October 13, 2022

FinCEN and OFAC Announce Settlements with Cryptocurrency Platform Operator Bittrex

On October 11, 2022, Treasury's Financial Crimes Enforcement Network ("FinCEN") and the Office of Foreign Assets Control ("OFAC") announced resolutions with Bittrex, Inc. ("Bittrex") for violations of the Bank Secrecy Act/AML laws and OFAC sanctions.[1] OFAC announced a $24,280,829.20 penalty, while FinCEN announced a $29,280,829.20 penalty, though FinCEN credited the full amount Bittrex agreed to pay OFAC against its own penalty, making the total amount Bittrex agreed to pay $29,280,829.20.

The combined penalties represents the largest fine yet levied by the U.S. government against a crypto business for violating sanctions.[2] This also represents the first set of coordinated enforcement actions by FinCEN and OFAC in the crypto space, and is further evidence of heightened federal government focus on crypto-related enforcement, most notably with the Justice Department's formation of a National Cryptocurrency Enforcement Team by veteran DOJ official Eun Young Choi earlier this year.[3]

Key practice notes for U.S. companies—and non-U.S. companies that engage in U.S. nexus transactions—include the following:

- Screening against OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List") is not sufficient to ensure compliance with U.S. sanctions. OFAC expects companies to use information they obtain in the normal course to screen for persons or entities located in comprehensively sanctioned jurisdictions as well.

- Entities transacting in "Anonymity-Enhanced" Cryptocurrencies ("AECs") should take care to fully address the enhanced risks posed by such currencies.

- Substantial improvements and enhancements to an entity's compliance program can help mitigate the magnitude of a penalty even if a regulator has determined that violations occurred during the relevant time period.

Bittrex is a U.S.-based owner and operator of a cryptocurrency trading platform, which facilitates trading in over 250 cryptocurrencies and includes a digital wallet service for storing and transferring various cryptocurrencies.[4] During an almost

---

1 FinCEN, "FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act," (Oct. 11, 2022), available here (the "FinCEN Press Release"); OFAC, "Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.," (Oct. 11, 2022), available here (the "OFAC Press Release").

2 David Yaffe-Bellany, *U.S. Fines Crypto Exchange a Record $24 Million for Breaking Sanctions*, New York Times (Oct. 11, 2022), available here.

3 Dep't of Justice, "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," (Feb. 17, 2022), available here.

4 FinCEN, *In the Matter of Bittrex, Inc.*, No. 2022–03, at 2, available here (the "FinCEN Consent Order").

five-year period from February 2014 through December 2018, Bittrex facilitated almost 546 million trades, including transactions involving over $17 billion worth of bitcoin.[5]

FinCEN's consent order with Bittrex focused on the inadequacy of Bittrex's compliance program and its failure to monitor and report suspicious activity. OFAC's investigation determined that Bittrex had access to IP and physical address information collected from customers at onboarding that gave it reason to know that a certain number of its customers were located in jurisdictions subject to comprehensive sanctions, including Iran, Sudan,[6] Syria and Crimea. OFAC found, however, that Bittrex did not take action to screen its customers' information for terms associated with such jurisdictions, leading to over $260 million worth of crypto-related transactions being carried out by persons apparently located in sanctioned jurisdictions from March 2014 through December 2017. OFAC's action is one of several in recent years, including in the crypto space, that have faulted organizations for their failure to adequately screen customers based on their IP addresses and other available address information.

FinCEN Consent Order

Because of its business activities, Bittrex qualified as a "money services business" ("MSB"), and was therefore required to comply with FinCEN's regulations applicable to MSBs, including the maintenance of an effective AML program.[7] FinCEN's order finds that Bittrex's transaction monitoring practices were "inadequate and ineffective." In 2016, for example, Bittrex averaged 11,000 transactions per day on its platform with a daily value of approximately $1.54 million, but rather than utilize transaction monitoring software Bittrex instead relied on "two employees with minimal AML training and experience to manually review all of the transactions for suspicious activity."[8] Further, this responsibility was in addition to the employees' other work duties. In 2017, Bittrex's daily transaction volume increased to an average of 23,800 transactions per day with a daily value of $97.9 million, yet the company's transaction monitoring practices remained unchanged.[9] Bittrex did not file a single SAR from its founding in 2014 through May 2017, and only one from May 2017 until November 2017.[10] Despite this, FinCEN's order noted that there were undetected suspicious transactions in the relevant time period that included "direct transactions with online darknet marketplaces such as AlphaBay, Agora, and the Silk Road 2," marketplaces known to be used for trading in "stolen identification data, illegal narcotics, and child pornography."[11]

The order notes that in October 2017, the IRS notified Bittrex that it would be examined for its compliance with the BSA, and that one month later Bittrex filed 119 SARs with FinCEN, and hired additional compliance staff. Its first "qualified BSA officer" was hired in late 2017, but the order notes that the AML program remained seriously under-resourced and continued to employ a manual review system through December 2018.[12]

The order also notes that Bittrex, by transacting in certain AECs that present "unique money laundering risks and challenges for MSBs," had an enhanced risk profile. The order noted the cryptocurrencies monero, zcash, pivx and dash by name, and singled

5 *Id.*

6 Sudan is no longer subject to comprehensive sanctions, though it was for the period in which the relevant violations occurred. *See* U.S. Dep't of the Treasury, "ADVISORY: Risks and Considerations for U.S. Businesses Operating in Sudan," (May 23, 2022), available here.

7 *Id.* at 2–3.

8 *Id.* at 4.

9 *Id.*

10 FinCEN Consent Order at 4.

11 *Id.* at 5.

12 *Id.*

out monero as a "particularly challenging AEC." FinCEN states that Bittrex was aware of the risks posed by such cryptocurrencies, but failed to fully address those risks either in practice or in its written compliance program.[13]

FinCEN also faulted Bittrex for failing to file SARs concerning certain sanctions violations. While Bittrex had hired a third-party vendor in 2016 to install and integrate software into its platform that would conduct some OFAC screening, the software only screened transactions to identify potential matches to lists such as the SDN List. It did not screen "customers or transactions for a nexus to sanctioned jurisdictions until at least October 2017."[14] The order notes that, 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—including Iran, Sudan, Syria and Crimea—during the relevant time period and failed to file SARs on this activity.[15]

FinCEN's consent order discussed eight of the ten enforcement factors outlined in its August 18, 2020 Statement on Enforcement of the Bank Secrecy Act.[16] On the extent of the violations and the harm to the public caused, FinCEN noted that the violations were "serious" and "exposed the public to a significant risk of possible harm," pointing to the volume of high-risk transactions, the failure to hire and train appropriate personnel, and the fact that Bittrex operated as an MSB for almost three years before filing a single SAR. The order stated that FinCEN financially benefited from its actions by gaining an unfair competitive advantage as compared to other companies that were investing in appropriate technology and personnel to comply with the BSA. The order did credit Bittrex with "substantial investments and improvements to its compliance program after the Relevant Time Period," and as a result FinCEN did not require additional remedial measures as part of the Consent Order. The order also noted that because the FinCEN violations stemmed from "some of the same underlying conduct" as was the subject of the OFAC investigation, full crediting of the OFAC penalty was appropriate.

OFAC Settlement

OFAC noted that Bittrex had available to it IP and physical address information for its customers, yet did not take appropriate steps to screen that information to determine the existence of any nexus to comprehensively sanctioned jurisdictions.[17] OFAC noted that Bittrex's compliance deficiencies led to 116,421 apparent violations of Crimea, Cuba, Iran, Sudan and Syrian sanctions.

This failure to conduct IP address screening or blocking has of late been a significant focus for OFAC in its enforcement actions. Several weeks ago, OFAC announced a $116,048 settlement with Tango Card, Inc. after OFAC determined that Tango Card had allowed transactions to occur on its platform involving persons with IP or email addresses associated with sanctioned jurisdictions.[18] OFAC's first two enforcement actions in the crypto space—against Bitpay and BitGo—also involved, among other issues, failure to screen IP addresses and other available information, such as email addresses and phone numbers, for a nexus to comprehensively sanctioned jurisdictions. OFAC's clear message is that companies are mistaken if they believe that screening against the SDN List is enough; rather, OFAC expects companies to use information they obtain in the normal course to screen for persons or entities located in comprehensively sanctioned jurisdictions as well.

We will continue to monitor enforcement actions taken and guidance issued by both FinCEN and OFAC and provide further updates as appropriate.

---

13 *Id.* at 7–8.

14 FinCEN Consent Order at 6.

15 *Id.*

16 Available here.

17 OFAC Press Release.

18 *See* Paul, Weiss, "OFAC Enforcement Action Again Highlights the Importance of IP Address Blocking; OFAC Also Issues Guidance for Instant Payments Industry," (Oct. 6, 2022), available here.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jessica S. Carey
+1-212-373-3566
jcarey@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

David Fein
+44-20-7367-1608
dfein@paulweiss.com

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Richard S. Elliott
+1-202-223-7324
relliott@paulweiss.com

Associates Patrick McCusker and Joshua Thompson contributed to this Client Alert.