BILLING CODE: 4810-02

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network (FinCEN)

31 CFR Chapter X, Part 1010

Imposition of Special Measure Prohibiting the Transmittal of Funds Involving PM2BTC

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

ACTION: Notice.

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), to prohibit certain transmittals of funds by any covered financial institution involving PM2BTC, a financial institution operating outside of the United States determined to be of a primary money laundering concern in connection with Russian illicit finance.

DATES: This action is effective [[INSERT DATE PUBLISHED IN THE FEDERAL REGISTER]], 2024.

FOR FURTHER INFORMATION CONTACT: The FinCEN Resource Center, 1-800-767-2825 or electronically at frc@fincen.gov.

SUPPLEMENTARY INFORMATION:

I. Summary of Order

This order (1) sets forth FinCEN's determination that PM2BTC, an unincorporated convertible virtual currency (CVC) exchanger (a type of virtual asset

service provider or VASP), is a financial institution operating outside of the United States that is of primary money laundering concern[1] in connection with Russian illicit finance; and (2) prohibits certain transmittals of funds involving PM2BTC by any covered financial institution.

As set out in this order, PM2BTC, a CVC exchanger offering CVC and fiat currency exchange services with significant ties to, and connections with, Russia, is of primary money laundering in connection with Russian illicit finance through its facilitation of funds transfers by illicit actors and association with a wide array of illicit activities, including fraud schemes, sanctions evasion, ransomware attacks, and child abuse.

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) (hereafter, "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 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] The application of FinCEN's authorities in this order is specific only to section 9714 of the Combating Russian Money Laundering Act, as amended. It is not intended to otherwise reflect the applicability of, or obligations under, any provision of the Bank Secrecy Act (BSA) or its implementing regulations, and FinCEN has not considered the extent to which PM2BTC does business in the United States.
[2] Section 9714 (as amended) may be found in a note to 31 U.S.C. 5318A.

(1) require domestic financial institutions and domestic financial agencies to take 1 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, if such transmittal of funds involves any such institution. The authority of the Secretary to administer both section 9714 and the Bank Secrecy Act (BSA) has been delegated to FinCEN.[4]

The six special measures set out in section 9714 are prophylactic safeguards that may be employed to defend the United States financial system from money laundering and terrorist financing risks with a nexus to Russian illicit finance. The Secretary may impose one or more of these special measures in order to protect the U.S. financial system from such threats. Specifically, the Secretary may impose any of the five special measures set out in 31 U.S.C. 5318A, commonly known as section 311 of the USA PATRIOT Act. Through special measure one, the Secretary may require domestic financial institutions and domestic financial agencies to maintain records, file reports, or both, concerning the aggregate amount of transactions or individual transactions.[5] Through special measures two through four, the Secretary may impose additional recordkeeping, information collection, and reporting requirements on covered domestic

[3] 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."

[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* section 9714(a)(1); 31 U.S.C. 5318A(b)(1).

financial institutions and domestic financial agencies.[6] Through special measure five, the Secretary may prohibit, or impose conditions upon, the opening or maintaining in the United States of correspondent or payable-through accounts for or on behalf of a foreign banking institution, if the class of transactions found to be of primary money laundering concern may be conducted through such correspondent account or payable-through account.[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. *PM2BTC*

PM2BTC is a CVC exchanger, a category of VASP, that exists as a collection of several exchange services. By its own account, PM2BTC is comprised of the following exchange services: PM2BTC.ME, BTC2PM.ME, PM2CASHIN.ME, BTC2CASHIN.ME, PM2WM.ME, and BTC2WM.ME.[9]

Although PM2BTC—through each of its constituent exchange services—is advertised as an automated web product, FinCEN assesses that this collective grouping of exchange services should be considered a single organization, and for that reason, FinCEN will correspondingly refer to this collective, its activities, and its website as "PM2BTC". Indeed, notwithstanding the characterization in its advertisements, PM2BTC holds itself out as a legal person insofar as PM2BTC states—in its terms of

[6] *See* section 9714(a)(1); 31 U.S.C. 5318A(b)(2)-(b)(4).
[7] *See* section 9714(a)(1); 31 U.S.C. 5318A(b)(5).
[8] *See* section 9714(a)(2).
[9] This statement was made by the BitcoinTalk user, "pm2btc," which FinCEN assesses is the official account for PM2BTC, on the CVC forum BitcoinTalk. *See* BitcoinTalk, PM2BTC Post, *available at* https://bitcointalk.org/index.php?topic=639799.msg7140395#msg7140395 (last accessed Sept. 17, 2024).

service—that use of its exchange services constitutes a contract between parties to an agreement, with PM2BTC expressly identified as a party. Consistent with that characterization in its terms of service, FinCEN assess that PM2BTC also operates as a standard organization, comprised of its founders/operators and employees, with consistent and coordinated internal operations and customer service interfaces. As a threshold matter, PM2BTC, including each of its constituent exchange services, is operated, with other persons, by Sergey Sergeevich Ivanov (Ivanov), a Russian national with an established history of advertising the use of U.S.-based money services businesses for cashouts and drops services on various Russian-speaking cybercrime forums, ties to top-tier cyber criminals and cybercrime services, and apparent ties to other online CVC exchanges and an associated payment processing service associated with ransomware, bank fraud, malware, and other suspected illicit activity. In addition, in its daily operations, PM2BTC relies on developers and other personnel. As set out in its terms of service, for example, PM2BTC's "administration" conducts anti-money laundering (AML) checks of all the transactions it processes, with corresponding authority to verify users and suspend the execution of the transactions, as well as to assess a "commission" for processing the transaction.[10] Moreover, each of PM2BTC's constituent exchange services offers an identical customer service point of contact—"pm2btc"—on a Russian messaging platform, and the same email address—"support@pm2btc[.]me"—with each apparently offering customer service support

[10] *See infra* Part III.A.3, for further discussion of PM2BTC's anti-money laundering program.

through PM2BTC personnel.[11] As such, FinCEN assesses that, rather than a mere automated web product, PM2BTC is an organization that operates as a service provider.[12]

Further, in light of its activities and the services it provides, PM2BTC is a financial institution within the meaning of section 9714. According to its official website,[13] PM2BTC allows customers to exchange between Russian Rubles (RUB) and various CVCs, including Bitcoin (BTC), Litecoin (LTC), and Dash (DASH), as well as other CVC offered by Russian money service businesses—Perfect Money[14] and WebMoney.[15] As a general matter, the names of PM2BTC's constituent exchange services denote the exchangeable direction of the offered CVC or fiat currencies. For example, PM2BTC as an exchange service, converts the digital currency Perfect Money—or "PM"—into Bitcoin—or BTC—and thus, taken together, the name of the exchanger—PM2BTC—captures the service and direction of exchange. As a general matter, transactions through PM2BTC's constituent exchange services follow generally

---

[11] PM2BTC's websites, *available at* https://pm2btc.me, https://pm2btc.me/terms, https://pm2wm.me, https://pm2wm.me/terms, https://pm2cashin.me, https://pm2cashin.me/terms, https://pm2cashin.me/terms, https://pm2cashin.me/terms, https://btc2wm.me, https://btc2wm.me/terms, https://btc2pm.me, https://btc2pm.me/terms, https://btc2cashin.me, https://btc2cashin.me/terms, https://pm2btc.me (last accessed Sept. 17, 2024).

[12] All references to PM2BTC's Terms of Service are sourced from https://pm2btc.me/terms (last accessed Sept. 17, 2024).

[13] Unless noted otherwise, all references to PM2BTC's official website, webpage, or policies are sourced from pages and links accessed via https://pm2btc.me, https://pm2btc.me/terms, https://pm2wm.me, https://pm2wm.me/terms, https://pm2cashin.me, https://pm2cashin.me/terms, https://btc2wm.me, https://btc2wm/terms, https://btc2pm.me, https://btc2pm.me/terms, https://btc2cashin.me, https://btc2cashin.me/terms (last accessed Sept. 17, 2024).

[14] Perfect Money, or PM, is a Russian financial service that allows its users to make anonymous instant payments and to make money transfers securely throughout the internet. Perfect Money, *available at* https://perfectmoney.com/about.html (last accessed Sept. 17, 2024); *see also* Ben [LNU], *The unregulated Russian payment and lending platform Perfect Money!*, FinTelegram (Feb. 14, 2022), *available at* fintelegram.com/r4i-the-unregulated-russian-payment-and-lending-platform-perfect-money (last accessed Sept. 17, 2024).

[15] WebMoney, or WM, is a Russia based global online payment system that facilitates online business activities. *See* WebMoney, Terms of Use, *available at* https://debt.wmtransfer.com/Rules.aspx?lang=en (last accessed Sept. 17, 2024).

similar processes. By way of illustration, PM2BTC's official PM2BTC.ME website details a transaction process whereby, for example, PM2BTC connects to a customer's Perfect Money (PM) account and coordinates the conversion of PM into BTC, subsequently receiving a fixed fee. To carry out this type of exchange transaction, a customer would enter their PM account information and a corresponding BTC wallet address to which PM2BTC would send BTC. Once the order is submitted, PM2BTC would effectuate the withdrawal of PM value and send BTC to the customer-designated wallet, completing the transaction.[16] Although section 9714 does not expressly define the term "financial institution," FinCEN has long defined that term to apply to foreign and domestic "money transmitters," including persons that accept and transmit value that substitutes for currency, such as CVC.[17] VASPs, such as PM2BTC, are "money transmitters" because they are engaged in the transfer of funds as defined in 31 CFR 1010.100. PM2BTC is therefore a financial institution within the meaning of section 9714.

Additionally, based on public and non-public information available to FinCEN, PM2BTC operates outside the United States and, although it is not incorporated in any jurisdiction, PM2BTC has significant ties to, and connections with, Russia. Indeed, PM2BTC presents substantial ties to the Russian financial sector and largely—but not exclusively—offers exchange services between individual, often Russian users as well as

[16] PM2BTC, *available at* https://pm2btc.me (last accessed Sept. 17, 2024).
[17] *See, e.g.,* 31 U.S.C. 5312; 31 CFR 1010.100(t)(3); 1010.100(ff); 1010.605(f)(iv); *see also* 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).

Russian financial institutions and financial services platforms. As a threshold matter, the "Exchange Regulations and AML & KYC" policies for certain of PM2BTC's constituent exchange services expressly reference, and indicate a need to comply with, Russian law under certain circumstances,[18] as well as require users to acknowledge that payments will be processed during the exchange's working hours, set on Moscow Standard Time (MSK).[19] More significantly, PM2BTC provides services that, as noted above, permit customers to exchange between Russian Rubles (RUB) and various CVCs. In fact, each of PM2BTC's constituent exchange services automatically converts the value of BTC the customer is preparing to send to the service to its equivalent value in Russian Rubles.[20] Among its services, PM2BTC also provides specific services to users in, or transacting in, Russia, including, for instance, offering services to convert BTC to cash at certain Russian banks, permitting users only to identify Russia for "Receivers [sic] Country" (meaning the service will transmit funds to Russia), providing customers ready access to numerous Russian banks and money service businesses, and offering Cyrillic script user interfaces.

PM2BTC can carry out such transactions quickly, with most transactions up to 30,000 RUB completed within 15-60 minutes, although PM2BTC's website notes that transactions with Alfa-Bank require up to two hours.[21] In addition, PM2BTC has

---

[18] BTC2CASHIN Terms, *available at* https://btc2cashin.me/terms (last accessed Sept. 17, 2024); PM2CASHIN Terms, *available at* https://pm2cashin.me/terms (last accessed Sept. 17, 2024).
[19] *Id.* According to the Central Intelligence Agency's World Fact Book, UTC +3 is the time zone used in Moscow, Russia. Central Intelligence Agency, *World Factbook: Russia*, *available at* https://www.cia.gov/the-world-factbook/countries/russia (last accessed Sept. 17, 2024).
[20] BTC2CASHIN, *available at* https://btc2cashin.me (last accessed Sept. 17, 2024).
[21] PM2CASHIN, *available at* https://pm2cashin.me (last accessed Sept. 17, 2024); BTC2CASHIN, *available at* https://btc2cashin.me (last accessed Sept. 17, 2024), https://pm2cashin.me (last accessed Sept. 17, 2024); BTC2CASHIN, *available at* https://btc2cashin.me (last accessed Sept. 17, 2024).

ongoing arrangements with numerous Russian financial institutions and financial service providers, including but not limited to JSC Alfa-Bank (Alfa-Bank),[22] Perfect Money, WebMoney, and Limited Liability Company YooMoney (YooMoney).[23] For instance, according to PM2BTC's official BTC2CASHIN.ME website, PM2BTC's services that offer conversion of BTC to cash for customers contain a drop-down menu called "method of obtaining" for customers to select which of the financial institutions they wish to transact with. The dropdown menu lists numerous Russian banks and money service businesses, including, but not limited to, Alfa-Bank and YooMoney.

III. Finding that PM2BTC 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 PM2BTC, a CVC exchanger with significant ties to and connections with Russia, is a financial institution of primary money laundering concern in connection with Russian illicit finance through its facilitation of funds transfers by Russian-affiliated illicit actors and associated with a wide array of

[22] On April 6, 2022, Treasury's Office of Foreign Assets Control (OFAC) sanctioned Alfa-Bank and six of its subsidiaries pursuant to E.O. 14024 for having operated in the Russian financial services sector. Treasury, Press Release, *U.S. Treasury Escalates Sanctions on Russia for its Atrocities in Ukraine* (Apr. 6, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0705.

[23] On February 24, 2022, OFAC sanctioned YooMoney (also known as Yoo Money, Yu Money, and Yandex Money). Treasury, Press Release, *U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs* (Feb. 24, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0608; *see also* Treasury, Press Release, *U.S. Treasury Escalates Sanctions on Russia for Its Atrocities in Ukraine* (Apr. 6, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0705; Treasury, Sanctions List Search, Limited Liability Company YooMoney, *available* https://sanctionssearch.ofac.treas.gov/Details.aspx?id=34597. Yoo Money is a Moscow, Russia based payment processor that was acquired by PJSC Sberbank (Sberbank) on July 2, 2020, *available at* https://www.crunchbase.com/organization/yandex-money (last accessed on Sept. 17, 2024). The BTC2CASHIN.ME website uses the spelling "Yu Money", but FinCEN assesses this is a transliteration variant and will subsequently refer to the entity as "Limited Liability Company YooMoney". *See id.*

illicit activities, including fraud schemes, sanctions evasion, ransomware attacks, and child abuse.

A. *The extent to which PM2BTC is of money laundering concern in connection with Russian illicit finance*

Based on blockchain analysis, FinCEN identified significant ties between PM2BTC and a broad spectrum of illicit actors and illicit activities. FinCEN's analysis, using the combined counterparty information from two clusters attributed to PM2BTC by commercially available blockchain analytic software found that a substantial percentage of transactions processed through PM2BTC were associated with wallet addresses linked to illicit actors and activity, including fraud shops, illicit actors or organizations, sanctioned persons and jurisdictions, ransomware attackers, darknet markets (DNMs), scam operators, child abuse materials traffickers, and entities that are the subject of FinCEN-imposed special measures. In addition to the specific categories of illicit activity with which PM2BTC is associated, FinCEN determined that PM2BTC facilitates a disproportionally high volume of suspected illicit activity compared to peer exchange service providers. Moreover, alarmingly, PM2BTC also employs a technique that is used to stymie the ability to trace illicit funds to or from PM2BTC, which permits illicit actors access to a money laundering platform and also decreases the risk of this activity being identified by investigating authorities.

1. *PM2BTC's disproportionate volume of transactions involving illicit activities*

As a threshold matter, FinCEN found that a predominant percentage of transactions processed through PM2BTC were linked to suspected illicit activity. Based on analysis conducted using commercially available blockchain analysis software A,

FinCEN has determined that, as a percentage of all funds transacted before July 2023, the cumulative value of suspected illicit funds accounted for up to 43.1 percent of all CVC received by PM2BTC. Those funds were associated with suspected illicit activities that include, in order of cumulative value, fraud schemes, transfers of stolen funds, sanctions evasion, terrorist financing, ransomware payments, and child abuse materials transactions. Significantly, further analysis comparing transactions through PM2BTC against transactions involving 1,244 other VASPs from around the world indicated that, after adjusting for the relative size of the other VASPs analyzed, PM2BTC is in the top one percent of direct receiving exposure and the top two percent of indirect receiving exposure to the categories deemed to be associated with suspected illicit activity. In short, PM2BTC has exceedingly high exposure to, and association with, transactions associated with suspected illicit activity compared to peer VASPs throughout the world, presenting a significant money laundering risk.

2. *PM2BTC's ties to illicit actors*

PM2BTC's exposure to, and facilitation of, transactions associated with suspected illicit activity is, importantly, consistent with its long-standing associations with a wide range of illicit actors, including, in particular, Russian ransomware groups, darknet markets, and sanctioned persons.

For several years, PM2BTC processed, for example, a substantial volume of transactions associated with the now-defunct Conti and Trickbot ransomware gangs.[24]

[24] Based on public and non-public information, FinCEN assesses that, on or around 2021, the Conti and Trickbot ransomware gangs had effectively merged and were effectively one and the same. For further details concerning Trickbot and its relation to Conti or their collective Russia connections, *see* WIRED*, Leaked Ransomware Doc Show Conti Helping Putin from Shadows* (Mar. 18, 2022), *available at*

According to blockchain analysis using commercially available blockchain analytic software, between February 5, 2018, and February 2, 2021, Trickbot, including its affiliates and associates, processed approximately $4,299,457 of CVC through PM2BTC.[25] Those transactions constituted, by value, a significant majority of PM2BTC's ransomware-related financial activity during the period. In addition, although the Conti and Trickbot ransomware gangs are now defunct, PM2BTC continues to process transactions involving CVC from sources attributed to other variants of ransomware.

In addition to ties to ransomware-related transactions, PM2BTC has a long history of facilitating transactions involving darknet[26] markets, including the now-defunct

---

https://www.wired.com/story/conti-ransomware-russia/ (describing Conti's pledged allegiance to Russia, its connection to Russian cybercrime and Russia's intelligence apparatus); CPO Magazine, *After Declaring Support for Russian Invasion, Conti Ransomware Gang Hit With Data Leak* (Mar. 8, 2022), *available at* https://www.cpomagazine.com/cyber-security/after-declaring-support-for-russian-invasion-conti-ransomware-gang-hit-with-data-leak/ (concerning Conti's relationship with Russian law enforcement); CyberScoop, *Conti Ransomware Group Announces Support of Russia, Threatens Retaliatory Attack* (Feb. 25, 2022), *available at* https://cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/; Reuters, *Russia-Based ransomware Group Conti Issues Warning to Kremlin Foes*(Feb. 26, 2022), *available at* https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/ (concerning Trickbot's support of the Russian Government); Security Week, *Conti Ransomware 'Acquires' Trickbot as it Thrives Amid Crackdowns* (Feb. 21, 2022), *available at* https://www.securityweek.com/conti-ransomware-acquires-trickbot-it-thrives-amid-crackdowns/; WIRED, *Inside Trickbot, Russia's Notorious Ransomware Gang* (Feb. 1, 2022), *available at* https://www.wired.com/story/trickbot-malware-group-internal-messages/ (concerning the connection between Trickbot and Conti); Department of Justice, *Russian National Sentenced for Involvement in Development and Deployment of Trickbot Malware* (Jan. 25, 2024), *available at* https://www.justice.gov/opa/pr/russian-national-sentenced-involvement-development-and-deployment-trickbot-malware; Treasury, *United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cybercrime Gang* (Sept. 7, 2023), *available at* https://home.treasury.gov/news/press-releases/jy1714 (concerning recent U.S. government actions against Trickbot).

[25] This analysis takes into account only direct transfers (e.g., where an address attributed to Trickbot transfers directly to PM2BTC). It does not include indirect exposure in which Trickbot sought to obfuscate the transactional path between their addresses and PM2BTC, nor does it include any transfers in which Trickbot first sent to another service and subsequently sent from that service to PM2BTC. All transaction values throughout this Order represent the USD exchange rate of the CVC at the time of the transaction.

[26] "Darknet" is a term used to refer to networks that are only accessible through the use of specific software or network configurations. In particular, darknet content is not indexed by web search engines, and is often

Russia-linked darknet markets Hydra—which was sanctioned by OFAC in April 2022[27]—and Ferum Shop.[28] Darknet markets are fundamentally illicit in nature and can operate largely as a result of the inherent anonymity of the darknet infrastructure, facilitating illicit activity because of the difficulty involved for law enforcement in identifying users, infrastructure, and even domains associated with the sale of illicit goods and services.[29] FinCEN assesses that, between 2016 and 2022, PM2BTC regularly processed transactions involving Hydra and Ferum Shop. For instance, between June 15, 2016, and January 30, 2021, Hydra sent a total of $41,361 worth of CVC to PM2BTC. Similarly, based on analysis conducted using commercially available blockchain analytic software, Ferum Shop sent a total of $3,453,610 worth of CVC to PM2BTC between April 6, 2021, and February 8, 2022. In addition, although Hydra and Ferum Shop have now been shut down,[30] PM2BTC continues to process a substantial volume of

---

accessed via anonymized, encrypted systems like the software The Onion Router (TOR). Darknet markets are online markets only accessible with the use of software like TOR, and because such markets are not indexed, they can only be found if the domain name and URL are already known to the user. As a result of the inherent anonymity of the darknet infrastructure, darknets facilitate criminal activity because of the difficulty involved for law enforcement in identifying users, infrastructure, and even domains associated with the sale of illicit goods and services.

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

[28] Elliptic, *Elliptic Analysis: Russia Seizes Four Major Dark Web Carding Sites with $263 million in crypto sales* (Feb. 9, 2022), *available at* https://www.elliptic.co/blog/russia-seizes-four-major-dark-web-carding-sites-with-263-million-in-crypto-sales.

[29] FinCEN, Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 FR 72701 (Oct. 23, 2023), *available at* https://www.federalregister.gov/documents/2023/10/23/2023-23449/proposal-of-special-measure-regarding-convertible-virtual-currency-mixing-as-a-class-of-transactions.

[30] In February 2022, the Russian Ministry of Internal Affairs took down four major illicit dark web sites: Sky-Fraud Forum, Trump's Dumps, UAS Store, and Ferum Shop. Elliptic, *Elliptic Analysis: Russia Seizes Four Major Dark Web Carding Sites with $263 million in crypto sales* (Feb. 9, 2022), *available at* https://www.elliptic.co/blog/russia-seizes-four-major-dark-web-carding-sites-with-263-million-in-crypto-sales. Because the Russian Ministry of Internal Affairs carried out what amounts to a coordinated, simultaneous takedown of multiple darknet markets, but indicated no coordination with any international partners, FinCEN assesses Ferum Shop was at least partially operated in Russia.

transactions, by value, associated with darknet markets. Indeed, based on analysis conducted using commercially available blockchain analytic software, PM2BTC processed transactions valued at over $600,000 involving other darknet markets between July 22, 2023, and January 14, 2024.

Finally, PM2BTC has long-standing and close ties to an array of Russian or Russian-affiliated financial institutions that are the subject of U.S. sanctions or other restrictions. As noted earlier, PM2BTC has ongoing arrangements with numerous Russian financial institutions and financial service providers, including but not limited to YooMoney (an affiliate of Sberbank) and Alfa-Bank, each of which are the subject of U.S. sanctions.[31] In addition, since 2020, PM2BTC has conducted an increasing volume of transactional activity with Garantex, a Russian-affiliated VASP that was sanctioned by the United States in April 2022.[32] Between November 11, 2020, and September 20, 2023, PM2BTC engaged in CVC transactions with a value of nearly $300,000 involving Garantex, and notably, the bulk of those transactions occurred only after sanctions were imposed on Garantex. During largely the same period, PM2BTC also engaged in a sizable volume of transactions with Bitzlato Limited (Bitzlato), a Russian-affiliated CVC exchanger identified by FinCEN in January 2023 as a financial institution operating outside of the United States that was of primary money laundering concern in connection with Russian illicit finance, under section 9714.[33] According to blockchain analysis

[31] *See supra* notes 22-23.
[32] *See* Treasury, Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (Apr. 5, 2022), *available at* https://home.treasury.gov/news/press-releases/jy0701.
[33] FinCEN, *Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato*, 88 FR 3919 (Jan. 23, 2023) *available at* https://www.federalregister.gov/documents/2023/01/23/2023-01189/imposition-of-special-measure-prohibiting-the-transmittal-of-funds-involving-bitzlato.

conducted by FinCEN using commercially available blockchain analytic software, between May 10, 2018, and January 17, 2023, Bitzlato sent approximately $154,429 worth of CVC to PM2BTC and, in turn, received approximately $541,307 worth of CVC from PM2BTC.

Taken as a whole, PM2BTC's historic and ongoing facilitation of transactions by, and associations with, illicit actors, including ransomware groups, darknet markets, and sanctioned persons connected to Russian illicit finance, combined with its access to international markets presents substantial money laundering risk.

3. *PM2BTC's lax anti-money launder policies and procedures*

The risks presented by PM2BTC associations with illicit actors and comparative high volume of transactional activity linked to suspected illicit activity are compounded by PM2BTC's lax KYC and AML policies and procedures, as well as recent technical changes that have the effect of obscuring PM2BTC's involvement in transactions.

Although PM2BTC purports to maintain KYC and AML policies and procedures, those policies and procedures appear inadequate and loosely implemented. According to its website, PM2BTC "adhere[s] to a number of rules and implements a number of procedures aimed at preventing the use of the service for the purpose of money laundering operations."[34] Moreover, as set out in its terms of service, PM2BTC retains the ability to, and may, suspend the execution of transactions until verification is carried

[34] PM2BTC Terms, *available at* https://pm2btc.me/terms (last accessed Sept. 17, 2024); BTC2CASHIN Terms, *available at* https://btc2cashin.me/terms (last accessed Sept. 17, 2024); BTC2WM Terms *available at* https://btc2wm.me/terms (last accessed Sept. 17, 2024); BTC2PM Terms, *available at* https://btc2pm.me/terms (last accessed Sept. 17, 2024); PM2WM Terms *available at* https://pm2wm.me/terms (last accessed Sept. 17, 2024); PM2CASHIN Terms *available at* https://pm2cashin.me/terms (last accessed Sept. 17, 2024).

out in accordance with the Financial Action Task Force (FATF) recommendations and "request from the User identification data and data confirming the source of funds."[35]

However, in practice, PM2BTC appears to only require users to provide the following information in order to conduct a transaction: (1) the type of CVC involved; (2) the value of the CVC to be sent or received; and (3) an email address (required "in order to communicate with the User, if necessary, to notify about Service's profitable offers").[36] Such limited information is not consistent with FATF recommendations. There appears to be no requirement to provide a name, date of birth, address, national identification, or any other proof of identification—all necessary to meaningfully establish and verify the identity of users and core features of the FATF's guidance on necessary official identity data points for an effective KYC and AML program.[37] Indeed, in contrast to PM2BTC's claim that it adheres to FATF standards, it represents that it offers "[c]omplete anonymity of exchanges" and that "[t]here is no need to register or undergo any verification to make an exchange."[38]

Notwithstanding its purported policies and procedures, FinCEN assesses that PM2BTC has implemented technical changes to its wallet arrangement that have the

[35] BTC2WM Terms, *available at* https://btc2wm.me/terms (last accessed Sept. 17, 2024); BTC2PM Terms *available at* https://btc2pm.me/terms (last accessed Sept. 17, 2024); BTC2CASHIN Terms, *available a*t https://btc2cashin.me/terms (last accessed Sept. 17, 2024).
[36] BTC2CASHIN, *available at* https://btc2cashin.me (last accessed Sept. 17, 2024); *see also*, BTC2PM *available at* https://btc2pm.me (last accessed Sept. 17, 2024); BTC2WM, *available at* https://www.btc2wm.me (last accessed Sept. 17, 2024); PM2BTC, *available at* https://pm2btc.me (last accessed Sept. 17, 2024); PM2CASHIN, *available at* https://pm2cashin.me (last accessed Sept. 17, 2024); PM2WM, *available at* https://pm2wm.me (last accessed Sept. 17, 2024).
[37] FATF, Guidance on Digital Identity (Mar. 2020), at 63, *available at* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.
[38] This statement was made by the BitcoinTalk user, "pm2btc," which FinCEN assesses is the official account for PM2BTC, on the CVC forum BitcoinTalk. *See* BitcoinTalk PM2BTC Post, *available at* https://bitcointalk.org/index.php?topic=639799.msg7140395#msg7140395 (last accessed Sept. 17, 2024).

effect of obscuring its involvement when transacting with other VASPs. On or around July 2023, FinCEN assesses that PM2BTC implemented a cyclical infrastructure setup—a continuous creation of new wallets which are rotating and temporary—that avoids the reuse of wallets and, contrary to standard practice among VASPs, impedes any capacity to capture long-term transactional histories that would allow financial institutions to identify PM2BTC as the counterparty to a transaction. This typology is not wholly new and, for instance, has been employed by several VASPs of concern, some of whom are subjected to OFAC sanctions. In FinCEN's assessment, this typology can be, and has been, used to facilitate evasion of U.S. sanctions. Here, FinCEN assesses that PM2BTC's cyclical infrastructure setup is an effort to avoid blockchain forensics-based transaction monitoring—an outcome that is already evident in the precipitous decline in observable transactions associated with suspected illicit activity since July 2023. FinCEN assesses that this decline in such observable transactions is a result of PM2BTC's efforts to avoid blockchain activity monitoring, and is not a true reflection of PM2BTC's actual business activity with illicit actors.

Taken together, PM2BTC's lax implementation of KYC and AML policies and procedures and adoption of a technical arrangement that inhibits effective blockchain analysis increases the risk PM2BTC poses to the international and U.S. financial systems.

B. *Whether the money laundering concern posed by PM2BTC outweighs any legitimate business activity it may conduct*

The record amply demonstrates that PM2BTC's services are used, to an unusually large extent by comparison to other CVC exchanges, to facilitate illicit activities by illicit actors. Although PM2BTC offers services that could potentially be used by licit actors,

those services may be found at other VASPs, including VASPs located in jurisdictions with robust AML/CFT frameworks and regulatory oversight. Legitimate actors have access to a broad range of comparable services that provide for appropriate transparency and can support international efforts to protect the integrity of the international financial system, including transactions involving CVC. Accordingly, given the extensive flow of illegitimate funds through PM2BTC, FinCEN assesses that the need to protect U.S. financial institutions from the money laundering risks presented by PM2BTC outweighs any potential legitimate utility its services may provide.

IV. Imposition of Special Measure Prohibiting Transmittals of Funds Involving PM2BTC

Having found that PM2BTC is a financial institution operating outside 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 PM2BTC is warranted.[39]

A. *Whether the prohibition of certain transmittals of funds involving PM2BTC will address the money laundering concern in a manner consistent with U.S. national security and foreign policy interests*

Given PM2BTC's extensive association with suspected illicit activity and illicit actors, FinCEN assesses that imposing a prohibition on certain transmittals of funds

[39] In connection with this action, FinCEN consulted 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 Board. Those consultations involved sharing drafts and information for the purpose of obtaining interagency views on the imposition of a prohibition on certain transmittals of funds by any domestic financial institution from or to PM2BTC, or from an account or CVC address administered by or on behalf of PM2BTC, and the effect that such a prohibition would have on the domestic and international financial system. Each of the Departments and agencies concurred in the issuance of this order.

involving PM2BTC is necessary to safeguard U.S. national security and the U.S. financial system, as well as serve key U.S. national security objectives. In light of the predominant percentage of transactions linked to known or suspected illicit activity processed through PM2BTC, prohibiting certain transmittals of funds involving PM2BTC will insulate the U.S. financial system from international money laundering and other financial crimes.

In particular, prohibiting certain transmittals of funds involving PM2BTC will further ongoing U.S. efforts to curtail suspected Russian-associated illicit activity and financial transactions. Targeting illicit proceeds obtained by ransomware actors, especially those with a nexus to Russia, is, for instance, a high priority for the United States. Recent actions by FinCEN, OFAC, and intergovernmental task forces have also focused on Russia-related illicit finance threats. Prohibiting certain transmittals of funds involving PM2BTC will serve the United States' national security and foreign policy interests by protecting U.S. businesses and interests from known ransomware threat actors, by publicly countering a financing mechanism used by illicit entities, including entities that seek to further the Russian state's aims of political and economic destabilization. Similarly, such a prohibition would sever a pathway that might facilitate circumvention of U.S. economic sanctions, supporting the efficacy of U.S. sanctions and complementing previous actions taken by the U.S. government.

Additionally, this action reinforces the expectations of AML/CFT compliance in the virtual asset ecosystem in order to improve the identification and reporting of suspicious activity by financial institutions around the world.

B. *Whether the prohibition of certain transmittals of funds involving PM2BTC would impose burdens on legitimate activity of PM2BTC or third parties*

FinCEN assesses that prohibiting certain transmittal of funds involving PM2BTC will impose limited burdens on legitimate activities currently transacted through PM2BTC and, indeed, will have a positive systemic impact on the international payment, clearance, and settlement system.

By U.S. and international standards, PM2BTC represents a limited percentage of total received BTC (directly and indirectly). As of April 15, 2024, PM2BTC's total received value was between .0002 and 0.0014 percent (respectively) of the largest U.S.-domiciled CVC VASP (hereinafter referred to as "VASP 1"). PM2BTC's transaction history with VASP 1 totals just over $32 million in CVC over nearly 11 years. By contrast, a CVC price and volume aggregator estimates that VASP 1 processed more than $3 *billion* in transfers *daily*[40] as of April 17, 2024. By comparison, PM2BTC's largest U.S.-based counterparty (hereinafter referred to as "VASP 2") sent approximately $147 million worth of CVC to PM2BTC between 2018 and 2024, which amounted to approximately 0.002 percent of VASP 2's overall sending activity. As such, there is no evidence that PM2BTC is a major participant in the international payment system or relied upon by the international banking community. Indeed, given its size and limited international presence, the legitimate business services that it offers would be readily available through other regulated institutions. Further, as noted in the February 16, 2022, Financial Stability Board's Assessment of Risks to Financial Stability, direct connections between CVC as a whole, and systemically important financial institutions and core

[40] CoinGecko, *Exchanges*, *available at* https://www.coingecko.com/en/exchanges (last accessed Sept. 17, 2024).

financial markets, are limited at present. Volatility and disruptions in the CVC ecosystem have been contained within the CVC markets and have not significantly spilled over to financial markets and infrastructures.[41]

Given widespread availability of other VASP services, as well as PM2BTC's predominant use for suspected illicit activity, imposing a prohibition on certain transmittals of funds involving PM2BTC will merely remove from transaction chains a VASP that facilitates illicit or otherwise unduly risky transactions that pose a risk to the international financial system. This action will not have an adverse impact on the international payment, clearance, and settlement system or on legitimate business activities currently involving PM2BTC.

Moreover, FinCEN assesses that imposing a prohibition on certain transmittals of funds involving PM2BTC will not present a significant competitive disadvantage for financial institutions organized or licensed in the United States given PM2BTC's relatively small size and the relatively limited burden that compliance with this order would impose. Given the small size of PM2BTC and the comparatively low value of activity between U.S. financial institutions and PM2BTC, FinCEN assesses that this would impose neither an undue cost nor substantial burden these financial institutions. Further, 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. In order to ensure that is the case, FinCEN has elected to provide within this order for the

[41] Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets* (Feb. 16, 2022), at 5, *available at* https://www.fsb.org/wp-content/uploads/P160222.pdf (last accessed Sept. 17, 2024).

rejection of certain transmittals of CVC that are received from or originate at PM2BTC 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 PM2BTC despite a desire and effort to limit such exposure.[42] This order 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 PM2BTC 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 PM2BTC. 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*

[42] FinCEN notes that CVC payment systems are often designed to limit the control of specific financial institutions over transactions and to prevent rejections 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).

FinCEN considered other special measures available pursuant to section 9714 prior to selecting the prohibition reflected in this order.[43] However, prohibiting certain transmittals of funds involving PM2BTC is the only means of adequately addressing the money laundering concern in connection with Russian illicit finance posed by PM2BTC.

In particular, none of the special measures described in 31 U.S.C. § 5318A would effectively address the illicit finance threat posed by PM2BTC.[44] 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 PM2BTC. Such measures may allow such transfers to continue to benefit of illicit actors connected to Russian illicit finance. Further, placing conditions upon or prohibiting the opening or maintaining in the United States of a correspondent account or payable-through account by any domestic financial institution or domestic financial agency for or on behalf of a foreign banking institution, as described in 31 U.S.C 5318A(b)(5), is similarly inadequate because the types of CVC transactions that PM2BTC facilitates do not rely on correspondent or payable-through accounts, and FinCEN is unaware of such relationships

[43] Pursuant to section 9714, these measures include: (1) the special measures described in 31 U.S.C. 5318A, including the imposition of additional recordkeeping, information collection, and reporting requirements on covered U.S. financial institutions and/or the prohibition or 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 imposition of conditions on the transmittal of funds, as an alternative to a prohibition on the transmittal of funds.

[44] Likewise, imposing conditions on transmittals of funds, pursuant to section 9714(a)(2), would be insufficient to address the threat. While imposing conditions, rather than a full prohibition, may be appropriate in circumstances where the institution provides services for legitimate business that are not easily replicated or where a complete prohibition on transactional activity would otherwise unduly harm legitimate economic activity, PM2BTC provides a service that is easily obtainable for legitimate customers through other providers, and in this case the value of any legitimate activity it may conduct is outweighed by the significant proportion of illicit financial activity identified and its lack of mandatory KYC.

between PM2BTC and U.S. or foreign financial institutions. In addition, PM2BTC's recordkeeping is incomplete, so imposing additional recordkeeping requirements is not likely to be successful or sufficient to address the risks it poses. For these reasons, FinCEN assesses that the prohibition on certain transmittals of funds, including CVC, involving PM2BTC is the most appropriate special measure.

D. *Whether the special measure prohibiting certain transmittals of funds should be imposed by order or regulation*

Pursuant to section 9714, the Secretary may impose specified 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 special measures by order or regulation. Although PM2BTC is not a large participant in the international payment system, FinCEN 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 PM2BTC facilitates as well as the ongoing transactions associated with suspected illicit activity that continue to be processed through PM2BTC.

A copy of this order will be published in the Federal Register. To the extent PM2BTC or other parties have information relevant to this order, they may submit it to FinCEN at frc@fincen.gov.

V. Order

A. *Definitions*

1. PM2BTC

The order defines PM2BTC, a CVC exchanger comprised of a collection of the services PM2BTC.ME, BTC2PM.ME, PM2CASHIN.ME, BTC2CASHIN.ME, PM2WM.ME, and BTC2WM.ME, to mean all subsidiaries, branches, and offices of PM2BTC operating in any jurisdiction, as well as any successor entity.

2. Convertible Virtual Currency (CVC)

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

3. Covered Financial Institution

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

4. CVC Exchanger

The order defines a CVC exchanger as any person engaged as a business in the exchange of CVC for fiat currency, funds, or other CVC.

5. Recipient

The order defines recipient as the person to be paid by the recipient's covered financial institution.

6. Successor Entity

The order defines successor entity as any person that replaces PM2BTC by acquiring its assets, in whole or in part, and/or carrying out the affairs of PM2BTC under a new name.

7. Transmittal of Funds

The order defines transmittal of funds as the sending and receiving of funds, including CVC.

8. 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 of the Transmittal of Funds Involving PM2BTC*

1. Prohibition

A covered financial institution is prohibited from engaging in a transmittal of funds from or to PM2BTC, or from or to any account or CVC address administered by or on behalf of PM2BTC.

2. Rejection of Funds and Condition on the Transfer of Rejected Funds

A covered financial institution will be deemed not to have violated this Order where, upon determining that it received CVC that originated from PM2BTC or from an account or CVC address administered by or on behalf of PM2BTC, that covered financial institution rejects the transaction, preventing the intended recipient from accessing such CVC and returning the CVC to PM2BTC, or to the account or CVC address from which the CVC originated.

C. *Order Period*

The terms of this order are effective [[INSERT DATE PUBLISHED IN THE FEDERAL REGISTER]], 2024, with no cessation date.

D. *Reservation of Authority*

FinCEN reserves its authority pursuant to section 9714 to impose conditions on certain transmittals of funds from or to PM2BTC, or from or to any account or CVC address administered by or on behalf of PM2BTC.

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 violating any of the terms of this order.[45]

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

[45] Section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (Public Law 117-81) amended section 9714 of the Combatting Russian Money Laundering Act (Public Law 116-283) to, among other things, provide that the penalties set forth in 31 U.S.C. 5321 and 5322 shall apply to violations of any order, regulation, special measure, or other requirement imposed under section 9714, in the same manner and to the same extent described in sections 5321 and 5322.