

FinCEN and CFTC assess \$100 million penalty on cryptocurrency derivatives exchange

August 17, 2021 | Client Update | 5-minute read

The CFTC and FinCEN recently announced a settlement with BitMEX for \$100 million to resolve an enforcement action related to the exchange's failure to register as a futures commission merchant and failure to establish a BSA/AML compliance program.

The order

On August 10, 2021, the Financial Crimes Enforcement Network (FinCEN) and the Commodity Futures Trading Commission (CFTC) [announced](#) that the agencies had assessed a \$100 million civil monetary penalty (CMP) against BitMEX, one of the world's largest cryptocurrency derivatives exchanges.¹ BitMEX is a peer-to-peer cryptocurrency trading platform that offers its users the ability to trade cryptocurrency derivatives, including swaps, futures, and options products.

In October 2020, the CFTC filed a [complaint](#) against BitMEX for failure to, among other things: (i) register as a futures commission merchant (FCM);² (ii) register as a swap execution facility or a designated contract market;³ and (iii) implement a Bank Secrecy Act/anti-money laundering (BSA/AML) program,⁴ comply with the Customer Identification Program Rule,⁵ and file suspicious activity reports.⁶ Significantly, BitMEX allegedly failed to implement policies, procedures, and internal controls that would exclude U.S. customers from using its platform, despite knowledge that such customers could do so and that BitMEX was not in compliance with U.S. BSA/AML requirements.⁷ Notably, the three BitMEX co-founders were also charged with one count of violating the BSA and one count of conspiracy in October 2020.

To resolve the CFTC's action, BitMEX agreed to a [consent order](#) for a permanent injunction, a CMP, and other equitable relief (the Order). Pursuant to the Order, BitMEX agreed to pay a \$50 million CMP assessed by the CFTC and a \$50 million CMP assessed by FinCEN. Moreover, BitMEX agreed to:

- remove all business operations and personnel from the United States, with the limited exception of certain employees responsible only for information technology, systems maintenance, cyber threat/intelligence, security testing, security assurance functions, corresponding administrative and compliance personnel, and board member participation; and
- block all U.S. Persons, as defined in BitMEX's Know-Your-Customer (KYC) policies and procedures, from its platform, unless and until BitMEX obtains the required registrations from the CFTC.

Cryptocurrency enforcement actions

The BitMEX enforcement action, along with recent enforcement actions against other cryptocurrency-related businesses, demonstrates the increased scrutiny with which U.S. financial regulators are monitoring the cryptocurrency industry. Indeed, in a recent [speech](#) before the Aspen Security Forum, SEC Chairman Gary Gensler stated, "If this [crypto] field is going to continue, or reach any of its potential to be a catalyst for change, we better bring it into public policy frameworks."⁸ The following cases further underscore U.S. financial regulators' close scrutiny of the cryptocurrency

industry, and their willingness to use their enforcement powers to address violations related to fraud, BSA/AML compliance, sanctions compliance and unregistered securities and commodities offerings:

- On August 9, 2021, the Securities and Exchange Commission (SEC) [announced](#) that a cryptocurrency exchange agreed to pay \$10 million to settle charges for operating an online digital asset trading platform without registering with the SEC as a national securities exchange.
- On March 2, 2021, the CFTC [announced](#) that a U.S. District Judge in the Southern District of New York entered a default judgment against an individual for operating a fraudulent scheme to solicit bitcoin from members of the public. The court ordered the individual to pay more than \$571 million as a penalty for the fraudulent scheme.
- On February 18, 2021, the United States Department of the Treasury’s Office of Foreign Assets Control entered into a \$507,375 [settlement](#) with a digital currency payment processing company for apparent violations of multiple sanctions programs that resulted from deficiencies in the company’s sanctions compliance program.
- On October 19, 2020, FinCEN assessed a \$60 million [CMP](#) against the founder of a digital currency “mixer” based on violations of the BSA and its implementing regulations for operating as an unregistered money service business and failure to comply with BSA/AML laws and regulations.

Looking forward

The above-referenced cases reinforce the growing expectation among financial regulators that participants in the cryptocurrency industry, as it continues to expand and impact a broader range of consumers, must comply with the relevant financial laws and regulations. Moreover, industry participants—which include trading exchanges, decentralized finance (i.e., DeFi) and blockchain platforms—should take note of the evolving legal and regulatory landscape. For example, the U.S. Senate recently passed the [Infrastructure Investment and Jobs Act](#), which, as currently drafted, would require businesses that transmit cryptocurrency to file tax information reports, similar to the Form 1099 requirements for securities brokers. Moreover, as discussed in our recent [client update](#), FinCEN and the Federal Reserve Board have [proposed amendments](#) to the Travel Rule and Recordkeeping Rule that, among other things, would clarify the application of those rules to cryptocurrency exchanges.⁹ Finally, FinCEN has [proposed a rule](#) that would impose new reporting, recordkeeping and verification requirements on banks and MSBs whose customers are involved in certain cryptocurrency transactions involving unhosted wallets.¹⁰ Businesses and individuals operating in the cryptocurrency industry should continue to monitor regulatory developments and ensure that their respective operations comply with a rapidly evolving legal and regulatory environment.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres

+1 212 450 4724
greg.andres@davispolk.com

Robert A. Cohen

+1 202 962 7047
robert.cohen@davispolk.com

Luigi L. De Ghenghi

+1 212 450 4296
luigi.deghenghi@davispolk.com

Kendall Howell

+1 202 962 7068
kendall.howell@davispolk.com

Paul Marquardt

+1 202 962 7156
paul.marquardt@davispolk.com

Tatiana R. Martins

+1 212 450 4085
tatiana.martins@davispolk.com

Paul J. Nathanson

+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

Daniel P. Stipano

+1 202 962 7012
dan.stipano@davispolk.com

Zachary J. Zweihorn

+1 202 962 7136
zachary.zweihorn@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

- ¹ The CMP was assessed against HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited, which collectively operate as an integrated enterprise doing business as BitMEX.
- ² Under the Commodity Exchange Act (CEA), an FCM is an individual or entity that solicits or accepts orders for the purchase or sale of any commodity for future delivery on or subject to the rules of any exchange. See 7 U.S.C. § 1a(28).
- ³ Under the CEA, a swap execution facility is a trading system or platform in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants in the facility or system. See 7 U.S.C. § 1a(50).
- ⁴ A FCM is required to establish and implement a written anti-money laundering program. See 31 CFR 1026.210.
- ⁵ 31 CFR 1026.220.
- ⁶ 31 CFR 1026.320.

- ⁷ Note, the Order appears to take the view that if a non-U.S. trading platform fails to implement a BSA/AML compliance program and does not screen for customers that use virtual private networks to circumvent IP address monitoring, the ability to monitor and screen IP addresses is not a sufficient internal control.
- ⁸ SEC Chairman Gary Gensler, Remarks Before the Aspen Security Forum, Aug. 3, 2021, <https://www.sec.gov/news/speech/gensler-aspen-security-forum-2021-08-03>.
- ⁹ See 85 FR 68005
- ¹⁰ See 85 FR 83840