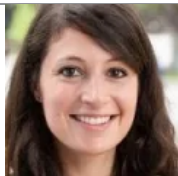


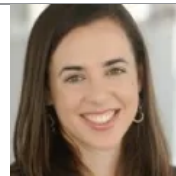
Proxy Tactics Are Changing: Can Advance Notice Bylaws Do What Poison Pills Cannot?

By John C. Coffee, Jr.



Asset Managers as Regulators

By Dorothy S. Lund



Reforming the Macroprudential Regulatory Architecture in the United States

By Kathryn Judge and Anil Kasra

Editor-At-Large
Reynolds Holding

THE CLS BLUE SKY BLOG

 COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge

[Our Contributors](#)

[Corporate Governance](#)

[Finance & Economics](#)

[M & A](#)

[Securities Regulation](#)

[Dodd-Frank](#)

[International Developments](#)

[Library & Archives](#)

Skadden Discusses First OFAC and FinCEN Parallel Enforcement Actions on Virtual Currency

By Alessio Evangelista, Eytan J. Fisch, Khalil N. Maalouf, Javier A. Urbina and Michael A. Darling November 23, 2022

Comment

On October 11, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) announced settlements for approximately \$24 million and \$29 million, respectively, with virtual currency exchange Bittrex, Inc. (Bittrex). The settlements represent the first parallel enforcement actions by FinCEN and OFAC in the virtual currency space and OFAC's largest virtual currency enforcement action to date. The investigations by OFAC and FinCEN found that the company engaged in apparent violations of several sanctions programs and willful violations of the Bank Secrecy Act's (BSA's) anti-money laundering (AML) program and suspicious activity report (SAR) filing requirements. FinCEN will credit the \$24 million payment to OFAC, resulting in a total payment of approximately \$29 million in penalties to the Treasury Department.

According to OFAC's enforcement release, Bittrex failed to prevent transactions with persons located in sanctioned countries, including when Bittrex had reason to know that users were located in sanctioned jurisdictions because it possessed information regarding users' IP and physical addresses. The release identified a number of deficiencies in Bittrex's sanctions compliance program during the relevant period, including that the third-party vendor Bittrex used for sanctions screening only screened transactions against OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) and did not otherwise screen transactions for a nexus to sanctioned jurisdictions.

According to FinCEN's consent order, Bittrex — a money services business under FinCEN's regulations — failed to maintain an effective AML program and adequately monitor transactions on its platform, resulting in exposure to illicit activity. Additionally, Bittrex's AML program did not appropriately address risks associated with its products and services, including the unique money laundering risks presented by anonymity-enhanced cryptocurrencies. Notably, Bittrex did not file any SARs between February 2014 and May 2017 and filed only one SAR between May 2017 and November 2017, despite processing an average of 11,000 transactions per day in 2016 and an average of 23,800 transactions per day by late 2017.

Key Takeaways

These parallel enforcement actions by OFAC and FinCEN demonstrate the Treasury Department's growing appetite to ensure, through enforcement, that virtual currency companies comply with U.S. AML and sanctions laws. Below is a summary of the key takeaways. Companies should:

- Maintain effective, risk-based compliance programs.** The Bittrex actions serve as a strong reminder for companies in the virtual currency space that they will be expected to implement effective sanctions compliance programs, and to the extent they are subject to the BSA, they must design and implement an AML program that meets regulatory requirements and expectations. New companies should incorporate AML and sanctions compliance into their business functions at the time of launch and should ensure that compliance resources, including staffing and technology, grow commensurately with the business. Bittrex relied on a small number of employees with little AML training to manually review thousands of transactions for suspicious activity. Additionally, companies should understand the risks that emerging technologies pose, and ensure that their compliance programs are equipped to address those risks. For instance, according to, it was not enough for Bittrex to disable the privacy-enhancing features for certain anonymity-enhanced cryptocurrencies, because doing so did not sufficiently address the broader risks posed by similar products that did not allow for such disabling. Companies should continue to reference "OFAC's Sanctions Compliance Guidance for the Virtual Currency Industry" (which we summarized in our November 10, 2021, client alert "US Treasury Provides Detailed Guidance for the Virtual Currency Industry on Sanctions Compliance") for further information about OFAC's expectations and views regarding best practices for sanctions

- compliance in this space. Companies may also want to review OFAC's May 2019 "A Framework for OFAC Compliance Commitments," which provides further information about evaluating sanctions-related risks and building a risk-based sanctions compliance program, among other things.
- **Leverage relevant data to assess sanctions risk.** OFAC highlighted as a primary deficiency that Bittrex established a sanctions compliance program in which its third-party vendor only filtered transactions against the SDN List. OFAC noted that Bittrex had IP addresses and other information that the company could have screened to detect a nexus to a sanctioned jurisdiction, but the company failed to do so. Previous OFAC enforcement actions in the virtual currency space have also focused on the failure to screen relevant information in a company's possession for sanctions risks, which further underscores OFAC's expectation that companies will implement thorough transaction and customer screening procedures. Companies should assess what customer information they possess and ensure that relevant data is being used to identify sanctions-related risks as part of their compliance procedures — regardless of whether such screening processes have been outsourced to a third-party vendor. Outsourcing compliance functions will not relieve a company of its own compliance obligations.
 - **Ensure compliance with SAR filing obligations.** FinCEN criticized Bittrex's transaction monitoring processes and its failure to file SARs during the relevant period. Companies should review their SAR reporting procedures and ensure that suspicious activity is being properly identified and reported. Further, companies should not necessarily consider their SAR filing obligations satisfied by virtue of filing blocking reports with OFAC. While the consent order states that in some instances a blocking report filed with OFAC can satisfy SAR reporting responsibilities, FinCEN explained that institutions remain obligated to report relevant information to FinCEN beyond that which they are required to include in an OFAC blocking report. A blocking report also would not satisfy a company's SAR reporting obligations in instances where the facts surrounding the OFAC match are "independently suspicious." Accordingly, the underlying activity that prompts an OFAC report should be reviewed to determine whether separate SAR reporting obligations may also apply.
 - **Implement adequate compliance tools.** FinCEN noted that Bittrex failed to utilize "widely available" transaction monitoring software tools to screen transactions, and OFAC cited Bittrex's subsequent use of a new software program for sanctions-related screening as one of the remedial measures that significantly curtailed the violations. Companies should ensure that they are technologically equipped to effectively screen transactions for suspicious activity or prohibited parties and jurisdictions and file required reports with FinCEN and OFAC as appropriate.
 - **Promptly remediate identified compliance issues.** The parallel enforcement actions also demonstrate the importance of implementing swift remedial measures when compliance issues arise. Among other things, when determining an appropriate enforcement response, OFAC and FinCEN will take into account investments in compliance programs, improvements to sanctions-related screening and transaction monitoring technology, additional compliance training and hiring of additional compliance staff. OFAC indicated that Bittrex's remediation efforts "significantly curtailed" the apparent sanctions violations and were a crucial mitigating factor in OFAC's assessment of a monetary penalty. Similarly, FinCEN expressly stated that in light of Bittrex's significant improvements to its compliance program, the company did not require additional remedial measures such as a monitor or independent consultant. Further, if a company discovers misconduct or compliance failures, it should carefully consider voluntarily self-disclosing the issue. Both OFAC and FinCEN suggested that voluntary disclosures would have constituted an additional mitigating factor, and we expect the emphasis on voluntary disclosure to grow given the Justice Department's recent corporate enforcement guidance (which we analyzed in our October 6, 2022, client alert "Revisions to the DOJ's Corporate Criminal Enforcement Policy Will Require Companies To Reevaluate Their Compliance Systems").
 - **Understand FinCEN's enforcement factors.** In August 2020, FinCEN published its "Statement on Enforcement of the Bank Secrecy Act," which set forth ten factors FinCEN will consider when evaluating the appropriate disposition of a BSA violation. The Bittrex enforcement action analyzes each of those enforcement factors and sheds light on how FinCEN will weigh them, including the nature and seriousness of the violations, how pervasive the wrongdoing was within the organization and whether a company promptly undertook and self-initiated effective remedial efforts.

The Bittrex settlements highlight the importance of implementing risk-based AML and sanctions compliance programs that can address evolving technologies and financial crime risks. Together with the recent Treasury and Justice Department reports on cryptoasset regulation (which we addressed in our September 28, 2022, client alert "Treasury and Justice Department Reports Signal Tougher Enforcement and Regulation in the Digital Assets Sector"), these actions signal that more enforcement is coming in the virtual currency space. Companies should proactively assess their existing compliance programs to ensure that they meet regulatory obligations and expectations.

This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's memorandum, "OFAC and FinCEN Announce First Parallel Enforcement Actions in the Virtual Currency Space," dated November 9, 2022, and available [here](#).