 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014).

3 31 C.F.R. § 1010.100(ff) (defining “money services business”).

## II. STATEMENT OF FACTS

The conduct described below took place from on or about February 13, 2014, through on or about December 7, 2018 (Relevant Time Period), unless otherwise indicated.

### A. Bittrex

Throughout the Relevant Time Period, Bittrex owned and operated a convertible virtual currency (CVC) trading platform known as “Bittrex.” The platform was primarily operated from offices located in Bellevue, Washington, and included a hosted digital wallet service for storing and transferring CVCs. Bittrex also operated as an “exchanger” of over 250 different CVCs,<sup>4</sup> including bitcoin, ether, monero, zcash, and dash.<sup>5</sup> During the Relevant Time Period, Bittrex facilitated almost 546 million trades on its platform in the United States and at times averaged over 20,000 transactions (deposits and withdrawals) through its hosted wallets daily during the Relevant Time Period, including transactions involving over \$17 billion worth of bitcoin during the Relevant Time Period.

### B. Bank Secrecy Act Requirements

The term “money services business” is defined in 31 C.F.R. §1010.100(ff) as any of the following categories of business: (1) dealers in foreign exchange; (2) check cashers; (3) issuers or sellers of traveler’s checks or money orders; (4) providers of prepaid access; (5) money transmitters; (6) U.S. Postal Service; or (7) sellers of prepaid access.<sup>6</sup> The regulations define the term “money transmitter” as a person that either “provides money transmission services” or who is otherwise “engaged in the transfer of funds.”<sup>7</sup>

4 See FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013 (explaining that exchangers of CVC are money transmitters under FinCEN’s regulations).

5 See 31 U.S.C. § 5312(a)(2)(R).

6 31 C.F.R. § 1010.100(ff). The definition also includes any “person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed [above] . . . . This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States.”

7 31 C.F.R. § 1010.100(ff)(5).

“Money transmission services” are defined in FinCEN’s regulations as “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”<sup>8</sup> Given these definitions and Bittrex’s activities within the United States, Bittrex was a “domestic financial institution,” specifically a “money services business,” operating in the United States.<sup>9</sup> As a result, Bittrex was required to comply with FinCEN’s regulations applicable to MSBs during the Relevant Time Period.

The BSA and its implementing regulations require an MSB, including a “money transmitter” like Bittrex, to develop, implement, and maintain an effective Anti-Money Laundering (AML) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.<sup>10</sup>

As of May 14, 2014, Bittrex was required to develop, implement and maintain an effective, written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance with the BSA and its implementing regulations; (b) designates an individual responsible to assure day-to-day compliance with the MSB’s AML program and all BSA regulations; (c) provides education and/or training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program.<sup>11</sup>

---

8 31 C.F.R. § 1010.100(ff)(5).

9 See 31 U.S.C. § 5312(b)(1) (defining domestic financial institution); 31 C.F.R. §§ 1010.100(ff) (defining “money services business”) and 1010.100(ff)(5) (defining “money transmitter”). FinCEN has issued interpretive guidance explaining why CVC exchangers are money transmitters. See FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” March 18, 2013; FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies,” May 9, 2019.

10 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210(a).

11 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1022.210(d) and (e) (“A [MSB] must develop and implement an [AML] program that complies with the requirements of this section on or before...the end of the 90-day period beginning on the day following the date the business is established.”).

### **C. Bittrex Failed to Develop, Implement and Maintain an Effective AML Program**

Bittrex was aware of its obligations under the BSA and its implementing regulations as an MSB, yet it failed to develop, implement, and maintain an effective AML program during the Relevant Time Period. In particular, Bittrex was required to develop and implement internal controls that were reasonably designed to assure compliance with the BSA's suspicious activity reporting requirements, but it failed to do so. For example, in 2016, Bittrex averaged 11,000 transactions (deposits and withdrawals) per day on its platform, with a daily value of approximately \$1.54 million. Instead of utilizing widely available transaction monitoring software tools to screen the transactions for suspicious activity, the company relied on two employees with minimal AML training and experience to manually review all of the transactions for suspicious activity. These manual transaction monitoring responsibilities were in addition to their other duties. Later in 2017, Bittrex's transaction volume and values increased to an average of 23,800 transactions per day with a daily value of approximately \$97.9 million, yet the company continued to rely on the same two employees to manually review all of its transactions for suspicious activity. The manual transaction monitoring process utilized by Bittrex was demonstrably ineffective. Bittrex did not file a single suspicious activity report (SAR) from its founding in 2014 through May 2017.

Bittrex did not take any steps to begin addressing its inadequate and ineffective transaction monitoring process until April 2017 when the company hired additional employees to help the two existing employees manually review thousands of transactions per day for suspicious activity. The new and existing employees were overwhelmed and the program remained highly ineffective throughout the Relevant Time Period. For example, Bittrex filed only one SAR between May 2017 and November 2017.

FinCEN's investigation revealed that Bittrex failed to detect suspicious transactions through its platform, in addition to the thousands of transactions that

were prohibited by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) as discussed below, during the Relevant Time Period. The suspicious transactions involved various types of illicit activity, including direct transactions with online darknet marketplaces such as AlphaBay, Agora, and the Silk Road 2. These markets are used to buy and sell contraband such as stolen identification data, illegal narcotics, and child pornography. The company also failed to detect, investigate and report transactions connected to ransomware attacks against individuals and small businesses in the United States during the relevant time period.

#### **D. Internal Revenue Service Examination**

In October 2017, the Internal Revenue Service (IRS) notified Bittrex that it intended to examine the company for compliance with the BSA and its implementing regulations.<sup>12</sup> A month later, Bittrex filed 119 SARs with FinCEN. Bittrex also hired additional compliance staff and began improving the development and implementation of its AML policies, procedures, and internal controls in late 2017. For example, in December 2017, Bittrex paused the opening of new customer accounts and used the pause to begin improving its Know Your Customer procedures in compliance with the BSA. Bittrex also hired its first qualified BSA officer in late 2017 to manage day-to-day compliance with the BSA. Despite these improvements and investments, the company's AML program remained seriously under-resourced and it continued to manually review tens of thousands of transactions per day for suspicious activity through December 2018.

Bittrex's failure to develop, implement, and maintain an effective AML program from February 2014 until December 2018 left its platform open to abuse by bad actors, including money launderers, terrorist financiers, and sanctions evaders.

---

<sup>12</sup> Authority to examine MSBs to determine compliance with the BSA and its implementing regulations is delegated to the IRS pursuant to 31 C.F.R. § 1010.810(b)(8).

## **E. OFAC-Prohibited Transactions**

As described above, Bittrex was required to develop, implement, and maintain an effective AML program that was reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. In 2015, and again in 2017, Bittrex adopted a written AML program that identified various money laundering risks stemming from its operations as well as policies, procedures, and controls that the company could use to mitigate those risks. One of the risks that the company identified was geographic risk, including the risk that its platform would be used to facilitate transactions subject to U.S. sanctions administered OFAC, as well as high-risk and non-cooperative jurisdictions identified by the Financial Action Task Force. In some cases, transactions that violate OFAC sanctions also constitute suspicious activity that must be reported to FinCEN.<sup>13</sup> From February 2014 through February 2016, Bittrex knew that it was required to ensure that it did not process transactions that violated OFAC sanctions, but the company failed to do so. In February 2016, Bittrex hired a third-party vendor to install and integrate software into its platform that automatically screened transactions for compliance with OFAC sanctions. However, the vendor's software only screened transactions to identify potential matches on the OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List") and other lists. The vendor's software did not begin screening some customers or transactions for a nexus to sanctioned jurisdictions until at least October 2017.

As a result, Bittrex conducted over 116,000 transactions, valued at over \$260 million, with entities and individuals located in jurisdictions subject to comprehensive OFAC sanctions during the Relevant Time Period, including transactions with entities and individuals operating openly from OFAC-sanctioned jurisdictions such as Iran, Cuba, Sudan, Syria, and the Crimea region of Ukraine. The transactions should have been investigated, blocked and reported to OFAC, or rejected, and potentially

---

<sup>13</sup> See 18 U.S.C. § 1956(a)(1)(A) (money laundering); 18 U.S.C. § 1956(a)(2)(A) (international money laundering). See also *infra* note 18.

reported to FinCEN. For example, Bittrex processed transactions with parties located in sanctioned jurisdictions that were hundreds of times larger than typical transactions for certain customers or for the customers on the platform as a whole, yet Bittrex took no action whatsoever with regard to these atypical transactions.

#### **F. Bittrex Lacked Proper Risk-Based Controls for Certain High Risk CVCs**

Effective AML programs must be risk-based and reasonably designed to address the nature and volume of the financial services provided by an MSB.<sup>14</sup> During the Relevant Time Period, Bittrex facilitated the purchase, trade, and sale of over 250 different CVCs on its platform. CVCs vary greatly and have different features that increase or decrease transparency and traceability. Certain Anonymity-Enhanced Cryptocurrencies (AECs) present unique money laundering risks and challenges for MSBs and other financial institutions seeking to comply with the BSA and its implementing regulations. Bittrex was aware of the risks and challenges presented by the AECs that were exchanged on its platform, such as monero, zcash, pivx, and dash, but the company failed to fully address the risks in practice or in the company's written AML compliance program. While Bittrex disabled privacy-enhancing features for most of the AECs it transacted in, Bittrex did not implement any other controls to manage the risks presented by AECs for which it was impossible to disable privacy-enhancing features until after the Relevant Time Period. Bittrex also failed to implement

---

<sup>14</sup> 31 C.F.R. § 1022.210(b).

appropriate policies, procedures, and internal controls to effectively mitigate the risks associated with particularly challenging AECs, such as monero, until several years after the Relevant Time Period.<sup>15</sup>

### **G. Bittrex Failed to File Suspicious Activity Reports**

The BSA and its implementing regulations require MSBs to report transactions that the MSB “knows, suspects, or has reason to suspect” are suspicious, if the transactions are conducted or attempted by, at, or through the MSB, and the transactions involve or aggregate to at least \$2,000 in funds or other assets.<sup>16</sup> A transaction is “suspicious” and requires the filing of a SAR if the MSB knows, suspects, or has reason to suspect it: (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or apparent lawful purpose, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose; or (d) involves use of the MSB to facilitate criminal activity.<sup>17</sup>

As discussed above, during the Relevant Time Period, Bittrex failed to develop and implement policies, procedures, and internal controls that were reasonably designed to assure compliance with its suspicious activity reporting obligations. Despite Bittrex’s substantial increase in transaction volume and value in 2017, Bittrex failed to develop or install widely available software tools to monitor its transactions for indicia of suspicious activity until September 2018, relying instead on a few employees with insufficient training to manually review thousands of transactions per day for

---

15 Monero’s protocol includes features that prevent tracking by using advanced programming to purposefully insert false information into every transaction on its private blockchain. The false information is impossible to separate from the valid payment details, effectively concealing sender data and completely hiding all transaction amounts. The Monero network ultimately sends funds to an auto-generated, one time use only, wallet known only to the transacting parties. It is designed to make supervisory transaction monitoring virtually impossible. Moreover, wallet addresses on monero’s private blockchain are selectively visible only when an observer has obtained a private “view key.” See The Monero Project, *Moneropedia: View Key* (last visited Sept. 30, 2022), <https://www.getmonero.org/resources/moneropedia/viewkey.html>.

16 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1022.320(a)(2).

17 31 U.S.C. § 5318(g)(1); 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv).



suspicious activity. Bittrex’s inadequate procedures and controls, and its ineffective and under-resourced transaction monitoring process, compromised its ability to identify, enhance, integrate, and analyze available and relevant information, including traceable CVC activity on public blockchains. This further undermined Bittrex’s ability to make appropriate and timely determinations regarding the suspicious nature of transactions and file SARs when appropriate.

As a result, Bittrex failed to file SARs on a significant number of transactions involving sanctioned jurisdictions. Bittrex opened hundreds of accounts on behalf of individuals located in jurisdictions subject to comprehensive OFAC sanctions programs including Iran, Syria and the Crimea region of Ukraine. Through these accounts, some individuals conducted transactions that were suspicious above and beyond the fact that they involved a comprehensively sanctioned jurisdiction. For example, Bittrex processed more than 200 transactions that involved \$140,000 worth of CVC—nearly 100 times larger than the average withdrawal or deposit on the Bittrex platform—and 22 transactions involving over \$1 million worth of CVC each. Bittrex’s failure to implement adequate procedures or controls led to its failure to identify and report these transactions to FinCEN.<sup>18</sup>

---

18 In some cases, FinCEN will deem reports filed with OFAC as sufficient to satisfy the financial institution’s SAR filing obligation. As FinCEN has explained in interpretive guidance, “reports filed with [OFAC] of blocked transactions with Specially Designated Global Terrorists, Specially Designated Terrorists, Foreign Terrorist Organizations, Specially Designated Narcotics Trafficker Kingpins, and Specially Designated Narcotics Traffickers will be deemed by FinCEN to fulfill the requirement to file [SARs] on such transactions for purposes of FinCEN’s suspicious activity reporting rules.” FinCEN, Interpretive Release 2004-02—Unitary Filing of Suspicious Activity and Blocking Reports, 69 Fed. Reg. 76,847, 76, 848 (Dec. 23, 2004). However, as FinCEN has also explained, “this interpretation does not affect a financial institution’s obligation to identify and report suspicious activity beyond the fact of the OFAC match. To the extent that the financial institution is in possession of information not included on the blocking report filed with OFAC, a separate [SAR] should be filed with FinCEN including that information. This interpretative guidance also does not affect a financial institution’s obligation to file a [SAR], even if it has filed a blocking report with OFAC, to the extent that the facts and circumstances surrounding the OFAC match are independently suspicious—and are otherwise required to be reported under existing FinCEN regulations. In those cases, the OFAC blocking report would not satisfy a financial institution’s [SAR] filing obligation.”

### III. VIOLATIONS

FinCEN has determined that Bittrex willfully violated the BSA and its implementing regulations during the Relevant Time Period with regard to its AML program and reporting of suspicious transactions.<sup>19</sup> Specifically, FinCEN has determined that Bittrex failed to develop, implement and maintain an effective AML program that was reasonably designed to prevent its CVC trading platform and hosted wallet service from being used to facilitate money laundering and the financing of terrorist activities, in violation of 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1022.210. Additionally, FinCEN has determined that Bittrex failed to accurately, and timely, report suspicious transactions to FinCEN, in violation of 31 C.F.R. § 1022.320.

### IV. ENFORCEMENT FACTORS

FinCEN has considered all of the factors outlined in its Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020.<sup>20</sup> The following factors were particularly relevant to FinCEN's evaluation of the appropriate disposition of this matter, including the decision to impose a Civil Money Penalty and the size of that Civil Money Penalty.

- Nature and seriousness of the violations, including extent of possible harm to the public and systemic nature of the violations. Bittrex's violations were serious and exposed the public to a significant risk of possible harm. Bittrex's CVC platform was facilitating thousands of high-risk transactions, yet it failed to implement appropriate policies, procedures, and internal controls to effectively manage that risk. FinCEN's investigation showed that Bittrex failed to detect,

---

<sup>19</sup> In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose.

<sup>20</sup> FinCEN, Statement on Enforcement of the Bank Secrecy Act (Aug. 18, 2020), [https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement\\_FINAL%20508.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN%20Enforcement%20Statement_FINAL%20508.pdf)

investigate, and report suspicious transactions, including transactions with sanctioned jurisdictions and darknet marketplaces. Bittrex failed to hire and train appropriate personnel to assure compliance with the BSA, and instead relied on an ineffective manual transaction review process that could not keep pace with the volume of transactions conducted through its platform. Moreover, Bittrex operated for almost three years as an MSB before filing its first SAR in May 2017, depriving law enforcement and others of critical financial intelligence used to protect national security and safeguard the financial system from illicit use. Further, because of its inadequate manual review process, the majority of SARs filed by Bittrex were filed well after the transaction dates.

- Pervasiveness of wrongdoing within the financial institution. From the beginning of Bittrex's operations in February 2014 until late 2017, Bittrex designated its Chief Executive Officer as the AML compliance officer responsible for complying with Bittrex's statutory and regulatory obligations under the BSA. This appointment was not commensurate with Bittrex's risk profile based on the volume and scope of its activity. Bittrex failed to adopt a written AML compliance program until August 2015, almost a year and half after it began operations as an MSB. The written AML program, while thorough and rigorous in many ways, did not adequately address Bittrex's overall risk environment, including the unique risks presented by some of the over 250 CVCs traded on its platform. It also failed to adequately address the geographic risks posed by its customer base, and the program was not fully implemented until December 2018. Bittrex processed tens of thousands of transactions every day, yet the company's management failed to utilize an appropriate transaction monitoring process resulting in the failure to file a significant number of SARs in a timely manner.
- History of similar violations or misconduct in general. Bittrex has not been the subject of any prior criminal, civil, or regulatory enforcement action.

- Financial gain or other benefit resulting from the violations. Bittrex increased revenue and grew its business without investing in appropriate resources, tools, and personnel to develop, implement, and maintain an effective AML compliance program. This gave the company an unfair competitive advantage in the marketplace as compared to other companies offering similar products and services that were investing in appropriate technology and personnel to comply with the BSA. The financial benefit resulting from the violations was more limited after Bittrex paused the opening of new customer accounts in December 2017 and began dedicating more resources to its compliance program.
- Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures. In late 2017, after receiving notification of an upcoming federal compliance examination, but prior to the issuance of the examination results, Bittrex began taking corrective actions to address its compliance failures. In December 2017, Bittrex hired a qualified AML compliance officer with significant BSA/AML experience. That same month, Bittrex paused new customer registrations for four months and used the pause to bolster its AML compliance program. To date, Bittrex has continued to increase compliance staffing and training, and it continues to develop and implement new policies and procedures, including the purchase and integration of several automated transaction monitoring systems. The company has also undergone independent audits by experienced auditing firms and significantly increased and improved its SAR filing quality and timeliness. After the Relevant Time Period, Bittrex compliance employees were required to take specialized training, including event driven training corresponding to regulatory changes, changes in technology, and/or the results of significant investigations. Bittrex has updated its SAR evaluation and filing procedures. The company has also contracted with a vendor to perform automated transaction monitoring for

fiat currency transactions. Bittrex also added automated CVC transaction monitoring and customer account surveillance capabilities. Bittrex also updated its OFAC blocking, rejection, and reporting procedures. Bittrex has updated its customer identification and verification processes, including a tool used to verify the authenticity of government-issued identification documents, among other enhancements. Additionally, Bittrex proactively works with U.S. government agencies on ways to improve BSA/AML compliance by virtual asset service providers. Due to the substantial investments and improvements to its compliance program after the Relevant Time Period, FinCEN is not requiring additional remedial measures as part of this Consent Order.

- Timely and voluntary disclosure of the violations to FinCEN. Bittrex did not voluntarily disclose its compliance failures to FinCEN.
- Quality and extent of cooperation with FinCEN and other relevant agencies. Bittrex has been responsive to requests for information from the IRS and FinCEN throughout the course of the IRS's examination and FinCEN's investigation. Bittrex agreed to waive any defense related to the statute of limitations for conduct occurring during the Relevant Time Period. The company's cooperation and significant investment and efforts to design and build an effective AML compliance program have led FinCEN to impose a significantly lower Civil Money Penalty than it would have otherwise imposed for Bittrex's serious and systemic violations.
- Whether another agency took enforcement action for related activity. Following a separate but parallel investigation by OFAC, Bittrex has agreed to pay approximately \$24 million to resolve OFAC's investigation into apparent violations of the Cuban Assets Control Regulations, 31 C.F.R. Part 515; the Sudanese Sanctions Regulations, 31 C.F.R. Part 538; the Syrian Sanctions

Regulations, 31 C.F.R. Part 542; Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560; and the Crimea region of Ukraine-related sanctions under Executive Order 13685. FinCEN will credit payments made by Bittrex to resolve OFAC's enforcement investigation because FinCEN's violations stem from some of the same underlying conduct.

## V. CIVIL PENALTY

FinCEN may impose a Civil Money Penalty of \$25,000 per day for willful violations of the requirement to implement and maintain an effective AML program occurring on or before November 2, 2015, and \$62,689 per day for violations occurring after that date.<sup>21</sup>

For each willful violation of a SAR reporting requirement occurring on or before November 2, 2015, FinCEN may impose a Civil Money Penalty not to exceed the greater of the amount involved in the transaction (capped at \$100,000) or \$25,000.<sup>22</sup> The per-violation cap increases to \$250,759, and the floor increases to \$62,689, for violations occurring after November 2, 2015.<sup>23</sup>

After considering all the facts and circumstances in this case, as well as the enforcement factors discussed above, FinCEN has decided to impose a Civil Money Penalty of \$29,280,829.20 in this matter. As discussed above, FinCEN will credit the \$24,280,829.20 Bittrex has agreed to pay for the OFAC violations. Accordingly, Bittrex shall make a payment of \$5,000,000 to the U.S. Department of the Treasury pursuant to payment instructions that will be transmitted to Bittrex upon execution of this Consent Order.

---

<sup>21</sup> 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

<sup>22</sup> 31 U.S.C. § 5321(a)(1).

<sup>23</sup> 31 C.F.R. § 1010.821.

## VI. CONSENT AND ADMISSIONS

To resolve this matter and only for that purpose, Bittrex admits to the Statement of Facts and Violations set forth in this Consent Order and admits to willfully violating the BSA and its implementing regulations. Bittrex consents to the use of the Statement of Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant, and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. Bittrex understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, Bittrex shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

To resolve this matter, Bittrex agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make a payment of \$5,000,000 to the U.S. Department of the Treasury pursuant to the payment instructions that will be transmitted to Bittrex upon execution of this Consent Order. If timely payment is not made, Bittrex agrees that interest, penalties, and administrative costs will accrue.<sup>24</sup> If Bittrex fails to pay the \$24,280,829.20 settlement arising out of its apparent OFAC violations, it must pay the entire \$ \$29,280,829.20 penalty imposed by this Consent Order within thirty days of default.

Bittrex understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. Bittrex understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver of Bittrex's obligation to make

---

<sup>24</sup> 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

Bittrex affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce Bittrex to agree to or approve this Consent Order, except as specified in this Consent Order.

Bittrex understands and agrees that this Consent Order implements and embodies the entire agreement between Bittrex and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. Bittrex further understands and agrees that there are no express or implied promises, representations, or agreements between Bittrex and FinCEN other than those expressly set forth or referred to in this Consent Order and that nothing in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

Bittrex understands and agrees that nothing in this Consent Order may be construed as allowing Bittrex, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

Bittrex consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, Bittrex authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.



## **VII. COOPERATION**

Bittrex shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. Bittrex understands that its cooperation pursuant to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record or other tangible evidence about which FinCEN may inquire of Bittrex. Bittrex's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

## **VIII. RELEASE**

Execution of this Consent Order and compliance with all of the terms of this Consent Order, settles all claims that FinCEN may have against Bittrex for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim that FinCEN may have for conduct by Bittrex other than the conduct described in this Consent Order during the Relevant Time Period, or any claim that FinCEN may have against any current or former director, officer, owner, or employee of Bittrex, or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct that occurs after the Relevant Time Period as described in this Consent Order.

## **IX. WAIVERS**

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to the Department of Justice.

In consenting to and approving this Consent Order, Bittrex stipulates to the terms of this Consent Order and waives:

- A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;
- B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;
- C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order, or the Civil Money Penalty, is in any way unlawful or violates the Constitution of the United States of America or any provision thereof;
- D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;
- E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law;

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administrative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. Bittrex agrees to bear its own costs and attorneys' fees.

#### **X. VIOLATIONS OF THIS CONSENT ORDER**

Determination of whether Bittrex has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against Bittrex shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, that a failure to comply with this Consent Order, or any portion thereof, has occurred, or that Bittrex has made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative proceedings; take any additional action that it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief that FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against Bittrex in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, Bittrex specifically agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time that may be applicable to the Statement of Facts in this Consent Order, until a date 180 days following Bittrex's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that Bittrex has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of Bittrex to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and

all proceedings brought by or on behalf of FinCEN. Bittrex agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements shall be treated as binding admissions, and Bittrex agrees that it shall be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of Bittrex in determining whether Bittrex has violated any provision of this Consent Order.

#### **XI. PUBLIC STATEMENTS**

Bittrex agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding or determination in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by Bittrex, or by any person under the authority, control, or speaking on behalf of Bittrex contradicts this Consent Order, and whether Bittrex has repudiated such statement.

#### **XII. RECORD RETENTION**

In addition to any other record retention required under applicable law, Bittrex agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. Bittrex agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

### **XIII. SEVERABILITY**

Bittrex agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and Bittrex shall be construed and enforced accordingly.

### **XIV. SUCCESSORS AND ASSIGNS**

Bittrex agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom Bittrex agrees to provide a copy of the executed Consent Order. Should Bittrex seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, Bittrex must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

### **XV. MODIFICATIONS AND HEADINGS**

This Consent Order can only be modified with the express written consent of FinCEN and Bittrex. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

### **XVI. AUTHORIZED REPRESENTATIVE**

Bittrex's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of Bittrex, and further represents and warrants that Bittrex agrees to be bound by the terms and conditions of this Consent Order.

## **XVII. NOTIFICATION**

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN: Associate Director, Enforcement and Compliance Division,  
Financial Crimes Enforcement Network  
P.O. Box 39  
Vienna, Virginia 22183

To Bittrex: Head of Litigation and Regulatory Affairs  
Bittrex, Inc.  
701 5th Avenue, Suite 4200  
Seattle, WA 98104-3100

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

## **XVIII. COUNTERPARTS**

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

**XIX. EFFECTIVE DATE AND CALCULATION OF TIME**

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/  
Himamauli Das Date:  
Acting Director

Consented to and Approved By:

/s/  
Richie Lai Date:  
Chief Executive Officer  
Bittrex, Inc.