

**UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY**

IN THE MATTER OF:)
)
)
) **Number 2021-02**
)
HDR Global Trading Limited,)
100x Holdings Limited,)
ABS Global Trading Limited,)
Shine Effort Inc. Limited,)
HDR Global Services (Bermuda) Limited)
d/b/a BITMEX)
_____)

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited, which operate as an integrated, common enterprise doing business as BitMEX (collectively, BitMEX or Respondents) pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.¹

Without admitting or denying any factual or legal findings or conclusions herein, BitMEX has consented to the assessment of a civil money penalty and entered into a CONSENT TO THE ASSESSMENT OF CIVIL MONEY PENALTY (CONSENT) with FinCEN. Pursuant to the CONSENT, BitMEX agrees to pay a civil penalty in the amount of \$100 million and to comply with the Undertakings set forth below. The CONSENT is incorporated into this ASSESSMENT OF CIVIL MONEY PENALTY (ASSESSMENT) as if fully set forth herein.

1. The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1959 and 31 U.S.C. §§ 5311-5314, 5316-5336. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.

II. RESPONDENTS

BitMEX is a convertible virtual currency (CVC) derivatives exchange. BitMEX is part of the 100x Group, which includes 100x Holdings Limited, and is wholly owned and operated by HDR Global Trading Limited, a company incorporated in the Seychelles. As described in the Statement of Facts below, BitMEX employed personnel and conducted operations and trading through various subsidiaries and affiliates, including ABS Global Trading Limited; Shine Effort Inc. Limited; and HDR Global Services (Bermuda) Limited, in various locations and offices throughout the world, including, but not limited to, New York, San Francisco, Milwaukee, Hong Kong, Singapore, and Bermuda. Respondents operate and do business as an integrated, common enterprise, “BitMEX.”

III. JURISDICTION

FinCEN, a bureau of the United States Department of the Treasury, is the primary regulator and administrator of the BSA with overall authority for enforcement and compliance, including the assessment of civil money penalties on financial institutions that violate the BSA and implementing regulations and coordination and direction of other agencies exercising delegated authority under the BSA and its implementing regulations.²

At all times relevant to this proceeding, FinCEN has had jurisdiction over BitMEX and the matters that are the subject of and related to the CONSENT and this ASSESSMENT because BitMEX was a “financial institution”³ within the meaning of the BSA and its implementing regulations and was required to meet the statutory and regulatory obligations under the BSA and implementing regulations. Specifically, beginning on or about November 1, 2014 through on or

2. 31 U.S.C. § 5321(a); 31 C.F.R. §§ 1010.810(a), 1010.810(d); Treasury Order 180-01 (July 1, 2014).

3. See 31 CFR §§ 1010.100(t)(3); 1010.100(t)(8), 1010.100(x), 1010.100(ff)(5); 1010.100(ff)(8)(ii).

about December 12, 2020 (Relevant Time Period), BitMEX operated as a “futures commission merchant” (FCM) that was required to register with the Commodity Futures Trading Commission (CFTC) under the Commodity Exchange Act (CEA).⁴ During the Relevant Time Period, BitMEX conducted significant aspects of its business and maintained offices in the U.S., solicited and accepted orders from U.S. persons⁵ and other individuals and entities located in the United States (collectively, U.S. Customers) on commodity futures contracts and swaps, and in connection with these activities, accepted deposits and, otherwise, accepted money, securities, or property, including bitcoin, to margin, guarantee, or secure resulting trades on the BitMEX platform. In addition, while operating in substantial part in the United States, BitMEX provided money transmission services, transmitting funds for U.S. Customers by accepting currency, funds, or other value that substitutes for currency from one person and transmitting currency, funds, or other value that substitutes for currency to another location or person.⁶

Accordingly, FinCEN has jurisdiction over BitMEX and the matters contained in and related to the CONSENT and this ASSESSMENT, and FinCEN has the authority to enter into and adopt the CONSENT. BitMEX agrees not to object to or contest FinCEN’s jurisdiction and authority to enter into and adopt the CONSENT in this proceeding or any related proceedings brought by or on behalf of FinCEN based on a violation of or to enforce the CONSENT.

4. 31 C.F.R. §§ 1010.100(t)(8); 1010.100(x); *see also* 7 U.S.C. §§ 1-26 (2018).

5. 31 C.F.R. § 1010.100(iii).

6. A person doing business wholly or in substantial part in the United States that provides money transmission services is not a money services business if the person is registered with, and functionally regulated or examined by, the CFTC. 31 C.F.R. § 1010.100(ff)(8)(ii). However, BitMEX does not qualify for this exception because BitMEX was not registered with the CFTC and, therefore, BitMEX was also subject to FinCEN’s jurisdiction on this separate basis. *See* 31 CFR §§ 1010.100(t)(3); 1010.100(ff)(8)(ii).

IV. FINDINGS AND DETERMINATIONS

FinCEN has determined that during the Relevant Time Period, BitMEX willfully violated certain of its obligations under the BSA and its implementing regulations.⁷ Specifically, as described below, BitMEX willfully (a) failed to implement and maintain a compliant AML program;⁸ (b) failed to implement and maintain a compliant customer identification program (CIP);⁹ and (c) failed to report certain suspicious activity.¹⁰

A. STATEMENT OF FACTS

The following facts took place during the Relevant Time Period.

Background

BitMEX is one of the oldest and largest CVC derivatives exchanges. With more than 1.3 million accounts, BitMEX has consistently ranked among the largest by trade volume, having facilitated over a trillion U.S. dollars' worth of trades, accepted over \$11 billion in convertible virtual currency deposits, and collected over \$1 billion in fees. BitMEX offered leveraged trading of CVC derivatives to retail and institutional customers throughout the world, including to U.S. Customers, through BitMEX's website, www.bitmex.com, the BitMEX mobile app, and by direct connection to its trading engine servers via the BitMEX application programming interface (API). BitMEX specifically offered futures, options, and swaps on CVC assets such as bitcoin, ether, and litecoin, amongst others. All derivatives were settled in bitcoin, and all deposits and withdrawals were made exclusively in bitcoin.

7. In civil enforcement of the BSA under 31 U.S.C. §5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose.

8. 31 U.S.C. § 5318(h) and 31 C.F.R. § 1026.210.

9. 31 U.S.C. § 5318(l) and 31 C.F.R. § 1026.220.

10. 31 U.S.C. § 5318(g)(1) and 31 C.F.R. § 1026.320.

Two U.S. citizens and one citizen of the United Kingdom founded BitMEX. The trading platform is wholly owned and operated by HDR Global Trading Limited (HDR), a company incorporated in the Seychelles. 100x Holdings Limited describes itself as, “the holding group for HDR Global Trading Limited and its assets, including the BitMEX platform.” BitMEX operates through ABS Global Trading Limited (ABS), a subsidiary incorporated in Wilmington, Delaware, and conducted proprietary trading through the Hong Kong subsidiary of HDR, Shine Effort Inc. Limited (Shine). Certain personnel performing duties for BitMEX operate out of HDR Global Services (Bermuda) Limited (HDR Global Services) as well. HDR, 100x, ABS, Shine, and HDR Global Services operate and do business as a single, common, integrated enterprise, BitMEX, with a global presence, and has maintained employees, including maintaining at least half of its workforce, at its headquarters in San Francisco, California, and New York, and also operated out of Chicago, Illinois, Milwaukee, Wisconsin, Hong Kong, Bermuda, and Victoria, Seychelles.

BitMEX Willfully Failed to Implement an Anti-Money Laundering Program

FFCMs must have a written anti-money laundering (AML) program approved by senior management that satisfies all AML program requirements under the BSA and implementing regulations.¹¹ The AML program must include, at a minimum: i) the establishment and implementation of policies, procedures, and internal controls reasonably designed to prevent the financial institution from being used for money laundering or the financing of terrorist activities and to achieve compliance with the BSA and implementing regulations; ii) independent testing for compliance; iii) designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls of the program; iv) ongoing training of appropriate personnel; and v) appropriate risk-based procedures for conducting

11. 31 U.S.C. §§ 5318(h)(1), (2); 31 C.F.R. § 1026.210(b).

ongoing customer due diligence, including, but not limited to, understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and conducting ongoing monitoring to identify and report suspicious transactions.¹² BitMEX willfully failed to implement an AML program that met these requirements.

1. Policies, Procedures, and Controls

Throughout its operations, BitMEX failed to (1) establish and implement policies, procedures, and internal controls reasonably designed to prevent the financial institution from being used for money laundering or the financing of terrorism; (2) conduct independent testing for compliance; (3) designate an individual responsible for implementing and monitoring operations and internal controls of an AML program; (4) conduct ongoing training for appropriate persons; and (5) establish appropriate risk-based procedures for conducting ongoing customer due diligence.

BitMEX represents that, since its engagement with U.S. regulators, it has accelerated the implementation of its enhanced internal controls designed to detect and prevent suspicious transactions. BitMEX also represents that it has engaged in remedial measures, including the development of an AML program and user verification program, and it has appointed a new Chief Compliance Officer.

BitMEX's founders, executive officers, and additional senior leaders at the company were aware of their AML obligations at the beginning of its operations, including specifically how providing services to U.S. Customers could affect the company, as reflected in internal communications regarding licenses and other legal obligations. Yet throughout the Relevant Time Period, until at least late 2020, BitMEX continued to operate without establishing and implementing a written AML program approved by senior management with adequate AML policies, procedures, and internal controls.

12. 31 C.F.R. §§ 1026.210(b)(1)-(5).

For example, in an email dated October 28, 2014, just prior to the first bitcoin transactions occurring on the BitMEX platform, BitMEX's co-founder and Chief Executive Officer (CEO) discussed with his co-founders the regulatory environment as it applies to BitMEX's business model, demonstrating knowledge of both the CFTC ("this is the organization that policies [sic] derivatives in the states") and FinCEN ("this most affects us currently"). Furthermore, in this email, BitMEX's co-founder and CEO recognized the obligations financial institutions have under the different regulatory frameworks when providing services to U.S. Customers and evaluated options that "might allow us not to have to ban US customers." Despite this, BitMEX did not implement any of the requirements of an AML program when it first launched on or about November 2014.

Similarly, almost a year after it began operating, in an email dated September 20, 2015, BitMEX's co-founder and CEO stated, "CFTC rules Bitcoin is a commodity this will have an impact on our business, and our legal will advise," and "[t]he CFTC ruled through a cease and desist enforcement letter against a small Bitcoin options operator in California that Bitcoin is a commodity. This complicates the regulatory landscape because different U.S. agencies have classified Bitcoin as a commodity, currency, and property. Our legal team will be providing an opinion as to how this will affect our business." Despite knowledge of regulatory application to BitMEX's business from its inception, BitMEX did not implement appropriate policies, procedures, and controls to comply with its various obligations.

a. Warnings from Other U.S.-Based Financial Institutions

BitMEX tried to establish business relationships with other U.S.-based financial institutions subject to the BSA to support their trading liquidity. In these discussions with U.S.-based CVC exchanges, BitMEX acknowledged that they traded in commodities regulated by the CFTC. For example, BitMEX's co-founder and CEO told

his employees about an email conversation he had with a CVC exchange employee: “I shot [employee at CVC Exchange] another email about us just needing them to state we trade cftc commodities with them, will see what he comes back with.” In these communications, BitMEX made admissions to other U.S.-based financial institutions that it conducted trades in commodities regulated by the CFTC.

Many of these U.S.-based CVC exchanges directly asked about BitMEX’s AML policies, procedures, and internal controls. For example, on June 21, 2016, BitMEX’s co-founder and CEO responded to an email from a U.S.-based CVC exchanger’s onboarding form that requested compliance information, stating that, “the answer to all AML questions is no.” In response to a separate request by a different U.S.-based CVC Exchange to fill out an AML onboarding questionnaire, BitMEX’s co-founder and CEO stated, “No we don’t do any [Office of Foreign Assets Control] screening. The only country banned from our platform is the USA....we do no other [Know Your Customer] as we are not required to under Seychelles law,” and, “for non-US persons we require only a verified email address.” In response, the U.S.-based CVC Exchange decided against entering into business with BitMEX stating, “[W]e cannot allow [BitMEX] to create an account and trade on [CVC Exchange]. Should [BitMEX] amend its [Know Your Customer] and sanctions screening process, we are happy to revisit this decision.” Nevertheless, BitMEX continued to operate without appropriate policies, procedures, or internal controls in place throughout the Relevant Time Period, until at least late 2020.

2. Compliance Officer

An FCM is required to designate a person or persons responsible for implementing and monitoring the operations and internal controls of the program.¹³ Some of the core responsibilities of this person include, but are not limited to, ensuring the FCM files reports and creates and retains records, updates the compliance program

13. 31 C.F.R. § 1026.210(b)(3).

as necessary to reflect the current requirements of the BSA, and provides adequate training. Throughout the Relevant Time Period, until at least late 2020, BitMEX failed to designate a compliance officer to ensure day-to-day compliance with an AML program or any of the BSA's implementing regulations.

BitMEX's senior leadership acknowledged that it did not have appropriate compliance personnel in place and that compliance personnel were necessary. In an internal chat dated December 14, 2018, BitMEX's Chief Operating Officer asked the Head of Business Development, "are we almost done with hiring a real compliance person to take over onboarding" to which the Head of Business Development responded, "We are hiring a compliance person, not sure when that person is going to come aboard."

Nevertheless, the individual designated as responsible for compliance in 2019 failed to ensure compliance with the BSA and did not establish a formal AML program, including any policies, procedures, and internal controls or procedures to identify, detect, and report suspicious activity. BitMEX did not hire an individual responsible specifically responsible for AML compliance until October 2020.

3. Training

An FCM must provide for training of personnel,¹⁴ including training in the detection of suspicious transactions. Senior leadership acknowledged BitMEX provided no training programs or materials to BitMEX employees, and no individual was identified as responsible for BSA/AML training. As a result, BitMEX failed to train its personnel to meet recordkeeping and reporting requirements, and failed to train its personnel in identifying, monitoring, and reporting suspicious activity.

14. 31 C.F.R. § 1026.210(b)(4).

4. Independent Testing

An FCM must provide for independent review to monitor and maintain an adequate AML program.¹⁵ BitMEX did not conduct required independent testing during the Relevant Time Period.

5. Failures to Conduct Customer Due Diligence and Transaction Monitoring

FCMs must conduct both due diligence to understand the nature and purpose of customer relationships for the purpose of developing customer risk profiles, and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.¹⁶ Throughout the Relevant Time Period, until at least May 2018, BitMEX did not conduct due diligence to develop a customer risk profile or make a risk-based decision to maintain and update customer information. Instead, BitMEX chose not to conduct customer due diligence, allowed customers to create an account with only an email address, and decided not to collect, maintain, or update any customer information or supporting verification documents at all throughout the Relevant Time Period. Even after BitMEX began to put certain due diligence measures in place, until at least late 2020, they did not satisfy the BSA's due diligence requirements.

Transactions conducted in CVCs such as bitcoin are generally pseudonymous. However, certain information about past transactions and counterparties that have transacted with certain CVC wallets can be determined by applying address-clustering tools. These tools can uncover the identity of the transacting parties by linking CVC wallet addresses controlled by the same user based on the information available from the blockchain. Financial institutions utilize public information, transactional information on public, immutable CVC ledgers, and internal customer due diligence information to assist in identifying suspicious activity or patterns of suspicious activity

15. 31 C.F.R. § 1026.210(b)(2).

16. 31 C.F.R. § 1026.210(b)(5).

occurring through the financial institution. Despite the availability of such tools, BitMEX failed to implement any policies, procedures, and internal controls to review bitcoin transactions and identify potentially suspicious transactions occurring through their platform both at the time transactions took place and as new information about past transactions, customers, and counterparties became available to them.

Based on FinCEN's analysis, BitMEX's failure to conduct due diligence and transaction monitoring allowed thousands of transactions with suspicious counterparties, including numerous transactions with darknet markets; high-risk jurisdictions; unregistered MSBs offering enhanced CVC anonymity services, such as mixing services; and fraud schemes. Significantly, BitMEX failed to conduct proactive suspicious activity screening to determine whether transactions involved possible terrorist financing. When directly asked if BitMEX conducted any transaction monitoring or reporting to detect or report potential terrorist financing, the co-founder and CEO stated only, "if alerted to something from law enforcement we will assist." A financial institution may not rely solely on communications from law enforcement to satisfy its obligations to conduct ongoing monitoring to identify and report suspicious transactions.

In addition, BitMEX failed to implement additional policies, procedures, and internal controls specifically related to jurisdiction screening, including to exclude U.S. Customers from its platform. BitMEX continued to welcome openly U.S. Customers until at least late 2015. In an email sent by BitMEX's co-founder and CEO to a mailing list titled, "Bye Bye, New York State," he announced that the platform would only stop doing business in New York State effective August 16, 2015. The email did not describe the impact on customers in other U.S. states and territories.

Further, in 2015 a potential business partner for BitMEX asked the co-founder and CEO about BitMEX's "regulatory compliance landscape," asking, "do you have any particular licenses or registrations in any jurisdictions to conduct your business? Such as FinCEN, BitLicense or money transmitter licenses? Do you do business in the US (ie do you accept customers resident in the US)?" The co-founder and CEO responded, "We do not have any licenses. We are incorporated in the Seychelles, and accept customers globally except for [New York] State."

BitMEX received reports from its third-party user verification vendor reflecting that customers providing a U.S. identification accounted for 4.3% of all customers who verified their identity on BitMEX in September 2018, 8% of all customers in October 2018, and 5.1% of all customers in November 2018.

While BitMEX continued to represent that it only did business outside the U.S. – at times, representing that the U.S. was the only jurisdiction where transactions were prohibited – in practice BitMEX actively ignored signs that U.S. Customers traded on the platform and chose to overlook or alter data indicating that customers were located in the U.S. For example, a BitMEX co-founder and employee discussed user statistics for the platform and ignored signs that U.S. Customers may be accessing BitMEX in December 2018:

[BitMEX Co-Founder]

Looks pretty good, lines up w/what we talked about earlier. Will also want to talk w/the rest of the team about it. Re: the last pages where did you get that data especially re: USA traders in October? We don't have any USA traders.

[BitMEX Employee]

I meant to flag that datapoint, it was in our country revenue reports for October, figured we should purge/scrub the data of any US stuff.

[BitMEX Co-Founder]

Yeah. May be erroneous, could be corporate customers that are actually offshore or false [Internet Protocol (IP) address location] - yeah please remove[.]

In other instances, BitMEX employees guided U.S. Customers to establish shell companies to trade on the platform. For example, one BitMEX support desk ticket told a U.S. Customer “Unfortunately [sic] you will not be able to trade on our platform. However, you do have the option to set up a non-US company and open a corporate account with us.” The customer indicated they would do so.

BitMEX co-founders also directly altered customer information to mask the location of its U.S. Customers. In one such example, a BitMEX co-founder proactively altered data related to a prominent U.S.-located investor to show that they were located in Canada when, in fact, their IP address placed them in New York.

[BitMEX Head of Customer Support]

Yo. When you get a chance can you check for me [account number].”

[BitMEX Co-Founder]

Hahah that’s [U.S.-based bitcoin investor]. He’s a US based affiliate. And we kind of let him keep it as a favour. He’s famous in Bitcoin

[BitMEX Head of Customer Support]

Ok, so i dont send him an email? Can i change the country to something else?

[BitMEX Co-Founder]

I’ve just edited it to Canada

[BitMEX Head of Customer Support]

Cool

[BitMEX Co-Founder]

But yes, he has NY [IP Address]

[BitMEX Head of Customer Support]

That needs changing too please

Based on BitMEX documents and admissions by BitMEX’s employees, BitMEX further failed to implement appropriate policies, procedures, and internal controls to screen for customers that use a virtual private network (VPN) to access the trading platform and circumvent IP monitoring. When reviewing customer activities in October 2018, BitMEX identified 43,422 accounts whose country of registration at that time was set to the U.S., one of its territories, or a U.S. or U.N. sanctioned country, such as Cuba, Iran, Syria, North Korea, and Sudan, or whose IP address field at that time indicated Quebec. A separate October 2018 query conducted by BitMEX identified

over 800 accounts opened by users located in China logging in to BitMEX from U.S.-based IP addresses. In December 2018, a BitMEX employee highlighted this compliance weakness, stating to the company co-founders, “at some point we should start discussing vpn detection.”

BitMEX also failed to implement controls over its mirror website available through The Onion Router (TOR).¹⁷ While use of TOR in and of itself is not suspicious, transactions through a torrent service may be a strong indicator of potential illicit activity when no additional due diligence is conducted to determine customer identity and whether funds are derived from illegal activity. As an internet-based financial institution, BitMEX can collect specific metadata, including the IP addresses of its users. Not only did BitMEX fail to identify, assess, and mitigate the risks associated with browsers using IP anonymizers such as TOR web browsers, BitMEX deliberately assisted their customer base in doing so by providing them with a TOR webpage to conduct transactions without any additional risk-based policies, procedures, or internal controls until it stopped doing so in or around 2016.

BitMEX Willfully Failed to Implement a Customer Identification Program

An FCM is required to implement a written CIP appropriate for its size and business that, at a minimum, includes the collection and verification of specific customer information, and corresponding recordkeeping.¹⁸ By its own admission, BitMEX never established or implemented a written CIP and did not collect or verify information regarding the majority of its customers during the Relevant Time Period. In fact, BitMEX deliberately instituted policies and procedures that violated these requirements. For example, BitMEX’s registration pages advertised, “Sign up takes less than 30 seconds and requires no personal information. Trade in minutes, deposits

17. TOR is an anonymizing torrent service that directs internet traffic through a series of layers to conceal a user’s location and identity. A “mirror website” is a copy of a website that is accessible both on the traditional internet as well as through TOR.

18. 31 C.F.R. § 1026.220(a).

only require one confirmation.” BitMEX was aware that it had a regulatory obligation to collect and verify customer information, but it refused to change its policy to comply with these requirements unless “under significant government pressure.” An internal senior leadership communication in 2014 stated:

“If we start getting pressure we institute an account verification process for any accounts with balances over 10,000 USD equivalent of [bitcoin]. The documents we would require would be name, address and address proof, and copy of government ID. We should not implement this policy unless we come under significant government pressure. The stated policy should just be a valid email address.”

These policies persisted despite communications with other U.S.-based CVC exchanges that inquired about BitMEX’s CIP measures. In addition to the examples cited above, in a February 2017 email, BitMEX’s Head of Business Development stated to a U.S.-based financial institution, “We do not require any [Know Your Customer information] to deposit, withdraw, or trade.”

BitMEX Willfully Failed to File Suspicious Activity Reports

The BSA and its implementing regulations require FCMs to report a transaction conducted or attempted by, at, or through the financial institution that involves or aggregates to at least \$5,000 in funds or other assets that the financial institution “knows, suspects, or has reason to suspect”: (a) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity to violate or evade various legal obligations; (b) is designed to evade reporting requirements or any other regulations under the BSA; (c) has no business or apparent lawful purpose or is not the sort in which a particular customer would normally be expected to engage, and the FCM knows of no reasonable explanation for the transaction after examining the available facts; or (d) involves use of the FCM to facilitate criminal activity.¹⁹ An FCM must file a suspicious activity report no later than

19. 31 C.F.R. § 1026.320(a)(2).

30 calendar days after initially detecting facts that may constitute a basis for filing a suspicious activity report.²⁰

Based on FinCEN's analysis and as discussed below, at least \$209 million worth of transactions were conducted by, at, or through BitMEX with known darknet markets or unregistered MSBs providing mixing services, as well as transactions involving high-risk jurisdictions and alleged fraud schemes. Of these transactions, BitMEX failed to file a SAR on at least \$15 million through at least 588 specific transactions that exceeded the minimum threshold and were either suspicious at the time of the transaction, or became suspicious when additional information about the suspicious nature of the transactions became available to BitMEX.

1. Darknet and Other Illicit Marketplaces

BitMEX processed transactions with darknet marketplaces and other illicit markets where individuals and vendors bought and sold illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. BitMEX-hosted CVC wallet addresses transacted over 2,371 times with 17 darknet markets from May 2015 to November 2020, sending 79.52 BTC and receiving 33.44 BTC during this timeframe. These transactions included marketplaces that were shut down and seized by law enforcement, such as AlphaBay and Wall Street Marketplace. At least 26 of these direct transactions were for an amount over the \$5,000 reporting threshold. BitMEX failed to file a SAR on all 26 of these transactions.

2. High-Risk and Prohibited Jurisdictions

BitMEX failed to report suspicious transactions originating from high-risk and prohibited jurisdictions. BitMEX conducted transactions with CVC exchanges operating in jurisdictions with AML/CFT deficiencies, including jurisdictions such as

20. 31 C.F.R. § 1026.320(b)(3).

Iran,²¹ that have restrictions placed on them by the U.S. and have been the subjects of advisories issued by FinCEN and the Financial Action Task Force (FATF).²² BitMEX failed to file a SAR on at least 16 transactions, valued at \$138,189 in total, that were conducted with Iranian CVC exchanges.

3. CVC Mixing Services

Between November 2014 and November 2020, BitMEX addresses transacted at least 2,036 times with 11 unregistered MSBs that provide so-called “mixing” services. Darknet marketplaces actively promote mixers as the primary method for obfuscating bitcoin transactions. BitMEX received over \$2 million U.S. dollars’ worth of bitcoin from unregistered CVC mixers and sent over \$6 million U.S. dollars’ worth of bitcoin to

21. See “Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System (FIN-2018-A006),” October 11, 2018, <https://www.fincen.gov/sites/default/files/advisory/2018-10-12/Iran%20Advisory%20FINAL%20508.pdf>.

22. See “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2014-A009),” November 12, 2014; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2015-A001),” March 16, 2015; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2015-A002),” July 20, 2015; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2016-A001),” January 19, 2016; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2016-A002),” March 21, 2016; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2016-A004),” September 7, 2016; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2017-A001),” January 19, 2017; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2017-A002),” April 5, 2017; “Advisory on the FATF-Identified Jurisdictions with AML/CFT Deficiencies (FIN-2017-A005),” September 15, 2017; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2018-A001),” February 9, 2018; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2018-A002),” April 27, 2018; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2018-A004),” September 21, 2018; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2018-A007),” October 31, 2018; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2019-A001),” March 8, 2019; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies and Relevant Actions by the United States Government (FIN-2019-A004),” July 12, 2019; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies and Relevant Actions by the United States Government (FIN-2019-A007),” November 12, 2019; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2020-A001),” March 26, 2020; “Advisory on the Financial Action Task Force-Identified Jurisdictions with Anti-Money Laundering and Combatting the Financing of Terrorism Deficiencies (FIN-2020-A004),” July 14, 2020; and, “High-risk and other monitored jurisdictions,” FATF, <https://www.fatf-gafi.org/countries/#high-risk>, accessed January 14, 2021.

unregistered CVC mixers. This included at least 32 transfers of over \$5,000 with Helix Mixer, the subject of a publicly-available FinCEN Assessment of Civil Money Penalty imposing a \$60 million civil money penalty in October 2020.²³ BitMEX failed to file a SAR on at least 223 transactions with unregistered CVC mixers, with no evidence of a reasonable explanation for the transactions.

4. High-Risk Unregistered MSB Transactions

BTC-e was an unregistered CVC exchange before a coordinated U.S. government action in July 2017 shut it down for alleged money laundering and operating as an unlicensed money transmitter.²⁴ FinCEN assessed a \$110 million civil money penalty against BTC-e and a \$12 million civil money penalty against one of its operators, Alexander Vinnik, for violations of the BSA and its implementing regulations.²⁵

From November 2014 through November 2020, BitMEX sent and received over \$3 million worth of bitcoin from BTC-e in 133 covered transactions. BitMEX failed to file SARs on all 133 transactions.

5. Transactions Involving Alleged Fraud and Scams

BitMEX was involved in transactions with high-risk counterparties engaged in activity publicly identified as alleged fraud. BitMEX accepted and transmitted CVC for wallets containing the proceeds of potentially suspicious activity, including large-scale pyramid schemes and elder financial exploitation publicly identified as suspicious. More than 4,000 bitcoin transactions worth over \$5 million were conducted with at least 23 potentially suspicious counterparties involved in alleged fraud. At least 190 of these direct transactions were for an amount over the \$5,000 threshold, and BitMEX failed to file a SAR on any of these transactions.

23. *In the matter of Larry Dean Harmon d/b/a Helix Mixer*, Assessment of Civil Money Penalty Number 2020-02, Financial Crimes Enforcement Network, October 19, 2020.

24. *United States v. BTC-e aka Canton Business Corporation and Alexander Vinnik*, CR 16-00227 SI (N.D. Cal. Jan. 17, 2017).

25. *In the matter of BTC-e aka Canton Business Corporation and Alexander Vinnik*, Assessment of Civil Money Penalty Number 2017-03, Financial Crimes Enforcement Network (July 27, 2017).

B. VIOLATIONS

Based on the foregoing, FinCEN has determined that from at least on or about November 1, 2014 through on or about December 12, 2020, BitMEX willfully violated the BSA and implementing regulations in the following ways:

- (1) BitMEX willfully failed to implement and maintain a written AML program approved by senior management that was reasonably designed to guard against money laundering or the financing of terrorist activities, in violation of 31 U.S.C. §§ 5318(a)(2) and 5318(h)(1) and 31 C.F.R. § 1026.210;
- (2) BitMEX willfully failed to implement a written Customer Identification Program appropriate for its size and business profile, in violation of 31 U.S.C. §§ 5318(a)(2) and 5318(l)(1), and 31 C.F.R. §1026.220; and,
- (3) BitMEX willfully failed to accurately and timely report suspicious transactions, in violation of 31 U.S.C. § 5318(g), and 31 C.F.R. § 1026.320.

V. CIVIL MONEY PENALTY

A. LEGAL BACKGROUND

FinCEN may impose a civil money penalty of not more than \$59,017 for each willful violation of AML program requirements assessed on or after January 28, 2021.²⁶ A “separate violation” of the AML program requirements occurs “for each day that the violation continues.”²⁷ FinCEN may impose a civil money penalty of not more than \$59,017 for each willful violation of CIP requirements assessed on or after January 28, 2021.²⁸ The BSA states that a “separate violation” of the CIP requirements occurs “for each day that the violation continues.”²⁹ FinCEN may impose a penalty of not more than the greater of the amount involved in the transaction (but not to exceed \$236,071) or \$59,017 for each willful violation of SAR requirements assessed on or after January 28, 2021.³⁰

26. 31 U.S.C. § 5321(a)(1); 31 C.F.R. §§ 1010.820(i), 1010.821.

27. 31 U.S.C. § 5321(a)(1).

28. 31 U.S.C. § 5321(a)(1); 31 C.F.R. §§ 1010.820(i), 1010.821.

29. 31 U.S.C. § 5321(a)(1).

30. 31 U.S.C. § 5321(a)(1); 31 C.F.R. §§ 1010.820(i), 1010.821.

B. CFTC PENALTY

BitMEX is the subject of a civil enforcement action brought by the CFTC, an independent federal regulatory agency charged by Congress with the administration and enforcement of the CEA and its implementing regulations. On October 1, 2020, the CFTC filed a Complaint for Injunctive and Other Equitable Relief and Civil Money Penalties Under the Commodity Exchange Act and Commission Regulations in the U.S. District Court for the Southern District of New York against BitMEX and its founders Arthur Hayes, Ben Peter Delo, and Samuel Reed (collectively, CFTC Defendants).³¹ The CFTC claimed that the CFTC Defendants violated the CEA and its implementing regulations, including, but not limited to, by failing to register as an FCM in violation of CEA Section 4d, 7 U.S.C. § 6d (2018), and by failing to implement customer information program, Know Your Customer, and anti-money laundering procedures, in violation of Regulation 42.2, 17 C.F.R. § 42.2 (2019), which expressly requires compliance with the BSA and FinCEN's regulations.

To resolve the CFTC's action, the CFTC and BitMEX agreed to a Consent Order for Permanent Injunction, Civil Money Penalty, and Other Equitable Relief Against Defendants HDR Global Trading Limited, 100x Holdings Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited (the CFTC Order). Pursuant to the CFTC Order, BitMEX agreed to pay a \$100 million penalty, with a \$50 million payment to the CFTC, and \$50 million offset by payments made by, or amounts credited to, BitMEX pursuant to the CONSENT and this ASSESSMENT. In addition, BitMEX agreed to equitable relief, including, but not limited to, written certifications that BitMEX: (i) has removed 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, and

31. See *CFTC v. HDR Global Trading Ltd., et al.*, No. 1:20-cv-08132 (S.D.N.Y.) (Dkt. No. 1).

security assurance functions, corresponding administrative and compliance personnel, and board member participation, and (ii) has and will continue to block all U.S. Persons, as defined in BitMEX's KYC policies and procedures, from its platform, unless and until BitMEX obtains required registrations from the Commission.

C. CIVIL PENALTY DETERMINATION

Based on FinCEN's findings of fact and determinations that BitMEX willfully violated the AML program, CIP, and reporting requirements of the BSA and its implementing regulations as described in this ASSESSMENT, FinCEN has determined that grounds exist to assess a civil money penalty for these violations. FinCEN has determined that the appropriate civil money penalty in this matter is \$100 million (Civil Money Penalty) to be paid jointly and severally by HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc. Limited, and HDR Global Services (Bermuda) Limited). FinCEN has agreed to credit against the \$100 million Civil Money Penalty the payment of \$50 million to the CFTC pursuant to the CFTC Order. In addition, FinCEN has agreed to suspend \$10,000,000 of the Civil Money Penalty pending BitMEX's compliance with the SAR Lookback Undertaking (as defined in Section VI. A.), and will suspend \$10,000,000 of the Civil Money Penalty pending BitMEX's compliance with the U.S. Controls Undertaking (as defined in Section VI. B.). The suspended penalty amounts will not be due except as set forth below. Accordingly, BitMEX must make immediate payments totaling \$80 million of the Civil Money Penalty pursuant to this ASSESSMENT and the CFTC Order, respectively. Payment instructions for FinCEN are set forth below (Section VIII, *infra*).

VI. UNDERTAKINGS

By execution of the CONSENT and consent to this ASSESSMENT, BitMEX agrees to the following Undertakings:

A. SAR LOOKBACK UNDERTAKING

1. Within 30 days from the Effective Date of the CONSENT, BitMEX will hire, at its own cost, a qualified independent consultant, subject to FinCEN approval, to conduct a "SAR Lookback Review." The independent consultant will review all transactions or attempted transactions, focusing on deposits, withdrawals, or attempted deposits or withdrawals from, on, by, at, or through the BitMEX platform, that occurred during the period from November 1, 2014 through December 12, 2020 (Covered Transactions) to determine whether activity was properly identified and reported under 31 U.S.C. § 5318(g) and implementing regulations, assuming for purposes of settlement that BitMEX was subject to the Bank Secrecy Act and implementing regulations at the time of those transactions, and assuming that BitMEX and the independent consultant have agreed to appropriately calibrated blockchain analytics, with reference to BitMEX's risk profile and subject to FinCEN's approval. BitMEX and the independent consultant will provide those blockchain analytics to FinCEN for approval prior to commencement of the lookback.

2. Within four months from the date of engagement of the independent consultant and no later than December 31, 2021, the independent consultant will deliver a detailed report (SAR Lookback Report) to FinCEN and BitMEX that summarizes the methodology and findings of its review and identifies the Covered Transactions that may require a suspicious activity report (SAR) be filed pursuant to 31 U.S.C. § 5318(g) and implementing regulations. BitMEX will make interim reports, drafts, work papers, or other supporting materials available to FinCEN upon request. BitMEX will comply with the findings and recommendation from the independent consultant or FinCEN that BitMEX file SARs on any of the Covered Transactions.

3. Within 30 days of receipt of the SAR Lookback Report, BitMEX will file with FinCEN SARs regarding all of the Covered Transactions identified by the independent consultant as ones that would have required a report pursuant to 31 U.S.C. § 5318(g) and implementing regulations. The Company shall be entitled to one 60-day extension of this SAR filing deadline as of right. Any additional extensions may be granted with the written consent of FinCEN. This SAR filing will be a one-time filing by the Company as part of the settlement and does not constitute acceptance by BitMEX that it is subject to SAR filing requirements pursuant to the BSA and its implementing regulations.

4. If BitMEX fails to comply with any of the requirements of the SAR Lookback Undertaking, which shall be determined by FinCEN in its sole discretion, the \$10,000,000 suspended penalty associated with the SAR Lookback will be triggered, and Respondents, jointly and severally, will be required to pay the suspended penalty. This payment must be paid in full within 10 days of receipt of written notice by FinCEN that the suspended penalty is triggered and payment is required.

B. U.S. CONTROLS UNDERTAKINGS

1. Within 30 days of the Effective Date of the CONSENT, BitMEX will hire, at its own cost, a qualified independent consultant, subject to FinCEN approval, to conduct two reviews, including testing of BitMEX's operations, policies, procedures, and controls, including its User Verification Program, to confirm that they are effective and reasonably designed and implemented to ensure that BitMEX is not operating wholly or in substantial part in the United States, including, but not limited to, that BitMEX is not transacting with, or otherwise making purchases from or sales to U.S. Customers, either directly or indirectly; and no U.S. Customers are able to trade, transfer, convert, buy, sell, deposit, or withdraw, from, on, by, at, through, or in connection with the BitMEX platform, either directly or indirectly, including that (i)

U.S. Customers are prohibited from accessing BitMEX's services, including the BitMEX trading platform; (ii) all active users of the BitMEX platform have undergone BitMEX's user-verification process, which incorporates BitMEX's "US Persons" policy; and (iii) all U.S. Customers have in fact been blocked from trading on the platform or making deposits or withdrawals.³² In addition, testing will confirm that BitMEX has made clear on its website, blog, and account opening materials that U.S. Customers are prohibited, and BitMEX is not otherwise soliciting specifically to U.S. Customers.

2. The independent consultant will submit a written report to BitMEX and FinCEN detailing the results of its first review no later than 90 days from the Effective Date of the CONSENT and a second report no later than one year from the Effective date of the CONSENT. Interim reports, drafts, work papers, or other supporting materials will be made available to FinCEN upon request. Each report shall describe:

- a. the review performed, including the scope, methodology, and testing;
- b. the total number of U.S. Customers able to trade, transfer, convert, buy, sell, deposit, or withdraw from, on, by, at, through, or in connection with the BitMEX platform from the end of the Relevant Time Period through the date of the independent consultant's report, and information about their access to and use of the BitMEX platform, either directly or indirectly, including, but not limited to, location, duration of access, transactions by volume and value, and how they were able to access the BitMEX platform notwithstanding BitMEX policies, procedures, and controls;

32. It is understood that deposits to BitMEX-hosted wallets cannot be blocked. To the extent there are any deposits by U.S. Customers, BitMEX will not allow for the use or transfer of any funds deposited by U.S. Customers except that it will allow withdrawal of the deposited funds to the U.S. Customer's designated address outside the BitMEX platform.

- c. all activity by which BitMEX is soliciting, marketing to (as described above in Section VI. B. (1)), transacting with, or otherwise making purchases from or sales to U.S. Customers, either directly or indirectly, including quantification of such solicitation, marketing, transactions, purchases, and sales, as appropriate;
- d. all business operations of BitMEX in the United States;
- e. the conclusions reached, including an overall determination as to whether BitMEX's operations, policies, procedures, and controls, including its User Verification Program, or any portion thereof, are reasonably designed and implemented to ensure that BitMEX is not permitting any U.S. Customers to access BitMEX's services, including the BitMEX trading platform (as described above in Section VI. B (1)), soliciting or marketing to U.S. Customers (as described above in Section VI. B. (1)), or otherwise making purchases from or sales to U.S. Customers, either directly or indirectly; no U.S. Customers are able to trade, transfer, convert, buy, sell, deposit, or withdraw from, on, by, at, through, or in connection with the BitMEX platform, either directly or indirectly; and BitMEX is not operating wholly or substantial part in the United States as described above; and
- f. recommendations to address any and all deficiencies identified during the review to ensure BitMEX's operations, policies, procedures, and controls, including its User Verification Program, or any portion thereof, are reasonably designed and implemented to ensure no U.S. business, operations, and U.S. Customers as described above.

3. For each of the independent consultant's reports, upon consideration of the report, supporting information, and other relevant facts and circumstances, if FinCEN, in its sole discretion, determines that BitMEX's operations, policies, procedures, and controls, including its User Verification Program, or any portion thereof, are not effective and reasonably designed and implemented to ensure that:

- a. BitMEX is not permitting any U.S. Customers to access BitMEX's services, including the BitMEX trading platform (as described above in Section VI. B(1)); soliciting, or marketing to U.S. Customers (as described above in Section VI. B. (1)), or otherwise making purchases from or sales to U.S. Customers, either directly or indirectly;
- b. no U.S. Customers are able to trade, transfer, convert, buy, sell, deposit, or withdraw on, by, at, through, or in connection with the BitMEX platform, either directly or indirectly; and/or
- c. BitMEX is not operating in the United States,

such determination will constitute a negative finding (Negative Finding) and FinCEN will issue written notice that it has made a Negative Finding (Notice of Negative Finding).

4. BitMEX shall remediate any and all Negative Findings within 30 days of the Notice of Negative Finding pursuant to the recommendations of the independent consultant. Any extensions to the 30-day time period may be granted by the written consent of FinCEN. BitMEX will provide FinCEN written certification that it has adopted and implemented all recommendations of the independent consultant. The certification shall describe how the issue was remediated and be supported by exhibits sufficient to demonstrate compliance. BitMEX will provide further evidence of the remediation to FinCEN upon request.

5. Upon consideration of the Negative Findings and BitMEX's remediation thereof, including supporting information and relevant facts and circumstances, FinCEN, in its sole discretion, will determine whether the Negative Finding triggers payment of the \$5 million suspended penalty per report and will notify BitMEX in writing of such determination. The \$5 million penalty shall be paid pursuant to the payment instructions below (Section VIII, *infra*) within 10 days from written notice from FinCEN.

Failure to comply with either Undertaking will constitute a violation of the CONSENT. If FinCEN determines that a failure to comply with either Undertaking has occurred, FinCEN may take any additional enforcement action against BitMEX that it deems appropriate, notwithstanding the release and waivers set forth below. Additional actions taken by FinCEN may include, but are not limited to, the imposition of additional civil money penalties, seeking injunctive relief, and other remedial actions within the authorities of FinCEN.

VII. RELEVANT CONSIDERATIONS

In making the determinations as to the Civil Money Penalty and Undertakings, FinCEN considered the following:

- Nature and seriousness of the violations, including the extent of possible harm to the public and amounts involved. Since its inception in 2014, BitMEX has operated one of the largest bitcoin derivative platforms in the world without establishing any AML program, CIP, or SAR reporting regime. BitMEX openly advertised its lack of customer due diligence and even operated a TOR-based mirror site to attract customers. BitMEX processed billions of dollars' worth of bitcoin transactions and failed to file even a single SAR, denying law enforcement critical information. The extensive scope and grave seriousness of the violations weighs in favor of requiring robust remedial undertakings and the assessment of a significant financial penalty.

- Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security. Throughout its operations BitMEX failed to implement even basic AML controls, including establishing a written AML program, designating a qualified compliance officer, providing AML training to employees, conducting independent testing, and conducting customer due diligence. BitMEX also failed to establish an appropriate CIP to identify and verify customer identity. These basic program failures make it difficult to identify the true extent to which BitMEX failed to identify and report potentially suspicious transactions. FinCEN's initial assessment identified at least 588 transactions on which BitMEX should have filed a SAR. These reporting failures denied law enforcement access to critical information on transactions with darknet marketplaces, high-risk jurisdictions including Iran and Venezuela, and other illicit actors. This serious harm and widespread impact of the violations also weigh in favor of requiring robust remedial undertakings and the assessment of a significant monetary penalty.
- Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violations. BitMEX owners and senior leadership openly disregarded their obligations, despite knowing that they had regulatory obligations in the U.S. BitMEX maintained that, even in extreme instances of terrorist financing, they would not report activity unless first contacted by law enforcement. This reckless disregard of compliance obligations unnecessarily exposed the U.S. financial system to illicit activity by conducting numerous suspicious transactions with darknet marketplaces, unregistered MSBs, and mixing platforms that offered money laundering services. Violations

continued even after FinCEN issued guidance to the CVC industry in 2013 and again in 2019. Senior management never prioritized AML obligations, and BitMEX never made a risk-based decision to update and maintain customer information. Instead, senior management decided not to manage any customer information at all. This made compliance with the BSA and its implementing regulations virtually impossible, and as a result, BitMEX failed to identify and report significant suspicious transactions. The extensive knowledge and involvement of senior management in the violations weighs in favor of requiring robust remedial undertakings and the assessment of a significant monetary penalty

- History of similar violations, or misconduct in general, including prior criminal, civil, and regulatory enforcement action. Prior to this action, BitMEX had not been cited for non-compliance or charged with any violations of the BSA or its implementing regulations. The activity during the Relevant Time Period that is the subject of this action encompasses the entirety of BitMEX's operations since its inception. The extended duration of the violations for the entirety of BitMEX's operations also weighs in favor of requiring robust remedial undertakings and the assessment of a significant monetary penalty.
- Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures. BitMEX did not begin to mitigate its AML risks until approached by the U.S. government. Beginning in late 2020, BitMEX began instituting changes to its operations by developing and implementing know your customer procedures alongside the creation of a written AML program, hiring a Chief Compliance Officer, launching a user verification program, starting the removal of U.S. Customers from its accounts, and by starting to remove its domestic operations from the U.S. This work

is ongoing and to date BitMEX has not filed any suspicious activity reports with FinCEN. While FinCEN acknowledges the cooperation provided, the lack of timely and complete cooperation weighs in favor of requiring robust undertakings and the assessment of a significant monetary penalty.

- Financial gain or other benefit resulting from or attributable to the violation.
During the Relevant Time Period, BitMEX actively established and grew business with U.S. Customers, attracted users to its platform that sought to evade identification and compliance controls, and enabled myriad illicit activity to transit its platform, including but not limited to facilitating transactions with high-risk jurisdictions, darknet markets, CVC mixers, known fraud schemes, and more without establishing appropriate AML policies, procedures, and internal controls. BitMEX profited significantly via commissions and fees collected from the illicit activity transiting its platform, generating at least \$1 billion in fees on trillions of U.S. dollars' worth of trades during the Relevant Time Period. The significant benefit weighs in favor of requiring robust undertakings and the assessment of a significant monetary penalty.
- Quality and extent of cooperation with FinCEN and other relevant agencies.
BitMEX has partially cooperated with FinCEN by producing documents in response to FinCEN's Notice of Investigation. BitMEX made presentations to FinCEN regarding its remedial efforts, and agreed to toll the statute of limitations. However, on multiple occasions, BitMEX was either slow or failed to provide information to FinCEN and the CFTC. BitMEX's untimely and incomplete cooperation weighs in favor of requiring robust remedial undertakings and the assessment of a significant monetary penalty.

- Timely and voluntary disclosure of the violations. BitMEX did not voluntarily self-disclose the BSA violations to FinCEN, even after it learned it was being investigated by other government agencies. The lack of a voluntary self-disclosure by BitMEX weighs in favor of requiring robust remedial undertakings and the assessment of a significant monetary penalty.
- Systemic nature and duration of violations. BitMEX failed to establish an effective AML program, CIP, or SAR reporting since it began operations in 2014. BitMEX's continuous and systemic failure to report potentially suspicious activity has denied likely critical intelligence information for at least a six-year period. BitMEX's failure to implement any AML controls had a detrimental impact on its ability to prevent its platform from being exploited by potentially suspicious transactors. Indeed, FinCEN found that BitMEX conducted numerous potentially suspicious transactions with darknet marketplaces, scammers, individuals sanctioned by the Office of Foreign Assets Control (OFAC), and unregistered mixing platforms offering money laundering services. BitMEX's poor policies, procedures, and internal controls, as well as its lack of CIP, prevented BitMEX from even identifying these potentially suspicious transactions. The systemic and long-running nature of the violations weighs in favor of requiring robust undertakings and a significant monetary penalty.
- Penalties by other government entities. BitMEX and its founders are Defendants in a separate but parallel enforcement action brought by the CFTC, which is being resolved by BitMEX simultaneously with the CONSENT. BitMEX's founders, but not the company, were also indicted in a case brought by the United States Attorney's Office for the Southern District of New York. The indictment charges the individual defendants with intentionally violating the BSA and with conspiracy to violate the BSA.

VIII. CONSENT AND ADMISSIONS

1. To resolve this matter, and only for that purpose, BitMEX consents to the CONSENT and this ASSESSMENT, and all terms thereof as described herein, and agrees to payment of a Civil Money Penalty in the sum of \$100,000,000 (\$100 million) and compliance with the specified Undertakings.
2. Respondents, jointly and severally, shall make the payments to satisfy the Civil Money Penalty pursuant to the terms set forth above to the U.S. Department of Treasury within ten (10) days of the date of this ASSESSMENT. If timely payment is not made, interest, penalties, and administrative costs shall accrue.³³ Payment must be made pursuant to the instructions in the CONSENT.
3. BitMEX must treat the Civil Money Penalty paid under the CONSENT and this ASSESSMENT as a penalty paid to the government for all purposes and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. BitMEX understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation shall not be deemed a waiver of BitMEX's obligation to make further payments pursuant to the CONSENT and this ASSESSMENT, or a waiver of FinCEN's right to seek to compel payment of any remaining balance.
4. The CONSENT shall not in any way be construed as an admission or denial by BitMEX to the facts or conclusions described herein. BitMEX consents to the use of the findings of fact, determinations, and conclusions of law set forth in the CONSENT and this ASSESSMENT in this proceeding and in any other proceeding brought by or on behalf of FinCEN, or to which

33. 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

FinCEN is a party or claimant, and, for those limited purposes only, agrees that they shall be taken as true and correct and be given preclusive effect therein, without further proof. BitMEX does not consent, however, to the use of the CONSENT or this ASSESSMENT, or the findings or conclusions herein, as the sole basis for any other proceeding brought by or on behalf of FinCEN or to which FinCEN is a party or claimant, other than: a proceeding in bankruptcy or receivership; or a proceeding to enforce the terms of the CONSENT and this ASSESSMENT. BitMEX understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it in connection with this proceeding, including any proceeding in which FinCEN (or the United States on FinCEN's behalf) seeks civil money penalties or equitable remedies, BitMEX will be precluded from disputing the facts set forth in the Statement of Facts and any other determination in the CONSENT or this ASSESSMENT. BitMEX does not consent to the use of the CONSENT or this ASSESSMENT, or the findings or conclusions herein, by any other party in any other proceeding.

5. BitMEX recognizes and states that it entered into the CONSENT and consents to this ASSESSMENT freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce BitMEX to enter into the CONSENT or consent to this ASSESSMENT, except for those specified in the CONSENT.
6. BitMEX understands and agrees that nothing in the CONSENT or this ASSESSMENT may be construed as allowing BitMEX, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

7. BitMEX understands and agrees that the CONSENT embodies the entire agreement between Respondents and FinCEN, and its terms relate only to this enforcement matter (and any related proceeding) and the facts and determinations contained herein. BitMEX further understands and agrees that there are no express or implied promises, representations, or agreements between Respondents and FinCEN other than those expressly set forth or referred to in the CONSENT and that nothing in the CONSENT or in this ASSESSMENT is binding on any other law enforcement or regulatory agency of government or other authorities, whether foreign, Federal, State, local.
8. Respondents consent to the continued jurisdiction of the courts of the United States over each of them, respectively, and waive any defense based on lack of subject matter or personal jurisdiction, for the purpose of enforcing the terms and conditions of the CONSENT and this ASSESSMENT or for any other purpose relevant to this action, even if Respondents now or in the future resides outside the jurisdiction of the United States. Solely in connection with an action filed by or on behalf of FinCEN to enforce the CONSENT and this ASSESSMENT and for any other purpose relevant to this action, Respondents authorize and agree to accept all service of process and filings through the Notification procedures below on behalf of each of the Respondents, respectively, and waive formal service of process.

IX. COOPERATION

Upon FinCEN's request, Respondents shall truthfully disclose to FinCEN all factual information and provide all data, documents, and materials in its possession, custody, or control, not protected by a valid claim of attorney-client privilege or work product doctrine, with respect to BitMEX and/or the conduct of its current or former directors, officers, employees, agents, affiliated entities or individuals, or others in any matter related to or arising from this matter brought by or on behalf of FinCEN.

X. RELEASE

Execution of the CONSENT, upon it being effective, and compliance with all of the terms of the CONSENT and this ASSESSMENT, settles all claims that FinCEN may have against BitMEX for the conduct described in the Statement of Facts of the CONSENT and this ASSESSMENT during the Relevant Time Period. Execution of the CONSENT, and compliance with the terms of this ASSESSMENT and the CONSENT, does not release any claim that FinCEN may have for conduct by BitMEX other than the conduct described in the Statement of Facts of the CONSENT and this ASSESSMENT during the Relevant Time Period, or any claim that FinCEN may have against any current or former director, officer, owner, or employee of BitMEX, or any individual or entity other than those named in this ASSESSMENT. In addition, neither the CONSENT nor this ASSESSMENT provides any protection against an investigation, enforcement action, penalty assessment, or injunction relating to any conduct that occurs after the Effective Date of the CONSENT.

XI. VIOLATIONS OF THE CONSENT

If FinCEN determines, in its sole discretion, that a failure to comply with the CONSENT or this ASSESSMENT, or any portion thereof, has occurred, FinCEN may void any and all releases or waivers contained in the CONSENT, reinstitute enforcement proceedings or take any additional enforcement action against any or all Respondents that it deems appropriate, and pursue any and all violations and maximum penalties and other relief that may apply to the conduct at issue, even if not sought or assessed against BitMEX in the CONSENT or this ASSESSMENT and notwithstanding the releases and waivers herein. Determination of whether BitMEX has failed to comply with the CONSENT or this ASSESSMENT and whether to pursue any enforcement action against any or all Respondents shall be in FinCEN's sole discretion, and Respondents each expressly agrees to waive any statute of limitations or other defense

based on the passage of time that may apply, and any such statute of limitations and other time-related defenses are hereby tolled from the Effective Date of the CONSENT, except as to claims already time barred as of the Effective Date of the CONSENT.

Additional actions taken by or on behalf of FinCEN may include, but are not limited to, the imposition of additional civil money penalties to the maximum extent available, seeking injunctive relief, and other remedial actions within the authorities of FinCEN.

In the event that FinCEN determines that BitMEX has failed to comply with the CONSENT or this ASSESSMENT, all statements made by or on behalf of BitMEX to FinCEN, whether prior or subsequent to the CONSENT, shall be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN, and BitMEX shall not assert any claim under the United States Constitution, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director, officer, or employee, or any person acting on behalf of, or at the direction of BitMEX will be imputed to BitMEX for the purpose of determining whether BitMEX has violated any provision of the CONSENT or this ASSESSMENT shall be in the sole discretion of FinCEN.

XII. PUBLIC STATEMENTS

BitMEX expressly agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf, make any public statement contradicting any terms of the CONSENT or this ASSESSMENT, including any fact in the Statement of Facts section of the CONSENT and this ASSESSMENT. If a contradictory statement is made, BitMEX may avoid a breach of the CONSENT and violation of this ASSESSMENT by repudiating such statement, in writing, in the forum or proceedings in which the statements are made, or

some other forum identified at FinCEN's discretion, within 48 hours of notification by FinCEN. The foregoing restrictions do not apply to any statement made by any current or former officer, director, employee, or agent of BitMEX in the course of any criminal, regulatory, or civil case initiated against such individual, unless such individual is speaking on behalf of BitMEX, or BitMEX later ratifies such statements, directly or indirectly. Nothing in this provision shall affect BitMEX's right to take positions in other criminal or civil proceedings to which FinCEN (or the United States on FinCEN's behalf) is not a party, so long as any position BitMEX takes in a separate proceeding does not inaccurately describe the CONSENT and the related proceedings.

FinCEN has sole discretion to determine whether any statement is made by, on behalf of, or ratified by BitMEX, either directly or indirectly, whether such statement is contradictory, and whether BitMEX has in fact repudiated such statement.

XIII. RECORD RETENTION

In addition to any other record retention required under applicable law, BitMEX agrees to retain all documents and records required to be prepared or recorded under the CONSENT or otherwise necessary to demonstrate full compliance with each provision of the CONSENT or this ASSESSMENT, including supporting data and documentation. BitMEX agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them longer under applicable law.

XIV. SEVERABILITY

BitMEX agrees that if any of the provisions of the CONSENT or this ASSESSMENT are considered unenforceable by any court of competent jurisdiction, such unenforceability shall not render unenforceable the entire CONSENT or ASSESSMENT. Rather, the entire CONSENT or ASSESSMENT shall be construed as if not containing the particular unenforceable provision(s), and the right and obligations of the FinCEN and BitMEX shall be construed and enforced accordingly.

XV. SUCCESSORS AND ASSIGNS

BitMEX agrees that the provisions of the CONSENT and this ASSESSMENT shall be binding on its owners, directors, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom it will provide a copy of the executed CONSENT and this ASSESSMENT. Should BitMEX seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of the CONSENT and this ASSESSMENT, BitMEX must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with the CONSENT and this ASSESSMENT.

XVI. HEADINGS

The headings in this ASSESSMENT are inserted for convenience only and are not intended to affect the meaning or interpretation of this ASSESSMENT or its individual terms.

XVII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by the CONSENT or this ASSESSMENT, they shall be made in writing and sent via first-class mail and simultaneous email, to the contacts listed in the CONSENT.

Notices submitted pursuant to this paragraph shall be deemed effective upon receipt unless otherwise provided in the CONSENT, this ASSESSMENT, or approved by FinCEN in writing.

