Crowell

CLIENT ALERT

FinCEN and CFTC Announce $100 Million in Regulatory Settlements With Foreign Cryptocurrency Exchange for BSA Violations and Failures to Register

August 25, 2021

On August 10, 2021, the Financial Crimes Enforcement Network ("FinCEN") and the Commodity Futures Trading Commission ("CFTC") jointly announced $100 million in civil settlements with five entities responsible for the operations of BitMEX, a foreign peer-to-peer convertible virtual currency ("CVC," or cryptocurrency) derivatives exchange. FinCEN said that the settlement represents FinCEN's first enforcement action against a futures commission merchant ("FCM"). The settlements signal continued regulatory scrutiny of cryptocurrency exchanges, particularly those based outside the U.S., for their anti-money laundering ("AML") compliance and compliance with related securities and derivatives laws.

The settlement provides important lessons about the potential exposure of non-U.S. virtual currency exchangers that transact with U.S. persons, and the expectations of the U.S. government that such entities either will take substantial measures to avoid such dealings or that they will register under appropriate U.S. authorities.

The FinCEN Civil Money Penalty

FinCEN's Findings

According to FinCEN's civil money penalty assessment ("Assessment"), BitMEX did significant business as a FCM in the U.S. from November 1, 2014 through December 12, 2020 (the "Relevant Period"), including maintaining U.S. offices, soliciting and accepting orders from U.S. persons and other individuals and entities located in the U.S. (collectively, "U.S. Customers"), actions that required it to register with the CFTC under the Commodity Exchange Act ("CEA") and subjected it to AML regulation under the Bank Secrecy Act ("BSA").

As one of the world's largest CVC derivatives exchanges, BitMEX offered leveraged trading of CVC derivatives to retail and institutional customers around the word, including U.S. Customers. Customers could deposit cryptocurrency and engage in leveraged trading of cryptocurrencies through the BitMEX website, its mobile app, and API interfaces with BitMEX's trading engine servers.

FinCEN found that BitMEX openly invited U.S. Customers until at least late 2015. Even after that, the agency found that BitMEX ignored account registration data and Internet Protocol ("IP") addresses suggesting that substantial numbers of its customers might be in the U.S. or otherwise were U.S. persons. For example, BitMEX received reports indicating that customers providing U.S. identification accounted for 4.3% of all customers in September 2018, 8% of all customers in October 2018, and 5.1% of all customers in November 2018. Reports from October 2018 indicated over 40,000 accounts whose country of registration at that time was set to the U.S., or to a sanctioned country such as Cuba, Iran, Syria, North Korea, or Sudan, or an IP address of Quebec. Another report showed 800 accounts for users located in China logged into BitMEX from U.S.-based IP addresses.

In some cases, senior employees even sought to conceal such evidence or help U.S. Customers conceal their U.S. identities. For example, BitMEX employees provided instructions to U.S. Customers to establish shell companies to trade on its platform. In one

instance, a BitMEX co-founder altered IP data about a prominent New York investor to show that the investor was located in Canada. The BitMEX co-founder apparently knew the individual was a U.S. investor but wanted to keep him on the platform because "[h]e's famous in bitcoin."

FinCEN also faulted BitMEX for failing to take steps to identify the use of virtual private networks ("VPNs") and TOR browsers to access its platform in a way that would conceal that the customers were in the U.S., or in sanctioned jurisdictions.

BSA Violations

FinCEN found that BitMEX failed to implement a written AML program despite evidence that BitMEX's founders, leadership and senior management were aware of their AML obligations to do so since the beginning of its operations. Likewise, FinCEN also assessed violations against BitMEX for willfully failing to implement a written customer identification program ("CIP"). BitMEX admitted that it never established or implemented a CIP, instead advertising that "[s]ign up takes less than 30 seconds and requires no personal information. Trade in minutes, deposits only require one confirmation." BitMEX leadership internally discussed that the company would refuse to change this policy unless it faced "significant government pressure" do so.

Finally, FinCEN penalized BitMEX for failing to file 588 suspicious activity reports ("SARs") on a wide variety of activity, including transactions with or involving: (1) known darknet markets used to launder funds from criminal activity; (2) high-risk and sanctioned jurisdictions, such as Iran; (3) virtual currency "mixers" intended to obscure the origin of virtual currency transactions and widely used for money laundering; (4) a high-risk, unregistered money transmitter, BTC-e, that was shut down in 2017 based on its alleged use for money laundering; and (5) high-risk counterparties engaged in elder fraud, pyramid schemes, and other scams. The agency noted BitMEX's failure to implement any form of transaction monitoring system to aid the detection of suspicious activity, and in particular its failure to use available blockchain analytics tools to identify such activity.

Monetary Penalty and Undertakings

FinCEN assessed, and BitMEX agreed to, a civil money penalty ("CMP") of $100 million, which would be partially satisfied by payment of BitMEX's $50 million CFTC settlement. FinCEN also agreed to suspend $10 million of the CMP pending BitMEX's compliance with a SAR lookback undertaking and U.S. controls undertaking. Specifically, BitMEX agreed to hire, at its own expense, a qualified independent consultant to review all transactions or attempted transactions during the Relevant Period to determine whether activity was properly reported as suspicious under the BSA, and to hire a qualified independent consultant to review BitMEX's policies, procedures, and user verification program to confirm they are effective and reasonably designed and implemented to ensure BitMEX is not operating in the U.S. Part of this review is to ensure BitMEX is not transacting with U.S. Customers, directly or indirectly, such users cannot access BitMEX's platform, and cannot buy, deposit, sell, or withdraw through the BitMEX platform. BitMEX must also make clear on its website and other materials that U.S. Customers are prohibited from accessing BitMEX's services and it is not soliciting specifically U.S. Customers.

The CFTC Consent Order

Background

The CFTC's settlement with BitMEX follows the agency's October 1, 2020, filing of a civil enforcement action against BitMEX and its three co-founders, charging them with operating an unregistered trading platform and violations of several CFTC regulations. Notably, the CFTC's Consent Order did not resolve its enforcement proceeding against BitMEX's three co-founders, who, along

with its former head of business operations, were separately indicted in October 2020 by the U.S. Attorney's Office for the Southern District of New York for criminal BSA violations.

CFTC's Findings

The CFTC's Consent Order contains many of the same facts as FinCEN's Assessment, including BitMEX's offering of leveraged trading of cryptocurrency to retail and institutional customers in the U.S. and around the world. The CFTC found that BitMEX offered its customers the ability to enter into commodity option transactions that were not executed on a registered board of trade and that BitMEX did not register as a foreign board of trade, as required under the CEA. The CFTC also found that BitMEX solicited or accepted orders for the purchase or sale of commodities futures, swaps, and retail commodity transactions on the BitMEX platform. This included facilitating the trading of swaps on digital assets without registering, as required with the CFTC, as a designated contract market or a swap execution facility.

The CFTC found BitMEX lacked an adequate supervisory system, including: (i) failing to implement a CIP or, in the alternative, a program that would allow it to identify U.S. persons attempting to use the BitMEX platform, (ii) failing to implement an adequate AML program to detect and prevent potential terrorist financing and criminal activity, and (iii) failing to implement procedures to identify transactions with persons subject to sanctions administered by the Treasury Department's Office of Foreign Assets Control.

Violations and Penalty

The CFTC concluded BitMEX committed six violations of the CEA: (1) executing futures transactions on an unregistered board of trade; (2) offering illegal off-exchange commodity options; (3) failing to register as a FCM; (4) failing to register as a swap execution facility or designated contract market maker; (5) failing to diligently supervise its officers, employees, and agents; and (6) failing to implement an AML program and CIP program. As part of its settlement with the CFTC, BitMEX agreed to a permanent injunction enjoining future unlawful conduct.

To resolve the CFTC's enforcement action, BitMEX agreed to pay $100 million, $50 million of which would be satisfied by payment of a CMP to FinCEN.

Practical Considerations

The FinCEN and CFTC resolutions continue the well-publicized and increasing regulatory scrutiny of digital assets businesses, especially foreign entities that transact with U.S. persons without complying with U.S. registration and other requirements.

Foreign cryptocurrency exchanges, including those that offer cryptocurrency derivatives and futures trading, should be mindful of the various U.S. regulatory obligations triggered by offering cryptocurrency trading services to U.S. persons. To the extent that foreign cryptocurrency platforms seek to avoid U.S. jurisdiction through stated policies of not offering services to U.S. persons, the BitMEX resolutions suggest that those entities must diligently execute on those policies in order to avoid regulation. The resolutions suggest not only that foreign businesses should avoid advertising or offering such services to U.S. persons, but also an expectation that such entities will screen IP addresses, user registration addresses, and other information available to them to detect and prevent transactions with U.S. Customers and, in the case of online access, take steps to guard against the use of VPNs and other methods by U.S. Customers. FinCEN also, in considering its jurisdiction over BitMEX, noted that BitMEX "conducted significant aspects of its business and maintained offices in the U.S.," explaining that BitMEX conducted its business in part through a Delaware subsidiary, was headquartered in San Francisco, California, and New York, and also operated out of

Chicago, Illinois, and Milwaukee, Wisconsin. Foreign businesses therefore may wish to consider not only their acceptance of business from U.S. Customers, but their U.S. presence more broadly.

Entities that serve U.S. Customers, or otherwise have reason to think that they may be subject to U.S. jurisdiction, may wish to revisit their approach to transaction monitoring to make sure that they are using appropriate blockchain analytic services to aid detection of suspicious activity and avoiding dealings with the types of high-risk parties highlighted by FinCEN. With respect to one of these, transactions with sanctioned jurisdictions, IP monitoring also may be useful, and this is something that OFAC separately has suggested, in a series of recent enforcement actions, that it expects digital assets companies to employ.

Finally, these actions show a continued interest by regulators and the U.S. Department of Justice in holding parties responsible in egregious cases. Given the complexities and evolving regulatory regime for digital assets, platforms should consult counsel to understand potential exposure and what options are available to mitigate potential regulatory risk.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Carlton Greene
Partner – Washington, D.C.
Phone: +1.202.624.2818
Email: cgreene@crowell.com

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1.202.624.2509
Email: cbrown@crowell.com

Anand Sithian
Counsel – New York
Phone: +1.212.895.4270
Email: asithian@crowell.com

Nicole Sayegh Succar
Counsel – New York
Phone: +1.212.803.4031
Email: nsuccar@crowell.com

Chris Murphy
Associate – New York
Phone: +1.212.895.4262
Email: cmurphy@crowell.com