



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Enforcement Release: NOVEMBER 21, 2023

**OFAC Settles with Binance Holdings, Ltd. for \$968,618,825
Related to Apparent Violations of Multiple Sanctions Programs**

Binance Holdings, Ltd. (“Binance”), a Cayman Islands virtual currency exchange with affiliates around the world, has agreed to pay \$968,618,825 to settle its potential civil liability for 1,667,153 apparent violations of multiple sanctions programs administered by the Office of Foreign Assets Control (OFAC). For over five years, between August 2017 and October 2022, Binance matched and executed virtual currency trades on its online exchange platform between U.S. person users and users in sanctioned jurisdictions or blocked persons. Although Binance took steps to project an image of compliance, including by misleading third parties about its controls, senior Binance management knew of and permitted the presence of both U.S. and sanctioned jurisdiction users on its platform, and did so despite understanding that Binance’s trade matching algorithm could cause violations of OFAC-administered sanctions programs due to the presence of U.S. users on the platform. In addition to disregarding known sanctions risks, Binance management also took steps to undermine its own compliance function, encouraging users to circumvent the company’s own ostensible controls.

In doing so, Binance (i) engaged in the direct or indirect exportation or other supply of goods and services from the United States, or by U.S. persons, to sanctioned jurisdictions and (ii) caused U.S. persons to engage, directly or indirectly, in transactions with users in sanctioned jurisdictions and with blocked persons (the “Apparent Violations”). The settlement amount reflects OFAC’s determination that the Apparent Violations were not voluntarily self-disclosed and that Binance’s conduct was egregious. The settlement amount also reflects Binance’s settlements with the Department of Justice (DOJ), the Financial Crimes Enforcement Network (FinCEN), and the Commodity Futures Trading Commission (CFTC), as well as the company’s agreement to retain an Independent Compliance Monitor (the “Monitor”) for five years, whose scope of work will include sanctions compliance.

Description of the Apparent Violations

Binance Structure and Operations

Binance was founded in 2017, and by March 2018 was running the largest virtual currency exchange in the world by trading volume. Binance’s primary online virtual currency exchange is operated on the Binance.com platform where users may trade fiat or virtual currency (e.g., bitcoin) through a variety of arrangements, including spot, futures, derivatives, and margin trading. To use Binance, a user must first open a Binance account and then fund the account by depositing assets, either through a virtual currency or fiat currency deposit. Upon onboarding, Binance users can transact in hundreds of virtual currencies and financial products using the funds in their Binance-

hosted wallets. Binance user funds are held in omnibus digital wallets that are visible on the blockchain. Users' funds are accounted for via an internal Binance ledger, and Binance acts as the custodian of user funds.

In general, Binance users trade by submitting orders to Binance to buy or sell virtual currency or virtual currency products. Binance's algorithmic matching engines ingest incoming buy/sell orders and match them with pending orders on Binance's orderbook solely according to price and time. Binance then records each transaction in its internal ledger and credits or debits users' Binance accounts to reflect the transaction. Transactions between Binance users do not occur on, and are not recorded on, the blockchain.

As described below, Binance knew or had reason to know the location of its user base, including the fact that it was matching users located in the United States with counterparties in sanctioned jurisdictions or with blocked persons. As Binance grew exponentially and expanded internationally it became increasingly aware of the regulatory obligations and sanctions exposure it faced in maintaining this arrangement and of the need to create at least the appearance of an effective compliance program.

Binance Establishes a Sanctions Compliance Program to Appear Compliant, While Undermining its Own Controls

In 2018, Binance began to develop its first sanctions-related compliance plans and procedures, including by hiring a Chief Compliance Officer (CCO) in April 2018. The next month, in May 2018, Binance issued a public statement on sanctions compliance when it updated its Terms of Use to explain that by using the platform users acknowledged and declared themselves not to be on "any economic sanctions list." The Terms of Use also stated that Binance "may restrict or deny its services to sanctioned countries." In June and July 2018, Binance issued compliance policies, including a Global Compliance Policy, which stated that Binance "adheres to the Sanctions list maintained by the Office of Foreign Assets Control" and that "Binance will not conduct business with any personnel, entities or countries listed in the Sanctions list under any conditions." In October 2018, Binance updated its policy, which by its terms prohibited new users from sanctioned and other high-risk jurisdictions, including Iran, Syria, North Korea, and Cuba.

Following issuance of these policies, Binance began taking steps to identify sanctioned jurisdiction users for offboarding. Efforts to offboard these users, however, were implemented inadequately, at least in part due to Binance senior management's decisions to appear compliant while disregarding known sanctions risks. Numerous communications between Binance leadership demonstrate that Binance's failure to implement effective controls was the product of deliberate choices by senior management that effectively ensured Binance's sanctions compliance program would primarily remain only a "paper program."

Examples of Binance's approach to compliance are reflected in multiple internal discussions, including in the following exchanges:

- On August 3, 2018, Binance's then CCO explained in a chat message to a Binance employee that "our stance is [n]ot to openly do business with Iran due to sanctions. [I]t affects our

banking relationships. I understand that we still support [I]ranian customers but that has to be done non-openly.”

- The following month, in a September 2018 response to an inquiry from the then Deputy Head of Compliance asking if Binance was servicing users from Iran on Binance.com, the then CCO explained that, with respect to users from sanctioned countries, “[w]e are servicing [them] but non-public.” He further added, “[I] [t]old [yo]u we have [I]ranian customers; [the CEO of Binance] knows also. And allows it.”
- The then CCO would go on to explain to the Deputy that sanctions restrictions in Binance’s Terms of Use “has to be there to protect us, [it is] protective language. In biz, ceo doesn’t want to enforce.”
- Later, in the same chat, Binance’s then Deputy Head of Compliance stated that Binance’s Operations Director said that Binance “can service sanctioned countries” on Binance.com.
- In another September 2018 message, the then Deputy Head of Compliance explained to the then CCO that “[the CEO] keeps saying that compliance is here to make Binance APPEAR compliant.” (Emphasis in original.)
- In an October 18, 2018 message regarding the potential blocking of sanctioned country Internet Protocol (IP) addresses, the then CCO informed Binance’s Chief Executive Officer (CEO) that “we currently have users from sanction[ed] countries on [Binance.com],” adding that the “[d]ownside risk is if fincen or ofac has concrete evidence we have sanction[ed] users, they might try to investigate or blow it up big on worldstage.”
- In June 2019, the CEO demonstrated his own broad awareness of U.S. sanctions prohibitions applicable to Binance when he told a senior Binance employee that “the U.S. has this law: you have to prevent Americans and any terrorists from doing any transactions. In order [for America] to accomplish this, if you serve Americans or service American sanctioned countries, you have to give your data to the American regulators.” He added, “the U.S. says we are not focusing on the dollar; if our citizens use your services we can arrest/catch you.”

Binance senior management’s interest in feigning compliance rather than addressing the company’s actual risk was reflected in the intentionally weak implementation of its controls. In November 2018, for example, Binance began to take putative steps to identify and offboard users who had self-identified as located in a sanctioned jurisdiction during the Know Your Customer (KYC) onboarding process. By April 2019, however, the population of identified U.S. users and sanctioned jurisdiction users remained on the platform. Later that year, a Binance engineer repeatedly alerted the Operations Manager to the continued presence of sanctioned jurisdiction users and noted that “this is a bigger issue than you realize and we’ve kind of slacked on addressing this properly for quite some time.” The engineer subsequently went on to observe (in a different chat several months later) that “the operations team was not very exhaustive in their restrictions unfortunately,” and that the platform’s IP address screening allowed for a user to change their IP address using a Virtual Private Network (VPN) and access trading services even after failing Binance’s KYC screening.

Binance's failure to implement its sanctions compliance program did not hinder the company from touting its purported sanctions compliance controls to third parties in support of maintaining its banking relationships. In June 2018, for example, the then CCO misled a financial institution by writing in a Due Diligence Anti-Money Laundering Compliance form that "we use IP blocking to deny business from sanctioned countries. It is also clearly written in our Terms and Conditions that we prohibit business with all sanctioned countries." Such statements, however, misrepresented Binance's actual compliance procedures and communicated a commitment and practices that did not in fact exist.

Binance Launches New U.S. Platform While Retaining U.S. and Sanctioned Jurisdiction Users on Binance.com

In June 2019, Binance announced the launch of a new U.S.-based exchange, called Binance.US, that would supposedly wall off U.S. users from the Binance.com platform catering to the rest of the world. After Binance.US was launched in September 2019, the then CCO wrote to a senior employee on October 31, 2019 that "[t]he ofac regulation clearly states U.S. Persons, doing biz with OFAC is wrong," adding, "so back to the clean block of U.S. persons on [Binance].com that effectively mitigates the OFAC risk to a minimal." The then CCO also stated that it was a priority to convince the CEO to "to do a clean block on US for [Binance].com." That is, one benefit of the creation of Binance.US was that it would minimize sanctions compliance risk by moving U.S. users off the Binance.com platform.

Binance, however, continued to rely heavily on its U.S. user base for a substantial portion of its trading volume and liquidity and did not take effective steps to block or remove them from the platform, particularly larger traders. It also sought to encourage the use of VPNs to circumvent the geofencing controls it might ostensibly impose. For example, in May 2019, as the management team discussed blocking U.S. IP addresses ahead of the Binance.US launch, the CEO stated that a very specific popup notice should appear for U.S. users trying to access a non-U.S. Binance platform, adding, "I'll have a look at it myself. We need to word it very carefully so that we let people know what they need to do, including using a VPN, without explicitly stating it." The CEO even joked that Binance "should probably include a Google ad with a VPN on it."

Early the following year, on February 12, 2020, the then CCO stressed to another Binance employee that the presence of U.S. users on the Binance.com platform would expose Binance to legal risk under laws and regulations administered and enforced by OFAC and other U.S. regulatory agencies, stating, "if US users get on [Binance].com we become subjected to the following US regulators, fincen ofac and SEC." He added, however, that Binance.com tried to ask U.S. users to "use VPN," "provide...non-US documents," or "get them through other creative means."

Even after Binance began to take steps to offboard U.S. users from the Binance.com platform, the company retained lucrative high volume and liquidity-providing U.S. users on Binance.com to boost the company's revenue. As late as July 2020, in response to a question from a Binance employee about how to onboard a new U.S. user, the then CCO stated, "we ask them to onboard with [Binance.]US, and then if their volume is really very big, we will push hard on [the] .com side to accept it on an exceptional basis." Thus, Binance allowed U.S. users to continue transacting on

the Binance.com platform with inadequate controls in place to prevent those users from trading with users in sanctioned countries and blocked persons.

Given the trading on the Binance.com platform, amounting to \$3.8 billion in transaction volume per day in 2020, the continued presence of both U.S. and sanctioned jurisdiction users through 2022, and the liquidity provided by U.S. users, the sanctions exposure Binance's senior management had identified was a practical inevitability. Notwithstanding the location-agnostic algorithm of its matching engine, Binance knew, or had reason to know, its platform was routinely matching U.S. users with users from sanctioned jurisdictions over many years and at significant volumes. Binance identified the sanctioned jurisdiction users as located in Iran, Syria, North Korea, the Crimea Region of Ukraine, Cuba, the so-called Donetsk People's Republic, and the so-called Luhansk People's Republic on the basis of a KYC process and other available information, including cell phone numbers, submitted documents, and/or IP addresses.

As a result of the conduct described above, between approximately August 2017 and October 2022, Binance processed 1,667,153 virtual currency transactions — totaling approximately \$706,068,127 — in violation of § 560.204 of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR); § 542.207 of the Syrian Sanctions Regulations, 31 C.F.R. part 542; § 3(a) and § 7(a) of Executive Order (“E.O.”) 13722 of March 15, 2016, § 510.206 and § 510.212 of the North Korea Sanctions Regulations, 31 C.F.R. part 510; § 1(a)(iii) and § 3(a) of E.O. 13685 of December 19, 2014 (E.O. 13685), § 589.207 and § 589.213 of the Ukraine-/Russia-Related Sanctions Regulations, 31 C.F.R. part 589; § 515.201 of the Cuban Assets Control Regulations, 31 C.F.R. part 515; § 1(a)(iii) and § 4(a) of E.O. 14065 of February 21, 2022; and Section 206(a) of the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq.

Penalty Calculations and General Factors Analysis

The maximum statutory penalty amount in this case is \$592,133,829,398. OFAC determined that the Apparent Violations were not voluntarily self-disclosed and egregious. Accordingly, under OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A (the “Enforcement Guidelines”), the base penalty for the Apparent Violations equals the statutory maximum. The settlement amount of \$968,618,825 reflects OFAC's consideration of the General Factors under the Enforcement Guidelines and Binance's agreement to retain a Monitor for a five-year term, pursuant to the provisions set forth in OFAC's Settlement Agreement, a copy of which can be found [here](#).

The Settlement Agreement also explicitly states that in the event OFAC determines that a material breach of, or misrepresentation in, the agreement has occurred, including due to a failure to perform the Compliance Commitments of the Settlement Agreement, OFAC may, following notice to Binance, seek to impose on Binance an additional penalty up to the statutory maximum.

OFAC is taking this action concurrently with DOJ, FinCEN, and the CFTC. Binance's obligation to pay \$898,618,825 of the settlement amount for its Apparent Violations shall be deemed satisfied by payment to DOJ for the ITSR violations arising out of the same pattern of conduct during the same period of time.

OFAC determined the following to be **aggravating factors**:

- (1) Binance knew that its conduct constituted, or likely constituted, a violation of U.S. law when it intentionally retained both sanctioned jurisdiction users and U.S. users on its platform while understanding the applicability of U.S. sanctions to trades in which Binance matched U.S. and sanctioned jurisdiction users as counterparties. Binance's knowledge that matching and executing trades between such users could cause the violation of sanctions is reflected in the statements of senior executives at the highest levels of the company, including the CEO and the then CCO. The company's steps to encourage the circumvention of its controls further reflect the company's knowledge of the applicability of U.S. sanctions to its conduct.
- (2) Based on the large number of U.S. users on Binance.com and the liquidity they provided for its global trading activity, Binance knew, or had reason to know, its matching engines were routinely matching U.S. users with users from sanctioned jurisdictions over many years and at significant volumes. Such matches were inevitable in light of the trading volumes at issue, and Binance personnel were aware of the presence of each group and their trading activities on the exchange.
- (3) Despite awareness of Binance's failure to implement sufficient controls, Binance senior management mischaracterized its sanctions controls and its commitment to compliance to third parties in private communications, and to the public through actions such as issuing misleading Terms of Use and by removing references to sanctioned countries from its website when, in fact, it continued to serve them. It also encouraged the use of VPNs and surreptitiously allowed U.S. users and sanctioned jurisdiction users to trade even after ostensibly blocking them. For example, Binance continued to allow trades by users who were logged in from an IP address in a comprehensively sanctioned jurisdiction so long as that user had submitted KYC documents from a non-sanctioned jurisdiction.
- (4) Binance provided economic benefit to a substantial number of persons located in sanctioned jurisdictions over the course of at least four years. Its platform provided a way to hold and transfer virtual currency and other valuable assets, enabling the benefits of global trading and other financial activity to be received in sanctioned jurisdictions in direct contravention of the objectives underlying multiple U.S. sanctions programs. Such a channel also provided an avenue for at least two blocked persons to access the global cryptocurrency market.
- (5) Binance was a commercially sophisticated actor during the time of the Apparent Violations, entering new jurisdictions within months of its founding and quickly establishing operations throughout the world, including in the Cayman Islands, Singapore, and over time approximately 30 different countries. Binance grew quickly since its launch in July 2017 to become the world's largest virtual currency exchange by trading volume with almost 8 million global users by March 2018. Binance's wide range of business services, spanning multiple fiat channels and over 600 cryptocurrencies and tokens, reflect its growth between 2017 and 2021. By the end of 2022, Binance stated it had over 120 million users.

OFAC determined the following to be **mitigating factors**:

- (1) OFAC has not issued Binance a Penalty Notice or Finding of Violation in the five years preceding the date of the earliest transaction giving rise to the Apparent Violations.
- (2) Binance provided substantial cooperation to OFAC, including by conducting an extensive, independent, internal investigation, responding promptly to OFAC's requests for information, providing large volumes of data regarding the Apparent Violations, making multiple presentations to OFAC, submitting inculpatory internal communications, and executing a statute of limitations tolling agreement.
- (3) OFAC considered the totality of the unique circumstances of this matter to ensure that the enforcement response is proportionate to the nature of the Apparent Violations, including the volume of violative conduct compared to Binance's overall activity, and its relative revenues and profits with respect to the trades underlying the Apparent Violations. Many of the Apparent Violations involved transactions for relatively small amounts. The transactional volume of the Apparent Violations in light of Binance's overall trading activity was relatively minimal, such that trades between users in the United States and sanctioned jurisdictions represented less than 0.0028% of Binance's total trading volume during the relevant time period. Its operating income from such transactions represented a relatively small total as well, estimated to be in the low hundreds of thousands of dollars.
- (4) Binance has implemented significant remedial measures, including:
 - Revamped compliance policies and procedures, such as the Binance Sanctions Manual that requires Binance to complete an annual enterprise-wide risk assessment and additional due diligence reviews of users suspected of being located in a sanctioned jurisdiction;
 - Required all users to pass KYC and implemented periodic customer reviews according to users' compliance risk ratings;
 - Engaged third-party vendors to detect and prevent certain parties, including blocked persons, from onboarding, and implemented further technological controls to screen and identify users from sanctioned jurisdictions, including IP blocking, geo-fencing, and blockchain monitoring;
 - Partnered with third-party companies to implement real-time transaction monitoring, including screening for sanctioned parties;
 - Will contract with third-party firms to complete audits and reviews of Binance internal controls, policies, and procedures;
 - Mandated sanctions training at initial onboarding of new hires and for all employees yearly at a minimum;

- Significantly increased line-level compliance resources, including for sanctions compliance;
 - Created two teams dedicated to cooperation with law enforcement, including by proactively sharing intelligence and to respond to time-sensitive requests;
 - Remodeled its compliance program governance and organization structure, including by hiring new compliance leadership with professional compliance experience in the financial sector and law enforcement; and
 - Conducted multiple lookback reviews of users to identify and offboard users from the United States as well as sanctioned jurisdictions, including a re-screening of all active users against sanctions lists from the United States and various other countries.
- (5) Binance agreed to undertake certain compliance commitments, including retaining a Monitor for five years. The Monitor will review and evaluate the effectiveness of Binance’s policies, procedures, and internal controls, as they relate to, *inter alia*, Binance’s current and ongoing compliance with U.S. sanctions laws, and make recommendations reasonably designed to improve the effectiveness of Binance’s sanctions compliance program.
- (6) OFAC’s settlement with Binance is part of a comprehensive settlement with DOJ, FinCEN, and the CFTC, pursuant to which it has undertaken to pay substantial additional penalties and undertake other significant remedial measures.

Compliance Considerations

OFAC’s [Sanctions Compliance for the Virtual Currency Industry](#) establishes management commitment as the first pillar of an effective, risk-based compliance program. This commitment should come from the top and begin on “Day One,” even as a company may still be establishing itself and developing its technologies and offerings. Such a commitment, moreover, should be backed by resources adequate to address a company’s risks. Compliance personnel must be empowered and receive the backing and authority necessary to effectively fulfill their function. A culture of compliance, where senior management is invested in and supports an organization’s program and allows it to operate effectively and without undue interference, is essential to avoid committing violations of OFAC sanctions.

Compliance controls should also be incorporated into a company’s platforms and systems, through KYC protocols, transaction monitoring, sanctions screening, algorithmic configurations, and other controls as appropriate. It is no defense that an algorithm or other “autonomous” system or formula serves as the mechanism for the underlying transactions or activities that violate sanctions; companies are responsible for the operation and consequences of the technologies they employ and will be held accountable where their technologies result in violations.

Further, as with all financial institutions and money services businesses, virtual currency exchanges based outside the United States that conduct business with U.S. persons or within the United States must take care that their activities do not cause U.S. persons to violate U.S. economic sanctions or result in the exportation, reexportation, sale, or supply, directly or indirectly, of goods, services, or technology from the United States to sanctioned jurisdictions or blocked persons. Firms that fail to do so not only expose themselves to significant civil monetary penalties, but may also face criminal liability. OFAC vigorously enforces its civil enforcement authorities across all industries, and foreign entities that conduct business in the United States or with U.S. persons, should not avail themselves of U.S. customers, goods, technology, and services, without instituting controls to maintain adherence to U.S. economic sanctions and other U.S. laws.

OFAC Enforcement and Compliance Resources

On May 2, 2019, OFAC published [A Framework for OFAC Compliance Commitments](#) (the “Framework”) in order to provide organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use goods or services exported from the United States, with OFAC’s perspective on the essential components of a sanctions compliance program. The Framework also outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements. The Framework includes an appendix that offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process.

Information concerning the civil penalties process can be found in the OFAC regulations governing each sanctions program; the Reporting, Procedures, and Penalties Regulations, 31 C.F.R. part 501; and the Enforcement Guidelines. These references, as well as recent civil penalties and enforcement information, can be found on OFAC’s website at <https://ofac.treasury.gov/civil-penalties-and-enforcement-information>.

FinCEN maintains a whistleblower incentive program for violations of OFAC-administered sanctions, in addition to violations of the Bank Secrecy Act. Individuals who provide information may be eligible for awards totaling between 10 to 30 percent of the monetary penalties collected in an enforcement action, if the information they provide leads to a successful enforcement action that results in penalties exceeding \$1,000,000. FinCEN is currently accepting whistleblower tips. Individuals with questions about the whistleblower program, including questions about how best to submit information, should contact FinCEN through its website, www.fincen.gov/contact.

For more information regarding OFAC regulations, please go to: <https://ofac.treasury.gov>