



Bittrex, the Crypto Platform Whose Motto Is to “Trade Beyond the Trend,” Runs Into OFAC’s Trend of Strict US Sanctions Enforcement

Update

October 14, 2022 | 5 minute read

On Tuesday, the Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) announced the largest penalty against a cryptocurrency company to date for violations of U.S. sanctions programs and reporting requirements under the Bankruptcy Secrets Act (“BSA”). While making clear that OFAC will treat crypto the same as any other currency—and its brokers as any other financial institution—the settlement provides useful insight into the types of sanctions controls the agency expects crypto companies to implement, and other factors relevant to the agency’s enforcement decisions. To avoid being next in OFAC’s enforcement trend, companies should implement a compliance solution predicated on and incorporating at least five essential components: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

Bittrex is the Latest Crypto Platform Punished for Violations of U.S. Sanctions

Bittrex Inc. (“Bittrex”), a Washington-based virtual currency exchange and wallet provider, has agreed to pay \$24,280,829.20 to resolve allegations that it facilitated more than 116,000 transactions in violation of multiple country-specific sanctions programs. Namely, Bittrex failed to prevent individuals based in the Crimea region, Cuba, Iran, Sudan, and Syria from conducting roughly \$263 million in crypto transactions between 2014 and 2017.

This settlement is the latest in a string of OFAC investigations and enforcement actions. In December 2020, OFAC reached a \$98,830 settlement with BitGo over the digital asset custodian allowing residents of many of the same sanctioned jurisdictions—Crimea, Cuba, Iran, Sudan and Syria—to conduct crypto transactions between 2015 and 2019, and in February 2021 it levied a

Related People

Seth D. DuCharme

Partner

NEW YORK

+1.212.508.6165

seth.ducharme@bracewell.com

Matthew G. Nielsen

Partner

DALLAS

+1.214.758.1039

matthew.nielsen@bracewell.com

Margaret B. Beasley

Senior Counsel

NEW YORK

+1.212.508.6180

margaret.beasley@bracewell.com

Related Industries

[Technology](#)

Related Practices

[Government Enforcement &](#)

[Investigations](#)

[Cryptocurrency & Blockchain](#)

\$507,375 fine against BitPay for facilitating “approximately \$129,000 worth of digital currency-related transactions with BitPay’s merchant customers” in sanctioned areas. More recently, reports emerged in July that OFAC is investigating Kraken, the second largest cryptocurrency exchange in the United States, for similar violations as those underlying the Bittrex settlement, and in August the agency barred Americans from using Tornado Cash, a crypto platform that criminals have used to launder billions of dollars. This steady stream of enforcement actions makes clear that, like other government agencies, OFAC won’t give a free pass to newcomers in the emerging industry of cryptocurrency. At the same time, the Bittrex settlement provides insight into the types of controls crypto companies should implement, and a pathway to mitigation should they find themselves in hot water with regulators.

According to the OFAC press release, when Bittrex began operating as a global cryptocurrency exchange in 2014 it lacked any form of a sanctions compliance program. In 2015 it began verifying customer identities, and in 2016 it retained a third-party vendor to screen transactions for sanctions compliance. However, the screening procedures were incomplete; although the vendor screened for customers on the Specifically Designated National’s (SDN) list—a list of entities with which OFAC bars transactions—it did not screen for violations of OFAC’s country-specific sanctions programs, which generally prohibit U.S. persons from engaging in or facilitating certain transactions with individuals residing in designated countries. According to Treasury, Bittrex did not screen users based on accessible location information in the sanctioned countries using internet protocol addresses. As a result, Bittrex facilitated 116,421 prohibited transactions totaling approximately \$263,451,600.¹³ Particularly concerning to OFAC was that Bittrex failed to identify the violations until *after* OFAC issued a subpoena to the company in late 2017—that they were not “voluntarily self-disclosed.” “When virtual currency firms fail to implement effective sanctions compliance controls, including screening customers located in sanctioned jurisdictions, they can become a vehicle for illicit actors that threaten U.S. national security,” said Andrea Gacki, director of OFAC. “Virtual currency exchanges operating worldwide should understand both who—and where—their customers are.”

OFAC’s Recognition of Mitigating Factors for Bittrex

Despite a potential statutory maximum penalty of more than \$35 million, OFAC determined that certain mitigating factors justified a reduced penalty in this case. First, OFAC noted that at the time of the apparent violations, Bittrex was a small and new company, and that the illicit transactions made up only a small percentage of the company’s total transactions. Bittrex also received credit for cooperating with OFAC during the investigation and for swiftly implementing remedial measures that effectively curtailed any further violations. Remedial measures in this case included, among other things, blocking all IP addresses

associated with a sanctioned country, restricting the accounts of all account holders identified as being located in countries subject to OFAC sanctions, implementing a new software program for up-to-date sanctions screening, and hiring a dedicated Chief Compliance Officer and staff who report directly to senior management.

OFAC has repeatedly stated that a risk-based sanctions compliance program, tailored to the size and sophistication of the company, is critical to avoiding enforcement actions and large fines. In more recent years, OFAC has made clear—in both words and in deeds—that this requirement applies with equal force to cryptocurrency transactions, which are notoriously difficult to trace.

Recognizing the added complexities that digital currency transactions pose, OFAC published guidance detailing how the five pillars of an effective sanctions compliance program—(1) senior management commitment to developing a culture of compliance; (2) thorough and routine risk assessment; (3) defined internal controls and recordkeeping; (4) comprehensive testing and auditing of transactions; and (5) periodic training for company personnel—apply in particular to companies engaged in cross-border cryptocurrency transactions.² Specifically, OFAC recommends that cryptocurrency companies employ transaction monitoring and investigation software to identify transactions that have physical, digital wallet, or IP addresses associated with sanctioned individuals and entities or those located in a sanctioned country. To assist in this effort, OFAC has begun to collect and provide virtual currency addresses for individuals on the SDN list. Note that this list is not comprehensive and that companies should ensure their screening procedures also account for country-specific sanctions lists to avoid the same pitfalls that led to the Bittrex settlement.

FinCEN Joins the Fray

In addition, Treasury's Financial Crimes Enforcement Network ("FinCEN") announced a parallel enforcement action in which Bittrex agreed to pay more than \$29 million, \$24 million of which will be credited to settle its potential liability with OFAC. According to FinCEN, the crypto exchange failed to maintain an effective Anti Money-Laundering ("AML") program from 2014 to 2018, "resulting in significant exposure to illicit finance" through privacy coins. The regulator further alleged that Bittrex failed to document many transactions in sanctioned jurisdictions from 2014 to 2017 through suspicious activity reports ("SARs"). "For years, Bittrex's AML program and SAR reporting failures unnecessarily exposed the U.S. financial system to threat actors," said FinCEN Acting Director Himamauli Das. "Bittrex's failures created exposure to high-risk counterparties including sanctioned jurisdictions, darknet markets, and ransomware attackers. Virtual asset service providers are on notice that they must implement robust risk-based compliance programs and meet their BSA

reporting requirements. FinCEN will not hesitate to act when it identifies willful violations of the BSA.”

Conclusion & Key Takeaways

The Bittrex settlement highlights several factors key to OFAC’s sanctions decisions and makes clear that the presence of several mitigating factors will not preclude liability and steep penalties:

- Length of time the company has been in operation
- Size of the company
- When the company implemented sanctions controls
- The sufficiency of the sanctions controls based on the company’s operations and risk portfolio
- The resources dedicated to upholding the sanctions controls
- Whether the company engaged in willful blindness to potential illegal activity on the platform
- Whether the company failed to voluntarily disclose potential violations
- The proportion of the illicit transactions to the company’s overall business
- The company’s cooperation with the agency once investigations begin
- The company’s implementation of remedial measures
- The company’s track record of similar violations

Ultimately, 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. Companies should implement a compliance solution predicated on and incorporating at least five essential components: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. Companies should also adopt a plan to proactively report suspicious activity and implement remedial measures should it become apparent that controls have failed.

They say that trends come and go, but it seems that OFAC’s dedication to strict enforcement of sanctions—regardless of industry—is here to stay.

1. The transactions violated five country-specific sanctions programs, including Executive Order 13685 of December 19, 2014, “Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine”; the Cuban Assets Control Regulations, 31 C.F.R. § 515.201; the Iranian Transactions and Sanctions Regulations, 31 C.F.R.

§ 560.204; the now-repealed Sudanese Sanctions Regulations, 31 C.F.R. § 538.205; and the Syrian Sanctions Regulations, 31 C.F.R. § 542.207.

2. The five essential components of an effective sanctions compliance program are discussed in more detail in a previous [article](#) as well as in the [Framework for OFAC Compliance Commitments](#).