PRESS RELEASE

Binance and CEO Plead Guilty to Federal Charges in $4B Resolution

Tuesday, November 21, 2023

For Immediate Release

Office of Public Affairs

Binance Admits It Engaged in Anti-Money Laundering, Unlicensed Money Transmitting, and Sanctions Violations in Largest Corporate Resolution to Include Criminal Charges for an Executive

Binance Holdings Limited (Binance), the entity that operates the world's largest cryptocurrency exchange, Binance.com, pleaded guilty today and has agreed to pay over $4 billion to resolve the Justice Department's investigation into violations related to the Bank Secrecy Act (BSA), failure to register as a money transmitting business, and the International Emergency Economic Powers Act (IEEPA).

Binance's founder and chief executive officer (CEO), Changpeng Zhao, a Canadian national, also pleaded guilty to failing to maintain an effective anti-money laundering (AML) program, in violation of the BSA and has resigned as CEO of Binance.

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

"Binance became the world's largest cryptocurrency exchange in part because of the crimes it committed – now it is paying one of the largest corporate penalties in U.S. history," said Attorney General Merrick B. Garland. "In just the past month, the Justice Department has successfully prosecuted the CEOs of two of the world's largest cryptocurrency exchanges in

two separate criminal cases. The message here should be clear: using new technology to break the law does not make you a disruptor, it makes you a criminal."

"Binance turned a blind eye to its legal obligations in the pursuit of profit. Its willful failures allowed money to flow to terrorists, cybercriminals, and child abusers through its platform," said Secretary of the Treasury Janet L. Yellen. "Today's historic penalties and monitorship to ensure compliance with U.S. law and regulations mark a milestone for the virtual currency industry. Any institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime or face the consequences."

"A corporate strategy that puts profits over compliance isn't a path to riches; it's a path to federal prosecution," said Deputy Attorney General Lisa O. Monaco. "Today's charges and guilty pleas – combined with a more than $4 billion financial penalty – sends an unmistakable message to crypto and defi companies: if you serve U.S. customers, you must obey U.S. law."

"Changpeng Zhao made Binance, the company he founded and ran as CEO, into the largest cryptocurrency exchange in the world by targeting U.S. customers, but refused to comply with U.S. law," said Acting Assistant Attorney General Nicole M. Argentieri of the Justice Department's Criminal Division. "Binance's and Zhao's willful violations of anti-money laundering and sanctions laws threatened the U.S. financial system and our national security, and each of them has now pleaded guilty. Make no mistake: when you place profits over compliance with the law, you will answer for your crimes in the United States."

"Binance's crimes gave sanctioned customers unfettered access to American capital and financial services," said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division (NSD). "This prosecution is a warning that companies that do not build sanctions compliance into their services face serious criminal penalties, as do the executives who lead them."

"From the beginning of its existence, Binance and founder Changpeng Zhao chose growth and personal wealth over following financial regulations aimed at stopping the laundering of criminal cash," said Acting U.S. Attorney Tessa M. Gorman for the Western District of Washington. "Because Changpeng Zhao knowingly operated a financial platform without basic anti-money laundering safeguards, the company caused illegal transactions between U.S. users and users in sanctioned jurisdictions such as Iran, Cuba, Syria, and Russian-occupied regions of Ukraine – transactions for which Binance profited with significant fees."

"Binance's activities undermined the foundation of safe and sound financial markets by intentionally avoiding basic, fundamental obligations that apply to exchanges, all the while collecting approximately $1.35 billion in trading fees from U.S. customers," said Chairman Rostin Behnam of the Commodity Futures Trading Commission (CFTC). "American investors, small and large, have demonstrated eagerness to incorporate digital asset products into their portfolios. It is our duty to ensure that when they do so, the full protections afforded by our regulatory oversight are in place, and that illegal and illicit conduct is swiftly addressed.

When, as here, an entity goes even further, deliberately avoiding to employ meaningful access controls, intentionally avoiding knowing customers' identities, and actively concealing the presence of U.S. customers on its platforms, there is no question that the CFTC will strike hard and aggressively."

"When you put growth above compliance, you end up in hot water," said Chief Jim Lee of the IRS Criminal Investigation (IRS-CI). "Our team of investigators uncovered that Binance disregarded anti-money laundering Know Your Customer laws, failed to register as a money transmitter, and willfully violated U.S. sanctions tied to the International Emergency Economic Powers Act. When you do so, your business becomes a playground for bad actors. Hundreds of millions of dollars in illicit proceeds from ransomware variants, darknet transactions, and various internet-related scams moved through Binance in an attempt to evade detection by law enforcement."

According to court documents, Binance admitted to prioritizing growth and profits over compliance with U.S. law. Binance launched in 2017 and focused on attracting high-volume customers, including U.S.-based customers. Binance quickly became the largest cryptocurrency exchange in the world, with the greatest share of its customers coming from the United States. As a result of serving U.S. customers, Binance was required to register with FinCEN as a money services business and to implement an effective AML program that was reasonably designed to prevent Binance from being used to facilitate money laundering. Binance chose not to comply with U.S. law and failed to implement controls and procedures to prevent money laundering. Binance also did not implement controls that would have prevented U.S. customers from conducting transactions with customers in sanctioned jurisdictions, despite knowing that the system it used to match customers for transactions would necessarily cause transactions in violation of IEEPA.

Instead of complying with U.S. law, in 2019, Binance announced that it would block U.S. customers and launched a separate U.S. exchange, Binance.US. Despite this announcement, Binance took steps to maintain a substantial number of U.S. customers. In particular, Binance focused on retaining valuable "VIP" customers, which were responsible for a large portion of Binance's trading volume and revenue. These VIP customers were critical to Binance's business because they helped provide the necessary liquidity to facilitate trades of digital assets. For example, Binance executives, including Zhao, made a plan to contact VIP customers and help the VIP register a new account for an offshore entity and transfer holdings to that account. Binance employees also called U.S. VIPs to encourage them to provide information that suggested the customer was not located in the United States.

Binance also did not implement the core components of an effective AML program: Binance did not implement comprehensive know-your-customer (KYC) protocols or systematically monitor transactions, and Binance never filed a suspicious activity report (SAR) with FinCEN. For years, Binance allowed users to open accounts and trade without submitting any identifying information beyond an email address. Binance began requiring all users to provide KYC information in August 2021 but allowed users who had not provided KYC to continue trading on the exchange until May 2022. Between August 2017 and October 2022,

U.S. users, including VIPs, conducted trillions of dollars in transactions on the platform, generating over $1.6 billion in profit for Binance.

As Binance's internal communications showed, Binance's compliance employees recognized that Binance did not have protocols to flag or report transactions for money laundering risks, which employees recognized would attract criminals to the exchange. As one compliance employee wrote, "we need a banner 'is washing drug money too hard these days - come to binance we got cake for you.'" Due in part to Binance's failure to implement an effective AML program, illicit actors used Binance's exchange in various ways, including conducting transactions for mixing services that obfuscated the source and ownership of cryptocurrency; transferring illicit proceeds from ransomware variants; and moving proceeds of darknet market transactions, exchange hacks, and various internet-related scams.

Binance also knew that U.S. sanctions laws prohibited U.S. persons – including its U.S. customers – from trading with its customers subject to U.S. sanctions, including customers in comprehensively sanctioned jurisdictions, such as Iran. Binance knew that it had a significant number of users from comprehensively sanctioned jurisdictions and a substantial number of U.S. users and that its matching engine would necessarily cause U.S. users to transact with users in sanctioned jurisdictions in violation of U.S. law. Nonetheless, Binance did not implement controls that would prevent U.S. users from trading with users in Iran; and, because of this intentional failure, between January 2018 and May 2022, Binance willfully caused over $898 million in trades between U.S. users and users ordinarily resident in Iran.

As part of the plea agreement, Binance has agreed to forfeit $2,510,650,588 and to pay a criminal fine of $1,805,475,575 for a total financial penalty of $4,316,126,163. Binance has also agreed to retain an independent compliance monitor for three years and remediate and enhance their anti-money laundering and sanctions compliance programs. Binance separately has also reached agreements with the CFTC, FinCEN, and OFAC, and the Department will credit approximately $1.8 billion toward those resolutions.

The Department reached its resolution with Binance based on a number of factors, including the nature, seriousness, and pervasiveness of the offense, as a result of which Binance processed billions of dollars of cryptocurrency transactions for U.S. persons and caused U.S. customers to engage in transactions in violation of U.S. sanctions. Binance did not make a timely and voluntary disclosure of wrongdoing, but it received partial credit for its cooperation with the Department's investigation, and it has taken steps to remediate its compliance program. Binance did not receive full credit for its cooperation because it delayed producing relevant evidence, including recorded meetings in which Binance executives discussed U.S. legal requirements. Accordingly, the total criminal penalty reflects a 20% reduction off the bottom of the applicable U.S. sentencing guidelines fine range.

In addition, according to court documents, Zhao, Binance's founder, owner, and CEO, admitted that he understood that Binance served U.S. users and was thus required to register with FinCEN and implement an effective AML program. Zhao knew that U.S. users

were essential to Binance's growth and were a significant source of revenue and knew that an effective AML program would include KYC protocols that would mean that some customers would choose not to use Binance. Zhao told employees it was "better to ask for forgiveness than permission," and prioritized Binance's growth over compliance with U.S. law. Without an effective AML program, Binance caused transactions between U.S. users and users in jurisdictions subject to U.S. sanctions. These illegal transactions were a clear and foreseeable result of Zhao's decision to prioritize Binance's profit and growth over compliance with the BSA.

IRS-CI is investigating the case. The case is being prosecuted by Bank Integrity Unit Deputy Chief and National Cryptocurrency Enforcement Team Deputy Director Kevin Mosley and Trial Attorney Elizabeth Carr of the Criminal Division's Money Laundering and Asset Recovery Section (MLARS), Trial Attorneys Beau Barnes and Alex Wharton of NSD's Counterintelligence and Export Control Section (CES), and Assistant U.S. Attorney (AUSA) Mike Dion for the Western District of Washington. Trial Attorney Julia Jarrett, formerly of MLARS and currently an AUSA for the District of Oregon, and Trial Attorney Matthew Anzaldi, formerly of CES and currently with NSD's National Security Cyber Section, made substantial contributions to this investigation and prosecution.

MLARS's Bank Integrity Unit investigates and prosecutes banks and other financial institutions, including their officers, managers, and employees, whose actions threaten the integrity of the individual institution or the wider financial system. The Criminal Division has surged resources to the Bank Integrity Unit, which has imposed over $12 billion in penalties on financial institutions for sanctions violations over the last decade. NSD's Counterintelligence and Export Control Section investigates and prosecutes individuals and corporations for violations of export control and sanctions laws, in addition to other national security crimes. NSD continues to expand its corporate enforcement efforts – including growing the ranks of prosecutors dedicated to this work and establishing a Chief Counsel and Deputy Chief Counsel for Corporate Enforcement.

Binance Plea Agreement Zhao Plea Agreement Binance Information Zhao Information

Updated February 6, 2025

Topics

CYBERCRIME NATIONAL SECURITY

Components

Office of the Attorney General | Criminal Division | Criminal - Money Laundering and Asset Recovery Section | National Security Division (NSD) | Office of the Deputy Attorney General | USAO - Washington, Western

Press Release Number: 23-1323

Related Content

PRESS RELEASE

Alabama Man Pleads Guilty in Connection with Securities and Exchange Commission X Account Hack

An Alabama man pleaded guilty today in connection with the January 2024 unauthorized takeover of the U.S. Securities and Exchange Commission (SEC)'s social media account on X, formerly known as...

February 10, 2025

PRESS RELEASE

Phobos Ransomware Affiliates Arrested in Coordinated International Disruption

The Justice Department today unsealed criminal charges against Roman Berezhnoy, 33, and Egor Nikolaevich Glebov, 39, both Russian nationals, who allegedly operated a cybercrime group using the Phobos ransomware that victimized more...

February 10, 2025

PRESS RELEASE

Canadian Man Charged in $65M Cryptocurrency Hacking Schemes

A five-count criminal indictment was unsealed today in federal court in New York charging a Canadian man with exploiting vulnerabilities in two decentralized finance protocols to fraudulently obtain about $65...

February 3, 2025

Office of Public Affairs

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington DC 20530

Office of Public Affairs Direct Line
202-514-2007

Department of Justice Main Switchboard
202-514-2000