Institute for
Financial Integrity

EXPERT INSIGHT

Binance Settles with Regulators

World's Largest Cryptocurrency Exchange to Pay Record Fine

Table of Contents

Binance Settles with Regulators

World's Largest Cryptocurrency Exchange to Pay Record Fine

Binance, the world's largest cryptocurrency exchange, on November 21st, 2023 pleaded guilty and agreed to pay more than $4.3 billion to resolve the US Justice Department's investigation into its violations of the Bank Secrecy Act (BSA) and US sanctions, as well as other criminal activities. Binance's founder and chief executive officer (CEO), Changpeng Zhao (known as CZ) also pleaded guilty to failing to maintain an effective anti-money laundering (AML) program and has resigned as CEO of the company.

- Binance's guilty plea is part of coordinated resolutions with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC), as well as the Commodity Futures Trading Commission (CFTC).

- Binance's penalty is one of the largest in US history, and Attorney General Merrick Garland noted that the company became the world's largest cryptocurrency exchange in part because it violated US laws. Treasury Secretary Janet Yellen added that Binance's willful criminal acts allowed terrorists, illicit cyber actors, and other malign actors to obfuscate the origin of illicit funds.

- Binance also knew that US sanctions laws prohibited US persons from transacting with its sanctioned customers, including customers located in comprehensively sanctioned jurisdictions, such as Iran. Nonetheless, Binance did not implement controls that would prevent US users from trading with users in Iran and willfully caused more $898 million in trades between US users and those located in the Islamic Republic.

- Binance also had significant exposure to Russian illicit finance, even after Russia's invasion of Ukraine in 2022. In addition to allowing US persons to transact with embargoed jurisdictions illegally annexed by Russia, the platform also processed transactions for sanctioned Russian exchanges and ransomware actors.

This Expert Insight will discuss Binance's violations of US law, including the Bank Secrecy Act and OFAC sanctions. It will delve into the company's efforts to obscure its violations and help its VIP customers alter their documents to avoid regulatory scrutiny. In addition, this assessment will highlight some of the lessons virtual asset service providers (VASPs) can learn from these recent regulatory actions and possible mitigating strategies financial institutions can use to reduce their vulnerabilities when transacting with companies such as virtual currency exchanges and new financial technologies that can present additional compliance risks.


BNB
BINANCE COIN
BINANCE COIN

BSA Violations

FinCEN assessed that Binance was a money services business (MSB) and a money transmitter operating in the United States based on definitions outlined in the BSA. As a result, Binance was required to comply with regulations applicable to MSBs, including registering as an MSB with FinCEN within 180 days of beginning its operations and renewing the registration every two years; and developing, implementing, and maintaining an effective AML program. Binance was also required to file suspicious activity reports (SARs).

- Binance never registered with FinCEN as an MSB, but it transacted as a money transmitter in substantial part within the United States and served more than a million US customers, who not only accessed the company's platform—Binance.com—but also used the platform to exchange cryptocurrency for fiat funds, according to the FinCEN consent order imposing a civil monetary penalty on Binance.

- Despite its assurances to US regulators that it had ceased serving US customers, Binance continued to operate as an unregistered MSB in the United States and employed numerous US-based personnel and partnered with a US financial institution to offer its users a dollar-based stablecoin. Binance also failed to block the IP addresses of US users, allowing them to "self-certify" that they were not US persons, and using the self-certification process as proof of their lack of US-nexus to allow them to transact on the platform, rather than checking their IP addresses.

Intentional Misrepresentations

According to FinCEN, Binance engaged in a series of misrepresentations to US regulators to maintain unregistered MSB operations in the United States. To deceive US regulators about its customers "geofencing" controls that were supposed to prevent US users from accessing the platform, the company helped its US customers to circumvent its own controls and notified its high-value, or VIP, users if they became the subject of a law enforcement inquiry.

- Two years after Binance.com launched its operations, US users were identified by their IP addresses, but were not fully blocked. Binance claimed that if a customer used a VPN to mask their IP address, it would employ "a secondary manual control during the KYC process" to ensure no US persons were using the platform. At the time of Binance's response, however, the company had no secondary manual control, and the majority of users on the platform were not required to undergo KYC.

- Binance encouraged its VIP users to alter know-your-customer (KYC) documents to obscure their nexus to the United States, use VPNs to obscure their location, and change their IP. According to FinCEN, Binance CEO and founder, CZ, described the goal as "reduc[ing] the losses to ourselves, and, at the same time, to make the US regulatory authorities not trouble us." CZ inquired about the process of changing KYC documents for VIP users that would reflect an offshore entity. The company's former Chief Compliance Officer (CCO) suggested that another VIP could have someone with a non-US passport submit KYC documents on the individual's behalf.

- Binance in 2019 developed a process to indirectly notify its VIP users that they may be investigated by law enforcement. The company would contact the user through "all available means (text, phone), to inform him/her that his account has been frozen or unfrozen," strongly hinting about an investigation by authorities.

- Senior managers obscured Binance's ties to US users by changing internal reports prepared by the company's finance department to reclassify the country code for US users from "US" to "UNKWN" and to restrict access to the information about these users within the company.

In addition, Binance employed "Exchange Brokers" whose clients were allowed to trade on the Binance.com platform via sub-accounts under the broker's Binance account. The sub-users were not required to register with Binance.com, and the company did not maintain AML controls over the broker program until late 2021. Roughly half of the 100 Exchange Brokers with which Binance maintained relationships either were US firms, exhibited clear indications of servicing US users, or appeared not to impose any restrictions applicable to US users, according to a review by US regulators.

Binance.us

According to the FinCEN consent order, Binance in 2018 established a "US" entity—separate from Binance.com that would be registered with FinCEN as an MSB—that would essentially serve as a "decoy" to divert law enforcement attention from the company's main platform. Leading up to the launch of Binance.us, the entity's CEO was assured that Binance would start blocking US users on Binance.com after the registration with FinCEN was complete. However, the geofencing controls—that were supposed to block US users on the Binance.com platform—were incremental, protracted, and ineffective, according to FinCEN. Moreover, Binance offered US trading firms the opportunity to maintain their accounts on the main platform in exchange for their commitment to increase their activity on Binance.us.

Despite Binance's claim that Binance.us would be a separate platform for all US operations, FinCEN asserts that Binance.us lacked autonomy from the main platform, remaining fully dependent on Binance for provision of wallet software services and the platform's matching engine, risk control center, and mobile applications. In addition, the US entity's board of directors has always consisted of three individuals: the CEO of Binance.us, the CEO of Binance.com (CZ), and a third director affiliated with Binance.com.

The lack of independence from Binance.com allowed CZ to use Binance.us to facilitate the activities of his proprietary trading firms: Sigma Chain AG (Sigma Chain) and Merit Peak Limited (Merit Peak). The latter also functioned as Binance.com's over-the-counter (OTC) trading desk and used Binance.us as a conduit for Binance.com to continue accessing the US market.

KYC Tiers and Illicit Actors

Binance initially adopted a "tiered" approach to conducting KYC and identifying its customers, characterizing the approach as "risk-based." Most significantly, from July 2017 through at least August 2021, "Tier One" (also referred to as "no-KYC") customers could open accounts and transact with only an email address and no due diligence performed. The "no-KYC" account holders could conduct daily withdrawals of convertible virtual currencies less than two bitcoins—a value which at times exceeded $130,000.

Senior managers at Binance were aware that these no-KYC accounts were being exploited by illicit actors. Emails in 2018 revealed that the company was "tracking some stolen money" that was coming from "one of the worst hacking groups we have seen." The group appeared to have been using Binance as one of their cash-out venues.

FinCEN assessed that following Russia's invasion of Ukraine in 2022, Binance continued to have significant exposure to Russian illicit finance, despite claiming that the company would focus on the risks associated with illicit Russian financial flows.

- Binance processed hundreds of millions of dollars for a cryptocurrency exchange co-owned by a Russian citizen who pled guilty to money laundering in February 2023.

- Binance processed several million dollars for an exchange that allowed its users to cash out at a US-designated Russian bank that had substantial exposure to the Russian darknet market Hydra Market. The company also continued to allow transactions with Russia Market—one of the biggest cybercrime websites in the world—until as recently as the summer of 2023.

- US-designated Russian cryptocurrency exchange, SUEX—sanctioned for facilitating illicit transactions from the proceeds of numerous criminal activities, including ransomware attacks—operated on the Binance.com platform via multiple high-tier accounts that did not undergo KYC.

- Russia-based virtual currency exchange Garantex, sanctioned by OFAC in 2022, conducted more than $100 million in potentially suspicious transactions with illicit actors, including $6 million associated with the Conti ransomware group, which is responsible for high-profile attacks on the healthcare industry.

Other High-Risk Activities

Binance had high volumes of activity with online and unlicensed casinos and gambling platforms, considered high-risk counterparties, even by Binance itself, according to documents obtained by the Treasury Department.

Binance's geofencing allowed users from high-risk jurisdictions to access the platform without appropriate controls. Binance personnel were aware that the platform's poor geofencing controls allowed users from jurisdictions included on the Financial Action Task Force's (FATF) grey list or subject to comprehensive sanctions to access the platform.

FinCEN also noted that Binance failed to designate an individual responsible for its AML program and BSA obligations for almost a year after beginning operations. And when a Chief Compliance Officer was hired, the individual was not qualified for the role, lacked knowledge of AML/CFT obligations, and had limited experience designing a compliance program.

Binance's lack of suspicious transaction reporting resulted in millions of dollars in transactions linked to ransomware, terrorist financing—including for ISIS and Hamas—fraud and scams, and child sexual abuse material, according to the FinCEN consent order.

Sanctions Violations

According to OFAC, although Binance worked to project an image of compliance, users in sanctioned jurisdictions used the platform with the knowledge of the company's senior management. Binance's leaders recognized that the company's matching algorithm, which would ingest incoming buy/sell orders and match them with pending orders on Binance's orderbook according to price and time, could cause sanctions violations. Further, Binance senior managers mischaracterized the company's 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.

- In January 2023, Binance joined the Association of Certified Sanctions Specialists (ACSS), claiming that the company would use ACSS training materials, databases, and networks to enhance its compliance team's expertise. Binance also asserted that compliance was its core focus and that the company grew its compliance team from 500 to 750 individuals as part of efforts to strengthen its compliance capabilities.

- To further project an image of compliance with US sanctions, Binance's Terms of Use specified that the company may deny or restrict services to sanctioned jurisdictions. However, OFAC asserts that Binance clandestinely transacted with sanctioned jurisdictions, such as Iran, and its then-CCO admitted in chat messages that "our stance is not to openly do business with Iran due to sanctions," but to continue transacting with Iranian customers "non-openly." The CCO also admitted that the language about sanctions restrictions in the company's Terms of Use was intended to protect the company and to make it appear compliant.

- Binance in 2022 implemented a global training program for prosecutors, regulators, and law enforcement agencies to help them tackle financial crimes linked to cryptocurrencies. By claiming to work with "law enforcement throughout the world," Binance almost certainly enhanced its credibility as a company dedicated to compliance and fighting financial crimes.

In addition, Binance's intentionally weak KYC and due diligence procedures and efforts to help customers obscure their location by using VPNs, also allowed sanctions to be violated and the platform to be used by individuals in embargoed jurisdictions, according to OFAC.


Binance – Cryptocurrency Exchange
Start the 2.0 Age of Cryptocurrency Exchange
Binance - Cryptocurrency Exchange
Binance Inc.
Your device isn't compatible with this version.
4.1
Finance
Similar
Downloads
Binance - Cryptocurrency Exchange
READ MORE

Lessons Learned for VASPs

As virtual currencies play an increasingly prominent role in world finance, VASPs must satisfy their OFAC compliance obligations, much like entities that transact in fiat currencies. VASPs are responsible for ensuring that they do not transact with entities or persons that are included on OFAC's Specially Designated Nationals (SDN) List and do not willfully or inadvertently facilitate money laundering and other financial crimes.

OFAC specifies that its 2021 guidance "Sanctions Compliance for the Virtual Currency Industry" establishes management commitment as the first pillar of an effective, risk-based compliance program. Management commitment is also one of the essential components in OFAC's framework for compliance commitments for all organizations. OFAC specifies that 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. Binance did not implement a sanctions compliance program until a year after it began operations.

OFAC also states that a leadership commitment to sanctions compliance should be backed by resources adequate to address a company's risks, and that compliance personnel must be empowered and receive the backing and authority necessary to effectively fulfill their function. Binance's management, including its CEO and CCO, knew that the company's conduct constituted violations of US law and their internal discussion confirmed that the company intended to continue allowing VIP US users to transact with embargoed jurisdictions in violation of 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, according to OFAC. Binance's then-CCO confirmed that the company asked US users to "use VPN," "provide…non-US documents," or "get them through other creative means" to maximize profits and avoid regulatory scrutiny.

Risk Mitigation Strategies for Banks and Other Financial Institutions

Banks and non-bank financial institutions can mitigate their risks when transacting with VASPs. In a 2021 Expert Insight, K2 Integrity highlighted five ways banks can lessen risks associated with cryptocurrencies. These included reviewing best practices for transacting with MSBs, since FinCEN classifies many VASPs, including Binance, as money transmitters that need to comply with regulatory requirements for MSBs; identifying high-risk digital currency customers by updating and strengthening risk assessments and reviewing best practices for these clients; and understanding the needs and compliance challenges of new technologies and services.

When deciding whether to transact with VASPs, banks, and other financial institutions should also research the platform to ensure the new business falls in line with its risk appetite. Much of this research is similar to due diligence that should be conducted for any other potential counterparty or correspondent account, with emphasis on the following factors.

Location. Is the VASP located in a high-risk or embargoed jurisdiction that achieved poor results on its FATF mutual evaluation or is included on the FATF grey or black list? Is the location known for strategic deficiencies in its AML/CFT regime? Is it known as an offshore secrecy haven? Is the VASP located in close proximity to a jurisdiction known for terrorist financing?

Sanctions status. Is the exchange sanctioned by the United States, UK, or EU? Is the company owned by a person included on these lists? Are any of the digital wallets included on sanctions lists?

Ownership/control structure. Who owns this VASP? Are the company's leaders real people or shell profiles with little information available about their experience and work history? Do they have a robust online presence that is linked to the VASP or lists the VASP as an employer? Are any owners or managers politically exposed persons (PEPs) or linked to designated individuals or companies?

KYC and CIP. What kind of KYC controls are in place at the exchange? If the VASP has little to no KYC for small amounts, illicit actors could use the exchange to structure deposits and launder money. What kind of documentation is required for identity and location verification? What kind of controls are in place to ensure that the VASP's protocols are being effectively implemented?

KYC history. Financial institutions can also use existing tools to examine the history of the company's compliance programs. How have KYC and CDD processes changed over time? Have they become more robust? When were their compliance programs implemented? Were they in place when the VASP first started operating?

High-risk transactions. What percentage of transactions in which the VASP is involved is high-risk? Does it process a significant number of proceeds from online gambling activities? Does it offer a high level of anonymity to its customers that can be exploited by illicit actors? Does the VASP offer its customers transactions in privacy coins or allow onramps (deposits of fiat currency into the exchange—whether directly or indirectly through a third-party intermediary—making exchanging cash for cryptocurrency easier for illicit actors)? Does the VASP allow customers to withdraw fiat currency, allowing potential criminals to exchange virtual assets for cash and enabling money laundering?

Adverse media and previous enforcement actions. Before onboarding a VASP, examine media reporting about the VASP. Is it under investigation by regulators? Have there been allegations about sanctions violations or other misconduct? Has the VASP had a finding of violation or a penalty imposed by regulators, and what measures did it take to remediate the causes of its violations?

Banking and financial transactions. What other financial institutions are transacting with or have accounts for the exchange? What sources are sending virtual assets through the exchange, and what is the destination of those assets? Has the exchange processed any criminally linked transactions? Is their number significant? If the exchange detected transactions involving criminal activity, such as ransomware, or dark web activity, have SARs been filed with FinCEN or foreign FIUs? How many SARs have been submitted?

Compliance team. How big is the exchange's compliance team? Has it grown along with the global risk environment? What are the team's qualifications and experience? Are the managers of the compliance team experienced in AML/CFT, sanctions, and other financial crimes? Do they have experience designing a compliance program?

New technologies are enabling smoother, more efficient financial transactions. However, digital currencies and other virtual assets also create more challenges and regulatory risks for compliance officers at banks and other financial institutions. Due diligence research should be a robust part of onboarding counterparties in the virtual asset space, but each compliance solution should be tailored to each financial institution's needs and risk appetite. A new business partner or counterparty that operates as a VASP should prompt an examination and possible update of the institution's risk assessment.

The mitigation strategies listed in this Expert Insight are not comprehensive, and the virtual assets sector continues to evolve. DOLFIN's resource on sanctions risks and compliance for virtual assets and VASPs can be a valuable tool to develop additional strategies and address vulnerabilities.