DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Enforcement Release: October 11, 2022

OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs

Bittrex, Inc. ("Bittrex"), a private company based in Bellevue, Washington, that provides an online virtual currency exchange and hosted wallet services, has agreed to remit $24,280,829.20 to settle its potential civil liability for 116,421 apparent violations of multiple sanctions programs. As a result of deficiencies related to Bittrex's sanctions compliance procedures, Bittrex failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its platform to engage in approximately $263,451,600.13 worth of virtual currency-related transactions. The applicable sanctions programs generally prohibited U.S. persons from engaging in transactions with these jurisdictions. Based on internet protocol ("IP") address information and physical address information collected about each customer at onboarding, Bittrex had reason to know that these users were in jurisdictions subject to sanctions. At the time of the transactions, however, Bittrex was not screening this customer information for terms associated with sanctioned jurisdictions. The settlement amount reflects OFAC's determination that Bittrex's apparent violations were not voluntarily self-disclosed and were not egregious.

This settlement is part of a global resolution with the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). Please refer to FinCEN's Enforcement Actions page for a description of FinCEN's settlement with Bittrex.

Description of the Apparent Violations

Between predominately March 28, 2014 and December 31, 2017, Bittrex operated 1,730 accounts that processed 116,421 virtual currency-related transactions totaling approximately $263,451,600.13 in apparent violation of multiple OFAC-administered sanctions programs (the "Apparent Violations"). Bittrex's policies and procedures dating back as far as August 2015 demonstrated that the company had some understanding of OFAC sanctions regulations, including knowledge that OFAC generally prohibits U.S. persons from engaging in activity with sanctioned jurisdictions. However, Bittrex had no internal controls in place until October 2017 to screen customers or transactions for a nexus to sanctioned jurisdictions. Bittrex did not, for example, screen IP address information that indicated the customer was in a sanctioned location or physical address information provided by the customer, such as an Iranian passport or a customer who self-identified at account opening as being in Iran.

Bittrex started offering its virtual currency services in March 2014, but it had no sanctions compliance program in place until December 2015, when it began verifying customer identity. In February 2016, Bittrex went a step further and retained a third-party vendor for sanctions screening purposes, but the screening was incomplete. Until October 2017, the vendor screened transactions only for hits against OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List") and other lists but did not scrutinize customers or transactions for a nexus to sanctioned jurisdictions.

Only after OFAC issued Bittrex a subpoena in October 2017 to investigate potential sanctions violations did Bittrex realize that the vendor was not scrutinizing whether customers were in a sanctioned jurisdiction and begin restricting accounts and screening IP and other addresses associated with sanctioned locations.

Bittrex subsequently implemented a number of other remedial measures, including implementing new sanctions screening and blockchain tracing software, conducting additional sanctions compliance training, and hiring additional compliance staff. Once implemented, these remedial measures substantially curtailed the number of Apparent Violations.

Bittrex's compliance deficiencies resulted in 13,245 apparent violations of Section 1(a)(iii) of Executive Order 13685 of December 19, 2014, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine"; 321 apparent violations of the Cuban Assets Control Regulations, 31 C.F.R. §515.201; 94,634 apparent violations of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. §560.204; 222 apparent violations of the now-repealed Sudanese Sanctions Regulations (SSR), 31 C.F.R. §538.205;[1] and 7,999 apparent violations of the Syrian Sanctions Regulations, 31 C.F.R. §542.207.

Penalty Calculation and General Factors Analysis

The statutory maximum civil monetary penalty applicable in this matter is $35,773,364,108.57. OFAC determined that the Apparent Violations were not voluntarily self-disclosed and were non-egregious. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines ("Enforcement Guidelines"), the base civil monetary penalty amount applicable in this matter equals the applicable schedule amount, which is $485,616,584.00. The settlement amount of $24,280,829.20 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines.

OFAC determined the following to be **aggravating factors**:

(1) Bittrex failed to exercise due caution or care for its sanctions compliance obligations when it operated with no sanctions compliance program for nearly two years (from March 2014 until February 2016) after beginning to offer virtual currency services worldwide. Even when it did implement a sanctions compliance program, Bittrex screened only for hits against the SDN List and not for a nexus to a sanctioned location, allowing persons in jurisdictions subject to sanctions to use its platform for more than four years despite having sufficient location information to identify those customers as being in those locations.

[1] Effective October 12, 2017, pursuant to Executive Order 13761 (as amended by Executive Order 13804), U.S. persons are no longer prohibited from engaging in transactions that were previously prohibited solely under the SSR. Consistent with the revocation of these sanctions, OFAC removed the SSR from the Code of Federal Regulations on June 29, 2018. However, the revocation of the SSR does not affect past, present, or future OFAC enforcement investigations or actions related to any apparent violations of the SSR arising from activities that occurred prior to October 12, 2017.

(2) Bittrex had reason to know that some of its users were in sanctioned jurisdictions based on those users' IP addresses and physical address data.

(3) Bittrex conveyed economic benefit to thousands of persons in several jurisdictions subject to OFAC sanctions and thereby harmed the integrity of multiple OFAC sanctions programs.

OFAC determined the following to be **mitigating factors**:

(1) Bittrex has not received a penalty notice or Finding of Violation from OFAC in the five years preceding the date of the earliest transaction giving rise to the Apparent Violations.

(2) Bittrex was a small and new company at the time of most of the Apparent Violations.

(3) Bittrex provided substantial cooperation in connection with OFAC's investigation into these Apparent Violations.

(4) Most of the transactions at issue were for a relatively small amount, and the volume of Apparent Violations represents a relatively small percentage as compared to the total volume of transactions conducted by Bittrex annually.

(5) In response to the Apparent Violations, Bittrex swiftly took a series of subsequent remedial measures that significantly curtailed the Apparent Violations. In particular, Bittrex:

- blocked all IP addresses associated with a sanctioned jurisdiction;
- restricted the accounts of all account holders identified as being located in jurisdictions subject to OFAC sanctions;
- began using a new software program for sanctions-related screening;
- implemented blockchain tracing software to assist in identifying and blocking virtual currency addresses associated with persons potentially identified on OFAC's SDN List;
- hired a dedicated Chief Compliance Officer who reports directly to the Chief Executive Officer and the Board of Directors and otherwise substantially increased its compliance staff;
- implemented a standalone Sanctions Compliance Policy and has undergone additional independent audits of its sanctions compliance functions; and
- conducted additional sanctions compliance training for all relevant personnel.

Compliance Considerations

This action highlights that virtual currency companies — like all financial service providers — are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as engaging in prohibited transactions with jurisdictions subject to sanctions. To mitigate such risks, virtual currency companies should develop a tailored, risk-based sanctions compliance program. OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry notes that OFAC strongly encourages a risk-based approach to sanctions compliance because there is no single compliance program or solution suitable to every circumstance or business. An adequate compliance solution for members of the virtual currency industry will depend on a variety of factors, including the type of business involved, its size and sophistication, products and services offered, customers and counterparties, and geographic locations served, but should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

This enforcement action emphasizes the importance of new companies and those involved in emerging technologies incorporating sanctions compliance into their business functions at the outset, especially when the companies seek to offer financial services to a global customer base. As part of these controls, companies should ensure that their sanctions compliance service providers are providing services commensurate with the institution's sanctions compliance risk. More specifically, when providing services globally, screening for location information, especially when available through IP addresses and information provided by customers (such as passports or when a customer self-identifies as being from a particular country), is particularly important in mitigating the risk of providing services to individuals in jurisdictions subject to sanctions. Finally, this case highlights the value of a company quickly implementing remedial measures after becoming aware of a potential sanctions issue.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments (the "Framework") in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC's perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A. These references, as well as recent final civil penalties and enforcement information, can be found on OFAC's website at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information.

For more information regarding OFAC regulations, please visit: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.