(BILLING CODE: 4810-02-P)

This document has been submitted to the Office of the Federal Register (FR) for publication and is currently pending placement on public display at the FR and publication in the Federal Register. The document may vary slightly from the published document if minor editorial changes have been made during the FR review process. Upon publication in the Federal Register, the order can be found at www.federalregister.gov and at www.treasury.gov. The document published in the Federal Register is the official document.

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network (FinCEN), Treasury.

31 CFR Chapter X, Part 1010

Imposition of Special Measure Prohibiting the Transmittal of Funds Involving MEXC Global

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Order.

SUMMARY: FinCEN is issuing notice of an order, pursuant to section 9714(a) of the Combating Russian Money Laundering Act (Public Law 116-283), as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81), finding that MEXC Global—including any of its subsidiaries, branches, and offices, as well as any successor entities, operating in any jurisdiction outside of the United States—is a financial institution operating outside of the United States of primary money laundering concern in connection with Russian illicit finance and prohibiting certain transmittals of funds involving MEXC Global.

DATES: This action is effective [**INSERT 30 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER***].

FOR FURTHER INFORMATION CONTACT: FinCEN's Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

SUPPLEMENTARY INFORMATION:

I. Summary of Order

As set out in this order, MEXC Global has facilitated funds transfers by Russia-affiliated illicit actors and in connection with other Russia-associated illicit activities, including sanctions evasion, and activity facilitated by Russian darknet markets. It has also facilitated billions of dollars in transactions benefitting Iran and its proxies, financial facilitators of the Democratic People's Republic of Korea (DPRK), and other cybercrime actors. Accordingly, this order (1) sets forth FinCEN's determination that MEXC Global, a convertible virtual currency (CVC) exchanger, along with any subsidiaries, branches, and offices of MEXC Global, and any successor entities, operating in any jurisdiction outside of the United States (collectively, MEXC Global)[1] is a financial institution operating outside of the United States of primary money laundering concern in connection with Russian illicit finance; and (2) prohibits certain transmittals of funds involving MEXC Global, by any covered financial institution.

II. Background

A. Statutory Provisions

Section 9714(a) of the Combating Russian Money Laundering Act (Pub. L. 116-283), as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Pub. L. 117-81) (section 9714),[2] provides, in relevant part, that, if the Secretary of the Treasury (Secretary) "determines that reasonable grounds exist for concluding that one or more financial

[1] This includes, but is not limited to, active and past MEXC affiliated entities MEXC Global Ltd/MX Global Ltd (Seychelles); MEXC Estonia OÜ (Estonia); GIDA Technology AG (Switzerland); and MXC Global Ltd (United Kingdom); affiliated entities formerly incorporated in Singapore MEXC Global Foundation Ltd and MEXC Singapore Pte Ltd; and any successor entities.

[2] Section 9714 (as amended) may be found in a note to 31 U.S.C. 5318A.

institutions operating outside of the United States ... is of primary money laundering concern in connection with Russian illicit finance," the Secretary may, "by order, regulation, or otherwise as permitted by law": (1) require domestic financial institutions and domestic financial agencies to take one or more of the special measures described in 31 U.S.C. 5318A(b);[3] or (2) prohibit, or impose conditions upon, certain transmittals of funds (as defined by the Secretary) by any domestic financial institution or domestic financial agency (collectively, covered financial institutions), if such transmittal of funds involves any such financial institution. The authority of the Secretary to administer both section 9714 and the Bank Secrecy Act (BSA) has been delegated to FinCEN.[4]

Pursuant to section 9714, the Secretary may impose one or more of six special measures. First, the Secretary may impose any of the five special measures provided for in 31 U.S.C. 5318A(b), commonly known as section 311 of the USA PATRIOT Act.[5] Through special measures one through four, the Secretary may impose additional recordkeeping, information collection, and reporting requirements on covered financial institutions.[6] Through special measure five, the Secretary, in consultation with the Secretary of State, the Attorney General, and the Chairman of the Board of Governors of the Federal Reserve System, may "prohibit, or impose conditions upon, the opening or maintaining in the United States of a correspondent

[3] *See infra* note [4].
[4] Pursuant to Treasury Order 180-01, the authority of the Secretary of the Treasury (Secretary) to administer the BSA, including, but not limited to, 31 U.S.C. 5318A, has been delegated to the Director of FinCEN. Treasury Order 180-01 (Jan. 14, 2020). On August 11, 2022, and in accordance with Treasury Order 101-05 and 31 U.S.C. 321(b), Treasury's Under Secretary for Terrorism & Financial Intelligence re-delegated to the Director of FinCEN the authority of the Secretary under section 9714.
[5] *See* 31 U.S.C. 5318A. 31 U.S.C. 5318A grants the Secretary the authority, upon finding that reasonable grounds exist for concluding that one or more financial institutions operating outside of the United States is of primary money laundering concern, to require domestic financial institutions and domestic financial agencies to take certain "special measures." Regarding the "special measures" that might be imposed, section 9714 references the five special measures set out in 31 U.S.C. 5318A(b)(1)-(5).
[6] 31 U.S.C. 5318A(b)(1)-(4).

account or payable-through account" for or on behalf of a foreign banking institution, if such correspondent account or payable-through account involves the financial institution operating outside of the United States found to be of primary money laundering concern.[7] In addition to the special measures set out in 31 U.S.C. 5318A, section 9714 also provides that the Secretary may impose a special measure prohibiting, or imposing conditions upon, certain transmittals of funds.[8]

B. MEXC Global

MEXC Global is a CVC exchanger founded in 2018 that is incorporated in the Seychelles, without a virtual asset service provider license[9] and operates in and across over 170 countries[10] through an array of current or former subsidiaries, branches, and offices, including, but not limited to, MEXC Global Ltd and MX Global Ltd in Seychelles; MEXC Estonia OÜ in Estonia; GIDA Technology AG in Switzerland; MXC Global Ltd in the United Kingdom; and, formerly, Singapore-registered MEXC Global Foundation Ltd and MEXC Singapore Pte Ltd.[11]

As of June 2026, MEXC Global processed more than USD 1 billion in daily transactions, while maintaining approximately USD 5 billion in reserve assets. As such, MEXC Global is among the 20 largest CVC exchangers in the world by trading volume.[12] As of December 2025, MEXC Global commanded approximately nine percent of the global market share of centralized

[7] 31 U.S.C. 5318A(b)(5).
[8] *See* section 9714(a)(2).
[9] *See* Financial Services Authority Seychelles, *Press Release - FSA Takes Enforcement Action Against MX Global Ltd for Unlicensed Virtual Asset Services Operations* (May 26, 2026), https://fsaseychelles.sc/news/press-releases/fsa-takes-enforcement-action-against-mx-global-ltd-for-unlicensed-virtual-asset-services-operations.
[10] *See* CoinPedia, *MEXC Overview,* https://app.coinpedia.org/company/mexc/.
[11] TRM Labs, *MEXC Global* (accessed Jun. 3, 2026). MEXC Global was formerly known as MXC before rebranding in 2021. *See* MEXC Global, "MXC Exchange Rebranded MEXC Global, Deepening its Global Compliance Strategy," Medium (June 10, 2021).
[12] *See* CoinPedia, *Top Crypto Exchanges By Trading Volume,* https://markets.coinpedia.org/exchanges/.

CVC exchangers by trading volume.[13] By comparison, the assets of the two largest centralized CVC exchangers together represented 47.4 percent of the global market share.[14]

According to its user agreement, MEXC Global allows customers to open user accounts for exchange between various fiat currencies and CVC, as well as for futures trading and other services.[15] And, according to non-public information available to FinCEN, as of July 2026, MEXC Global offers the ability to trade in over fifty currencies, including USD and Russian rubles (RUB), as well as access to over 3,000 different CVCs and tokenized assets.

III. Finding that MEXC Global is a Financial Institution Operating Outside the United States that is of Primary Money Laundering Concern in Connection with Russian Illicit Finance

Based on public and non-public information available to FinCEN, FinCEN finds that reasonable grounds exist for concluding that MEXC Global is a financial institution of primary money laundering concern in connection with Russian illicit finance—namely, through its facilitation of funds transfers by Russia-affiliated illicit actors and in connection with other Russia-associated illicit activities, including sanctions evasion, and activity facilitated by Russian darknet markets. Moreover, FinCEN assesses that, in addition to facilitating Russian illicit finance, MEXC Global has, in parallel, facilitated billions of dollars in transactions benefitting Iran and its proxies, financial facilitators of the Democratic People's Republic of Korea (DPRK), and other cybercrime actors.

In making this finding, FinCEN has considered the relevant evidence in light of factors identified in 31 U.S.C. 5318A(c)(2)(B), taking into account the specific circumstances of money

[13] *See* CoinGecko, *Market Share of Centralized Crypto Exchanges, by Trading Volume* (May 2, 2026), https://www.coingecko.com/research/publications/centralized-crypto-exchanges-market-share.
[14] *See* CoinGecko, *Market Share of Centralized Crypto Exchanges, by Trading Volume* (May 2, 2026), https://www.coingecko.com/research/publications/centralized-crypto-exchanges-market-share.
[15] *See* MEXC, *User Agreement* (May 29, 2025), https://www.mexc.com/terms.

laundering activities in connection with Russian illicit finance and the protection of U.S. national security and the U.S. financial system. While FinCEN is under no obligation pursuant to section 9714 to consider any particular factor or set of factors when making a finding that a financial institution operating outside of the United States is of primary money laundering concern in connection with Russian illicit finance, it nonetheless finds these factors instructive in guiding the analysis set forth below.[16]

A. MEXC Global is a Financial Institution Operating Outside the United States

Although section 9714 does not expressly define the term "financial institution," FinCEN has long defined that term to include "money transmitters," including persons that accept and transmit value that substitutes for currency, such as CVC.[17] MEXC Global, in operating as a CVC exchanger, is a "money transmitter" because it is engaged in the transfer of funds or value that substitutes for currency.[18]

By its own account and as described above, MEXC Global operates through affiliates throughout the world—over time maintaining, for instance, subsidiaries, branches, and offices in Seychelles, Hong Kong, Singapore, Estonia, and the United Kingdom—and offers a range of

[16] 31 U.S.C. 5318A(c)(2)(B) provides, as relevant here, that in making a finding that reasonable grounds exist for concluding that a class of transactions within, or involving, a jurisdiction outside the United States is of primary money laundering concern and to apply one or more of special measures one through four to such a financial institution, the Secretary shall consider such information as the Secretary determines to be relevant, including the following potentially relevant factors:

(1) The extent to which such financial institutions, transactions, or types of accounts are used to facilitate or promote money laundering in or through the jurisdiction, including any money laundering activity by organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction or missiles;
(2) The extent to which such institutions, transactions, or types of accounts are used for legitimate business purposes in the jurisdiction; and
(3) The extent to which such action is sufficient to ensure, with respect to transactions involving the jurisdiction and institutions operating in the jurisdiction, that the purposes of this subchapter continue to be fulfilled, and to guard against international money laundering and other financial crimes.

[17] *See, e.g.*, 31 U.S.C. 5312; 31 CFR 1010.100(t)(3); 1010.100(ff); 1010.605(f)(iv); FinCEN, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019); FinCEN, FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013); *see also* 31 U.S.C. 5312(a)(2)(J).

[18] *See* 31 CFR 1010.100(t)(3), (ff)(5).

money transmitter services for individual and institutional customers in the CVC sector in over 170 countries.[19] Considering the services that it provides and its places of registration, FinCEN assesses that MEXC Global is a financial institution operating outside of the United States within the meaning of section 9714.

Notably, to the extent that MEXC Global maintains or otherwise operates through affiliates, subsidiaries, branches, or offices in the United States, this order expressly excludes all such affiliates, subsidiaries, branches, or offices from the definition of "MEXC Global" and, accordingly, such affiliates, subsidiaries, branches, or offices are outside the scope of this order.

B. Finding That MEXC Global is a Financial Institution of Primary Money Laundering Concern in Connection with Russian Illicit Finance

While MEXC Global's anti-money laundering and countering the financing of terrorism (AML/CFT), customer identification and verification (sometimes referred to as "Know Your Customer" or "KYC" information), and other due diligence processes[20] prohibit, on paper, the opening of accounts by individuals in certain jurisdictions, FinCEN assesses that, based on public and non-public information, MEXC Global has facilitated transactions involving those prohibited jurisdictions. In addition, MEXC Global has facilitated transactions involving Russia-affiliated illicit actors and associated illicit activities, including sanctions evasion, and activity facilitated by Russian darknet markets, as well as transactions involving not only U.S.-, European Union-, and United Kingdom-sanctioned persons working on behalf of Iran and its proxies and the DPRK, but also an array of cybercrime actors.

---

[19] *See* CoinPedia, *MEXC Overview,* https://app.coinpedia.org/company/mexc/.

[20] While MEXC publicly claims to have certain AML/CFT processes in place, FinCEN assesses that any such processes, procedures, and policies, to the extent they exist, are insufficient and have failed to prevent substantial volumes of illicit finance involving Russia-affiliated illicit actors and associated illicit activities, including sanctions evasion, and activity facilitated by Russian darknet markets, as well as transactions involving not only U.S.-, EU-, and UK-sanctioned persons working on behalf of Iran and its proxies and the DPRK, but also an array of cybercrime actors. *See* MEXC, *User Agreement* (May 29, 2025), https://www.mexc.com/terms.

Notwithstanding MEXC Global's AML/CFT and other due diligence processes, FinCEN found that MEXC Global has skirted compliance with applicable regulatory requirements[21]—multiple nations' financial regulators have issued notices highlighting that MEXC Global has operated in their jurisdictions without the proper license, and in at least one case added the CVC exchanger to a list of suspicious CVC trading platforms[22]—and, importantly, that, between May 2021 and May 2026, MEXC Global facilitated the movement of USD 16.7 billion in funds connected to Russian illicit finance and other illicit activities, including sanctions evasion and cybercrime, posing a significant threat to the U.S. financial system. Indeed, within those transactions, FinCEN identified numerous instances in which MEXC Global processed transactions in violation of its own user agreement, including direct transactions between MEXC Global and sanctioned actors, some of whom were operating from MEXC Global's list of prohibited jurisdictions.[23]

1. *MEXC Global is used in furtherance of sanctions evasion in connection with Russian illicit finance*

MEXC Global has a history of processing CVC transfers for multiple key actors that support Russian illicit finance. According to FinCEN analysis of blockchain data, between May 2021 and May 2026, MEXC Global sent or received nearly USD 1.5 billion in direct and indirect exposure to transactions linked to Russian sanctions evasion and had significant exposure to

[21] MEXC Global has been the subject of regulatory scrutiny and has been found to be operating without a license in Seychelles, Hong Kong, and Japan. *See* Financial Services Authority Seychelles, *Press Release - FSA Takes Enforcement Action Against MX Global Ltd for Unlicensed Virtual Asset Services Operations* (May 26, 2026), https://fsaseychelles.sc/news/press-releases/fsa-takes-enforcement-action-against-mx-global-ltd-for-unlicensed-virtual-asset-services-operations; Hong Kong Securities and Futures Commission, *SFC Warns Public Against Unlicensed Virtual Asset Trading Platform MEXC* (Mar. 15, 2024), https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=24PR48; Japanese Financial Services Agency, *FSA Weekly Review No. 533* (Apr. 13, 2023), https://www.fsa.go.jp/en/newsletter/weekly2023/533.html.

[22] *See* Japanese Financial Services Agency, Newsletter, *FSA Weekly Review No.533* (Apr. 13, 2023), https://www.fsa.go.jp/en/newsletter/weekly2023/533.html.

[23] MEXC, *User Agreement* (May 29, 2025), https://www.mexc.com/terms.

Russian cyber actors connected to sanctions evasion and/or cybercrime. This includes USD 232 million in direct transactions with entities sanctioned by the United States, the European Union (EU), and/or the United Kingdom (UK).[24] For example, MEXC Global transacted with the sanctioned, Russia-backed CVC exchangers Garantex and Grinex. Between 2019 and 2025, Garantex facilitated the movement of over USD 100 million for ransomware actors and other cybercriminals.[25] Garantex's successor entity, Grinex, is itself a vehicle for sanctions evasion, as it was created by Garantex employees to move funds after Garantex was designated by OFAC for operating in Russia's financial services sector.[26] Following these public designations, MEXC Global directly facilitated approximately USD 129 million in activity with Garantex and USD 4.1 million in activity with Grinex, and MEXC Global continued to transact with both entities as recently as June 2026. Similarly, MEXC Global transacted with components of the Russia-based A7 Network,[27] a self-described sanctions-resistant payment service provider created by the U.S.-,

[24] *See* Treasury, Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701; European Commission, EU Sanctions Tracker, *Grinex* (Oct. 23, 2025), https://data.europa.eu/apps/eusanctionstracker/subjects/179375; European Commission, EU Sanctions Tracker, *Garantex* (Feb. 24, 2025), https://data.europa.eu/apps/eusanctionstracker/subjects/172907; Foreign Commonwealth Development Office, *UK targets sanctions circumvention and crypto networks exploited by Russia* (Aug. 20, 2025), https://www.gov.uk/government/news/uk-targets-sanctions-circumvention-and-crypto-networks-exploited-by-russia.

[25] *See* Treasury, Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.

[26] *See* Treasury, Press Release, *Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals* (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0225.

[27] The core of the A7 Network is formed by three Russia-based companies—A7 Liability Company (A7 LLC), and its subsidiaries, A71 Limited Liability Company (A71 LLC) and A7 Agent Limited Liability Company (A7 Agent LLC)—which are jointly owned by Ilan Shor and PSB and subject to sanctions imposed by the United States, European Union, and United Kingdom. These entities administer the network with and through several Russia- and Kyrgyz Republic-based persons, including businesses and digital asset exchanges subject to sanctions imposed by OFAC and the UK (as well as, in most cases, the EU), including Old Vector LLC, Garantex, Grinex, Independent Decentralized Finance Smartbank and Ecosystem (InDeFi Bank), ExVed, and Garantex co-founder Sergey Mendeleev (Mendeleev). *See* FinCEN, NPRM, *Proposal of Special Measure Prohibiting the Transmittal of Funds Regarding Transactions Involving the A7 Network's Sub-Agents*, 91 FR 63208 (Oct. 5, 2026).

EU- and UK-designated Moldovan oligarch Ilan Shor[28] and Russia's state-owned defense bank Promsvyazbank Public Joint Stock Company (PSB),[29] that has evolved into a conduit for illicit activity associated with a wide range of threat actors, including the Islamic Revolutionary Guard Corps (IRGC) and its Quds Force, DPRK-affiliated actors; Iran-backed terrorist organizations; and cybercriminals and ransomware actors.[30] Significantly, OFAC has designated the founders and core components and enablers of the A7 Network, and recently designated the A7 Network, itself, as a significant transnational criminal organization.[31] Further, FinCEN recently found that transactions involving any company operating outside of the United States that is controlled by the A7 Network belong to a class of transactions of primary money laundering concern in connection with Russian illicit finance.[32] Based on analysis of blockchain data, FinCEN assesses

[28] Ilan Shor was designated by OFAC in October 2022, pursuant to E.O. 14024, for his involvement in Russian malign influence operations in Moldova. He was previously arrested on money laundering and embezzlement charges related to a 2014 theft valued at approximately USD 1 billion from Moldovan banks. Treasury, Press Release, *Treasury Targets Corruption and the Kremlin's Malign Influence Operations in Moldova* (Oct. 26, 2022), https://home.treasury.gov/news/press-releases/jy1049. Ilan Shor was also sanctioned by the United Kingdom on December 8, 2022. *See* UK Foreign, Commonwealth and Development Office (FCDO), Uk Sanctions List, https://search-uk-sanctions-list.service.gov.uk/designations/GAC0029/Individual.

[29] PSB was designated by OFAC in February 2022, pursuant to E.O. 14024, for issuing billions of dollars in financial support for Russian defense sector companies in its role as Russia's state defense bank. Treasury, Press Release, *U.S. Treasury Imposes Immediate Economic Costs in Response to Actions in the Donetsk and Luhansk Regions* (Feb. 22, 2022), https://home.treasury.gov/news/press-releases/jy0602. PSB was later redesignated in January 2025, pursuant to E.O. 13662, for operating in the financial services sector of the Russian Federation economy. Treasury, Press Release, *Treasury Disrupts Russia's Sanctions Evasion Schemes* (Jan. 15, 2025), https://home.treasury.gov/news/press-releases/jy2785; *see also* Open Source Centre, *The Big Shor: A7 and the Illusion of Russian Financial Innovation* (2026), at. p. 9, https://static.opensourcecentre.org/assets/osc_a7_big_shor.pdf.

[30] *See generally* TRM Labs, "The A7 Leaks: TRM's On-Chain Analysis of Russia's Cryptocurrency Connections" (June 12, 2026). The A7 Network allows companies to transact in both fiat currency and CVC through complex trade-based money laundering schemes using a network of overseas sub-agents to enable sanctioned and other illicit actors to access the international financial system. *See generally* TRM Labs, *The A7 Leaks: TRM's On-Chain Analysis of Russia's Cryptocurrency Connections* (June 12, 2026), https://www.trmlabs.com/resources/blog/the-a7-leaks-trms-on-chain-analysis-of-russias-cryptocurrency-connections.

[31] On October 1, 2026, Treasury's Office of Foreign Assets Control (OFAC) sanctioned the A7 Network pursuant to Executive Order 13581, as amended by Executive Order 13863, for being a foreign person that constitutes a significant Transnational Criminal Organization. *See* Treasury, Press Release, *Operation Economic Outcast Takes Unprecedented Action Against Sanctions Evasion Network Used by Iran* (Oct. 1, 2026) https://home.treasury.gov/news/press-releases/sb0644/.

[32] *See* FinCEN, NPRM, *Proposal of Special Measure Prohibiting the Transmittal of Funds Regarding Transactions Involving the A7 Network's Sub-Agents*, 91 FR 63208 (Oct. 5, 2026); *see also* 31 CFR 1010.668.

that MEXC Global facilitated the transmission of at least USD 26 million benefitting the now sanctioned A7 Network and sent or received almost USD 200 million connected to the A7A5 token (a ruble-backed stablecoin that operates on the Tron and Ethereum blockchains[33] to transfer value across A7 Network-linked actors where banking channels are restricted or less dependable),[34] including its issuer Old Vector LLC and owner Ilan Shor, both sanctioned by OFAC, as well as the European Union and the United Kingdom.[35]

In addition, MEXC Global has repeatedly transacted with high-risk CVC exchangers that have been sanctioned or that allegedly have no customer identification verification requirements. For example, between May 2018 and July 2026, MEXC Global directly facilitated transactions cumulatively worth over USD 13 billion with at least four high-risk CVC exchangers sanctioned by the UK for facilitating Russian sanctions evasion and funding Russian military operations in Ukraine. [36] Between May 2021 and May 2026, it also processed approximately USD 2.9 billion

---

[33] The A7A5 tokens operate from smart contracts with addresses at 0x6fA0BE17e4beA2fCfA22ef89BF8ac9aab0AB0fc9 and TLeVfrdym8RoJreJ23dAGyfJDygRtiWKBZ. *See* https://etherscan.io/token/0x6fA0BE17e4beA2fCfA22ef89BF8ac9aab0AB0fc9#code; https://tronscan.org/token20/TLeVfrdym8RoJreJ23dAGyfJDygRtiWKBZ/code. Stablecoins are a type of digital asset for which the value of the token is tied to another asset, typically a fiat currency such as the U.S. dollar. Stablecoins are appealing to illicit actors due to their relative liquidity, ease of settlement, and exchange rate stability. *See* Treasury, *2026 National Proliferation Financing Risk Assessment* (Mar. 2026), at p. 16, https://home.treasury.gov/system/files/246/2026-NPFRA.pdf; *see also* Treasury, *2026 National Money Laundering Risk Assessment* (Mar. 2026), at pp. 52–53, https://home.treasury.gov/system/files/246/2026-NMLRA.pdf.

[34] *See* Treasury, Press Release, *Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals* (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0225.

[35] *See* Treasury, Press Release, *Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals* (Aug. 14, 2025), https://home.treasury.gov/news/press-releases/sb0225; Foreign Commonwealth Development Office, *UK targets sanctions circumvention and crypto networks exploited by Russia* (Aug. 20, 2025), https://www.gov.uk/government/news/uk-targets-sanctions-circumvention-and-crypto-networks-exploited-by-russia; Treasury, Press Release, *Treasury Targets Corruption and the Kremlin's Malign Influence Operations in Moldova* (Oct. 26, 2022), https://home.treasury.gov/news/press-releases/jy1049; UK Foreign, Commonwealth & Development Office (FCDO), UK Sanctions List, *Ilan Shor*, https://search-uk-sanctions-list.service.gov.uk/designations/GAC0029/Individual; European Commission, EU Sanctions Tracker, *Ilan Shor* (May 30, 2023), https://data.europa.eu/apps/eusanctionstracker/subjects/153809; European Commission, EU Sanctions Tracker, *Limited Liability Company Old Vector* (Oct. 23, 2025), https://data.europa.eu/apps/eusanctionstracker/subjects/179337.

[36] *See* FCDO, *Sanctions Notice: 26 May 2026 Regime: Russia* (May 26, 2026), https://assets.publishing.service.gov.uk/media/6a2a9de71f6fa5c3377e5da7/Sanctions_Notice_Russia_26_May_2026.pdf.

in direct transactions with Russian and other CVC exchangers that allegedly do not collect customer identification and verification information, which poses a high risk of transacting with sanctioned entities and individuals and for otherwise engaging in illicit activity. In addition, between September 2020 and July 2026, MEXC Global facilitated USD 8.5 million in transactions involving Russian darknet markets that are known to facilitate the sale of illicit goods and services.

Based on MEXC Global's facilitation of transactions for sanctioned and high-risk Russian CVC exchangers, including the A7 Network, which are widely known to move funds for sanctioned actors, cybercriminals, and ransomware actors, FinCEN assesses that MEXC Global is a financial institution of primary money laundering concern in connection with Russian illicit finance.

2. *MEXC Global is used in furtherance of international money laundering*

According to public and non-public information, MEXC Global also facilitates activity in furtherance of international money laundering in support of Iran and its proxies, financial facilitators of the DPRK, and cybercrime.

a. *MEXC Global facilitated transactions involving Iran and its proxies*

According to FinCEN analysis of blockchain information, between May 2021 and May 2026, MEXC Global facilitated the transmission of nearly USD 2 billion connected to identified Iranian actors or known or suspected terrorist groups, including approximately USD 1.87 billion in transactions with exposure to Iran, a jurisdiction that is the subject of comprehensive U.S. sanctions[37] and special measures imposed by FinCEN pursuant to section 311 of the USA

[37] The United States maintains comprehensive sanctions on Iran, which prohibit most transactions and activities with Iran by U.S. persons or within the United States, unless exempt or authorized by Treasury's Office of Foreign Assets Control (OFAC). For more information, *see* OFAC, *Iran Sanctions*, https://ofac.treasury.gov/sanctions-programs-and-country-information/iran-sanctions.

PATRIOT Act (31 U.S.C. 5318A) which prohibit covered financial institutions from opening or maintaining correspondent accounts in the United States for, or on behalf of, Iranian financial institutions.[38] Despite the fact that MEXC Global's user agreement states that individuals and entities located in Iran are not allowed to use its platform, FinCEN assesses that over USD 1 billion of this exposure took the form of direct transactions between MEXC Global and more than 40 identified Iranian CVC exchangers, some of which are the subject of U.S. and international sanctions. Between May 2021 and May 2026, FinCEN assesses that MEXC Global also facilitated the transmission of approximately USD 22 million in transactions associated with the U.S.- and EU-sanctioned Central Bank of Iran and the U.S.-, EU-, and UK-sanctioned IRGC and its Quds Force.[39]

MEXC Global has also been exploited by multiple Iran proxy groups. For example, FinCEN identified approximately USD 36 million in transactions that occurred between May 2021 and May 2026 that went to or from MEXC Global related to the Gaza-based U.S.- and UK-sanctioned Al-Qassam Brigades and other Iran linked terrorist groups.[40]

---

[38] *See* FinCEN, *Imposition of Fifth Special Measure Against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern,* 84 FR 59302 (Nov. 14, 2019); *see also* 31 CFR 1010.661.

[39] *See* Treasury, Press Release, *Treasury Sanctions Iran's Central Bank and National Development Fund* (Sept. 20, 2019), https://home.treasury.gov/news/press-releases/sm780; European Commission, EU Sanctions Tracker, *Central Bank of Iran* (Sept. 29, 2025), https://data.europa.eu/apps/eusanctionstracker/subjects/178339; Treasury, Press Release, *Treasury Designates the IRGC under Terrorism Authority and Targets IRGC and Military Supporters under Counter-Proliferation Authority* (Oct. 13, 2017), https://home.treasury.gov/news/press-releases/sm0177; FCDO, UK Sanctions List, *Islamic Revolutionary Guard Corps Quds Force* (Dec. 31, 2020), https://search-uk-sanctions-list.service.gov.uk/designations/INU0082/Entity; European Commission, EU Sanctions Tracker, *IRGC* (July 26, 2010), https://data.europa.eu/apps/eusanctionstracker/subjects/5760.

[40] *See, e.g.*, OFAC, *SDGT designations* (Nov. 2, 2001), https://ofac.treasury.gov/recent-actions/20011102; FCDO, UK Sanctions List, *Hamas including Izz al-Din al-Qassam Brigades* (Dec. 31, 2020), https://search-uk-sanctions-list.service.gov.uk/designations/CTI0031/Entity.

b. *MEXC Global facilitated transactions involving financial facilitators of the DPRK*

MEXC Global has also transmitted funds on behalf of a financial facilitator of the DPRK, a jurisdiction that, like Iran, is the subject of comprehensive U.S. sanctions[41] and special measures imposed by FinCEN that prohibit covered financial institutions from opening or maintaining correspondent accounts in the United States for, or on behalf of, DPRK financial institutions.[42] For instance, FinCEN assesses that MEXC Global facilitated U.S.-sanctioned DPRK money launderer Sim Hyon Sop's receipt of approximately USD 350,000 between June and September 2025, more than two years after Sop had been designated by OFAC and even though, as part of his April 2023 designation, OFAC specifically identified and sanctioned his CVC addresses.[43]

c. *MEXC Global facilitated transactions connected to cybercrime*

Finally, MEXC Global frequently processes transactions connected to cyber-enabled crimes, ranging from darknet marketplace activity (including the Russian darknet marketplace activity discussed above) and ransomware payments to scam proceeds and stolen funds. Between May 2021 and May 2026, FinCEN assesses that at least USD 1.99 billion in funds originating from or moving to illicit cyber actors moved through MEXC Global, an average of more than USD 1 million per day. Between January 2022 to July 2024, MEXC Global received more than USD 37.9 million in suspected ransomware payments, with exposure to over 125

[41] The United States maintains comprehensive sanctions on the DPRK, which prohibit most transactions and activities with the DPRK by U.S. persons or within the United States, unless exempt or authorized by OFAC. For more information, *see* OFAC, *North Korea Sanctions,* https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions.

[42] *See* FinCEN, *Imposition of Fifth Special Measure Against North Korea as a Jurisdiction of Primary Money Laundering Concern,* 81 FR 78715 (Nov. 9, 2016); *see also* 31 CFR 1010.659.

[43] *See* Treasury, Press Release, *Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs* (Apr. 24, 2023), https://home.treasury.gov/news/press-releases/jy1435.

ransomware variants. MEXC Global also hosts a particularly high-use ransomware-related deposit address, which received over USD 1.17 million during the same period.

C. The Extent to Which MEXC Global is Used for Legitimate Business Purposes

In reaching its finding that MEXC Global is a financial institution operating outside the United States of primary money laundering concern in connection with Russian illicit finance, FinCEN considered the extent to which MEXC Global is used for legitimate business purposes.[44] As of June 2026, MEXC Global conducted USD 1 billion in daily transactions, putting it among the top 20 largest CVC exchangers in the world by trading volume. Although FinCEN does not have full insight into the scope of MEXC Global's legitimate activities, for the purposes of this action, FinCEN assumes that a portion of MEXC Global's business activities are legitimate. However, FinCEN assesses that since May 2021, MEXC Global has facilitated at least USD 16.7 billion in likely illicit activity. Accordingly, any legitimate business conducted by MEXC Global is outweighed by the risks posed by MEXC Global's facilitation of illicit activity, including sanctions evasion by Russia and Iran, and the need to protect the U.S. financial sector from the money laundering and terrorist financing risks presented by MEXC Global.

D. The Extent to Which This Action Would Guard Against International Money Laundering and Other Financial Crimes Associated with Russian Illicit Finance

A finding that MEXC Global is of primary money laundering concern in connection with Russian illicit finance establishes—and emphasizes—the significant illicit finance risks posed by MEXC Global's provision of financial services to the Russian illicit finance ecosystem, Russian and other darknet markets and high-risk exchanges. Further, notwithstanding MEXC Global's ties to Russian illicit finance, FinCEN assesses that it has facilitated over USD 1.87 billion in transactions with exposure to Iran, including over USD 1 billion in direct transactions between

[44] *See* 31 U.S.C. 5318A(c)(2)(B)(ii).

MEXC Global and Iranian CVC exchangers, as well as transactions benefiting the DPRK and an array of illicit cyber actors, each of which present significant risks to the U.S. financial system. Accordingly, this order will place U.S. and foreign financial institutions and regulators on notice to guard against those risks. Moreover, such a finding—in combination with a prohibition on certain transmittals of funds involving MEXC Global by covered financial institutions—will help safeguard the U.S. financial system by severing MEXC Global's access.

IV. Imposition of a Special Measure Prohibiting Certain Transmittals of Funds Involving MEXC Global

Having found that MEXC Global is a financial institution operating outside of the United States that is of primary money laundering concern in connection with Russian illicit finance, FinCEN has determined that the imposition of a special measure prohibiting certain transmittals of funds involving MEXC Global is warranted.[45] In making this determination and assessing which special measures may be appropriate, FinCEN has considered the relevant evidence in light of factors identified in 31 U.S.C. 5318A(a)(4)(B). While FinCEN is under no obligation pursuant to section 9714 to consider any particular factor or set of factors in selecting one or more special measures, it nonetheless finds these factors instructive in guiding the analysis set forth below.[46]

[45] In connection with this action, and consistent with 31 U.S.C. 5318A(a)(4)(A), FinCEN shared a draft of this order with staff at the following Departments and agencies with regard to the proposed order and prohibition: the Department of Justice; the Department of State; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Securities and Exchange Commission; the Commodity Futures Trading Commission; the Office of the Comptroller of the Currency; and the National Credit Union Administration. None of the Departments or agencies objected to the issuance of this order based on the information provided to staff at the time.

[46] 31 U.S.C. 5318A(a)(4)(B) provides, as relevant here, that in selecting which special measure(s) to take, the Secretary shall consider:

(1) whether similar action has been or is being taken by other nations or multilateral groups;
(2) whether the imposition of any particular special measure would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States;

A. Whether the Prohibition Would Address the Money Laundering Concern in a Manner Consistent with U.S. National Security and Foreign Policy Interests

FinCEN has considered the effect this action will have on U.S. national security and foreign policy, as well as the extent to which multilateral groups or other nations have taken similar actions.[47] FinCEN has found that, in addition to facilitating Russian illicit financial activity and sanctions evasion schemes and serving as a high-density transactional node for high-risk CVC exchangers, MEXC Global plays a broader role in facilitating transactions for a diverse range of transnational illicit actors. In particular, MEXC Global processes transactions connected to Iranian sanctions evasion, terrorist financing, and the laundering of scam and ransomware proceeds. FinCEN, therefore, assesses that imposing a prohibition on certain transmittals of funds involving MEXC Global is necessary to safeguard U.S. national security and the U.S. financial system, as well as to serve key U.S. national security objectives.

In light of the quantity and volume of transactions linked to known or suspected illicit activity processed through MEXC Global, prohibiting certain transmittals of funds involving MEXC Global would insulate the U.S. financial system from money laundering and other financial crimes. In particular, prohibiting certain transmittals of funds involving MEXC Global would further ongoing U.S. efforts to curtail suspected Russia-associated illicit activity and financial transactions. And, targeting illicit proceeds moved by sanctions evasion networks, especially those with a nexus to Iran, is of highest priority for the United States. Consequently, prohibiting certain transmittals of funds involving MEXC Global will serve the U.S. national

(3) the extent to which the action or the timing of the action would have a significant adverse systemic impact on the international payment, clearance, and settlement system, or on legitimate business activities involving the particular jurisdiction, institution, class of transactions, or type of account; and

(4) the effect of the action on United States national security and foreign policy.

[47] *See* 31 U.S.C. 5318A(a)(4)(B)(i), (iv).

security and foreign policy interests by protecting the U.S. and international financial system from known threat actors.

Moreover, this action reinforces the expectations of AML/CFT compliance in the financial system, highlighting the importance of identifying and reporting suspicious activity by financial institutions around the world. With respect to the illicit finance risks posed by MEXC Global, that is of particular importance, as this order addresses primary money laundering concerns that are still ongoing after multiple jurisdictions' financial regulators have issued notices highlighting that MEXC Global has operated in their jurisdictions without the proper license, and in at least one case added the CVC exchanger to a list of suspicious CVC trading platforms.[48]

B. Whether the Prohibition of Certain Transmittals of Funds Would Impose Undue Burdens on Legitimate Activity of MEXC Global or Third Parties

FinCEN has considered whether prohibiting certain transmittals of funds would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organized or licensed in the United States, as well as the extent to which the action could have a significant adverse systemic impact on legitimate business activities currently being conducted on the MEXC Global platform.[49] Indeed, while MEXC Global is used by licit actors, the legitimate business services that it offers are commonly

[48] MEXC Global has been the subject of regulatory scrutiny and has been found to be operating without a license in the Seychelles, Hong Kong, and Japan. *See* Financial Services Authority Seychelles, *Press Release - FSA Takes Enforcement Action Against MX Global Ltd for Unlicensed Virtual Asset Services Operations* (May 26, 2026), https://fsaseychelles.sc/news/press-releases/fsa-takes-enforcement-action-against-mx-global-ltd-for-unlicensed-virtual-asset-services-operations; Hong Kong Securities and Futures Commission, *SFC Warns Public Against Unlicensed Virtual Asset Trading Platform MEXC* (Mar. 15, 2024), https://apps.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=24PR48; Japanese Financial Services Agency, *FSA Weekly Review No. 533* (Apr. 13, 2023), https://www.fsa.go.jp/en/newsletter/weekly2023/533.html.
See Japanese Financial Services Agency, Newsletter, *FSA Weekly Review No.533* (Apr. 13, 2023), https://www.fsa.go.jp/en/newsletter/weekly2023/533.html.

[49] *See* 31 U.S.C. 5318A(a)(4)(B)(ii), (iii).

offered by other regulated institutions, meaning that such licit actors could readily find alternatives to facilitate business.

And, FinCEN assesses that prohibiting certain transmittals of funds involving MEXC Global will not present a significant competitive disadvantage for or put an undue burden on financial institutions organized or licensed in the United States. Compliance with the prohibition on certain transmittals of funds set out in this order requires no tools or competencies other than those already employed by domestic financial institutions to maintain their current AML/CFT compliance programs. To aid covered U.S. financial institutions with compliance, FinCEN has elected to provide within this order for the rejection of certain transmittals of CVC that are received from or originate at MEXC Global and outline the steps a covered financial institution should take in such circumstances. In providing for the rejection of CVC under certain limited circumstances, FinCEN acknowledges that, at this time, there are technological limitations that may limit or preclude covered financial institutions from declining CVC transfers originating at addresses outside of their control, and compliant institutions may find themselves in receipt of CVC from MEXC Global despite a desire and effort to limit such exposure.[50] This order therefore allows covered financial institutions the flexibility to act with discretion based on the facts and circumstances of a particular transaction and comply with this order, even where the originating address is no longer accessible, where, for example, (1) CVC transfers originated from MEXC Global, but were held for an extended period of time in an unhosted wallet, or (2) the covered financial institution's risk mitigation procedures would preclude returning funds to

[50] FinCEN notes that CVC payment systems are often designed to limit the control of specific financial institutions over transactions and to prevent rejection of funds by persons or entities other than the sender of funds. As a result, although covered financial institutions may institute an internal prohibition on the sending of CVC transactions to another address or entity, FinCEN assesses that there are few, if any, readily available ways for covered financial institutions to "reject" incoming CVC transactions (prior to receipt).

MEXC Global. Moreover, by providing for the rejection of CVC, this order ensures that covered financial institutions will not be subject to an undue cost or burden associated with compliance.

C. Whether Any Other Reasonable Alternatives or Special Measures Would Adequately Address the Money Laundering Concern

Before deciding to impose a prohibition on certain transmittals of funds, FinCEN considered other available special measures.[51] After due consideration, FinCEN has determined that a special measure prohibiting certain transmittals of funds involving MEXC Global is the appropriate means to adequately address the illicit finance risks posed by MEXC Global.

None of the special measures set out in 31 U.S.C. 5318A—special measures one through five—would effectively address the illicit finance threat posed by MEXC Global. Any additional recordkeeping, information collection, or reporting requirements, as described in 31 U.S.C 5318A(b)(1)-(4), would be insufficient to guard against the risks posed by covered financial institutions processing transmittals of funds involving MEXC Global. Those special measures would allow such transfers to continue to the benefit of illicit actors connected to Russian illicit finance, as well as Iran-related and other illicit financial activity. Further, merely prohibiting and/or placing conditions upon the opening or maintaining in the United States of correspondent accounts or payable-through accounts for or on behalf of MEXC Global, as described in 31 U.S.C 5318A(b)(5), would be similarly inadequate. Neither prohibiting nor imposing conditions on such accounts would safeguard the U.S. financial system to the same degree as prohibiting transmittals of funds, as such a special measure would not address the movement of funds outside of a strict correspondent or payable-through relationship, for

[51] As noted in section II.A, pursuant to section 9714, these measures include: (1) the special measures described in 31 U.S.C. 5318A(b), including the imposition of additional recordkeeping, information collection, and reporting requirements on covered U.S. financial institutions and/or the imposition of conditions upon the opening or maintaining of correspondent or payable-through accounts for or on behalf of a foreign banking institution; and (2) the prohibition of, or imposition of conditions on, the transmittal of funds.

example, through the movement of funds outside the traditional banking relationship, which may permit MEXC Global to access USD through indirect correspondent relationships via other foreign financial institutions.

D. Whether the Prohibition Should be Imposed by Order or Regulation

Pursuant to section 9714, the Secretary may impose one or more special measures, including a prohibition on certain transmittals of funds, "by order, regulation or otherwise as permitted by law." In determining the appropriate approach in this instance, FinCEN considered imposing the prohibition by order or regulation, taking into account the nature of the underlying threat, and determined that proceeding by an order is the most appropriate course of action given the imminent threats posed by the illicit actors whose transactions and access to funds MEXC Global facilitates, as well as the ongoing transactions associated with suspected activity related to Russian illicit finance that continue to be processed through MEXC Global. Further, FinCEN has assessed that this order will not be unduly burdensome or impose new or unique compliance costs on financial institutions.

A copy of this order will be published in the Federal Register. To the extent MEXC Global or other parties have information relevant to this order, they may submit it to FinCEN at www.fincen.gov/contact.

V. Executive Order 14294

Section 5 of Executive Order 14294 directs that all future notices of proposed rulemaking (NPRMs) and final rules published in the *Federal Register*, the violation of which may constitute criminal regulatory offenses, should include a statement identifying that the rule or proposed rule

is a criminal regulatory offense and the authorizing statute.[52] Executive Order 14294 directs agencies to draft this statement in consultation with the Department of Justice.

Executive Order 14294 further directs that the regulatory text of all NPRMs and final rules with criminal consequences published in the *Federal Register* after May 9, 2025, should explicitly state a mens rea requirement for each element of a criminal regulatory offense, accompanied by citations to the relevant provisions of the authorizing statute.

Willful violations of any final regulations set forth in this order may be subject to criminal penalties pursuant to 31 U.S.C. 5322 and regulations promulgated in 31 CFR Chapter X. The statutory authority for criminal liability requires a mens rea of willfulness as an element pursuant to 31 U.S.C. 5322(a) and 31 U.S.C. 5322(b). FinCEN's existing regulation, 31 CFR 1010.840, that sets out criminal penalties for violations of regulations promulgated in 31 CFR Chapter X also includes a mens rea of willfulness. In drafting this statement, FinCEN has consulted with the Department of Justice.

VI. Order

A. Definitions

1. *MEXC Global*

The order defines "MEXC Global," a Seychelles-based CVC exchanger, to include its branches, subsidiaries, and offices operating as a financial institution in any jurisdiction outside of the United States, and any successor entities. For the purposes of this order, a successor entity means any person that replaces MEXC Global, its branches, subsidiaries, and offices by acquiring its assets, in whole or in part, and/or carrying on the affairs of MEXC Global under a new name. This includes, but is not limited to, any entities referenced in this order as being

[52] Executive Order 14294, *Fighting Overcriminalization in Federal Regulations*, 90 FR 20367 (issued May 9, 2025; published May 14, 2025), https://www.federalregister.gov/executive-order/14294.

branches, subsidiaries, or offices of MEXC Global operating as a financial institution in any jurisdiction outside of the United States. Any branches, subsidiaries, and offices of MEXC Global located in the United States are expressly excluded from the definition of "MEXC Global" for the purposes of this order.

2. *Convertible Virtual Currency*

The order defines "convertible virtual currency" (CVC) as a medium of exchange that either has an equivalent value to currency, or acts as a substitute for currency, but lacks legal tender status. Bitcoin, despite having legal tender status in at least one jurisdiction, is included as a type of CVC for the purpose of this order.

3. *Covered Financial Institution*

The order defines "covered financial institution" as having the same meaning as "financial institution" in 31 CFR 1010.100(t).

4. *Transmittals of Funds*

The order defines "transmittals of funds" as the sending and receiving of funds, including CVC. For avoidance of doubt, for this section, this definition of transmittal of funds applies rather than the definition of "transmittal of funds" in section 1010.100(ddd).

5. *Meaning of Other Terms*

All terms used but not otherwise defined herein shall have the meaning set forth in 31 CFR chapter X and 31 U.S.C. 5312.

B. Prohibition on Transmittals of Funds Involving MEXC Global

A covered financial institution is prohibited from engaging in any transmittal of funds from or to MEXC Global.

C. Order Period

The terms of this order are effective [**INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER***], with no cessation date.

D. Reservation of Authority

FinCEN reserves authority to impose conditions on certain transmittals of funds from or to MEXC Global and to grant appropriate exemptions from the requirements of this order.

E. Other Obligations

Nothing in this order shall be construed to modify, impair, or otherwise affect any requirements or obligations to which a covered financial institution is subject pursuant to the BSA, including, but not limited to, the filing of Suspicious Activity Reports (SARs), or other applicable laws or regulations, such as the sanctions administered and enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control.

F. Penalties for Noncompliance

The covered financial institution, and any of its officers, directors, employees, and agents, may be liable for civil or criminal penalties under 31 U.S.C. 5321 and 5322 for willfully violating this order.

G. Validity of Order

Any judicial determination that any provision of this order is invalid shall not affect the validity of any other provision of this order, and each other provision shall thereafter remain in full force and effect.

_____

Jimmy L. Kirby,
Deputy Director,
Financial Crimes Enforcement Network.