

**DEPARTMENT OF THE TREASURY**

**Financial Crimes Enforcement Network (FinCEN)**

**31 CFR Chapter X, Part 1010**

**RIN 1506-AB42**

**Imposition of Special Measure Prohibiting the Transmittal of Funds Involving  
Bitzlato**

**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<sup>1</sup> by any covered financial institution involving Bitzlato Limited (Bitzlato), 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 February 1, 2023.

**FOR FURTHER INFORMATION CONTACT:** The FinCEN Resource Center, 1-800-767-2825 or electronically at [frc@fincen.gov](mailto:frc@fincen.gov).

**SUPPLEMENTARY INFORMATION:**

---

<sup>1</sup> As defined in this order below.

## **I. Summary of Order**

This order: (1) sets forth FinCEN’s determination that Bitzlato Limited (Bitzlato), a virtual asset service provider (VASP) incorporated in the Hong Kong Special Administrative Region of the People’s Republic of China (Hong Kong), is a financial institution operating outside of the United States that is of primary money laundering concern<sup>2</sup> in connection with Russian illicit finance; and (2) prohibits certain transmittals of funds by any domestic financial institution or involving Bitzlato by any covered financial institution. Bitzlato, a convertible virtual currency (CVC) exchanger (a type of VASP) with significant operations in Russia that offers exchange and Peer-to-Peer (P2P) services, is a financial institution of primary money laundering concern in connection with Russian illicit finance, namely, through: (1) its facilitation of deposits and funds transfers by Russian ransomware groups<sup>3</sup> or affiliates, such as Conti;<sup>4</sup> and (2) its facilitation of transactions with Russian darknet markets on behalf of both darknet customers and darknet vendors.

---

<sup>2</sup> The application of FinCEN’s authorities in this order is specific only to section 9714 of the Combating Russian Money Laundering Act. It is not intended to 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 Bitzlato does business in the United States.

<sup>3</sup> A ransomware “strain” is the specific kind of malware that encrypts or exfiltrates data from a victim in order to perpetrate cyber extortion. The developers and owners of a strain are referred to as a ransomware “gang” or “group,” and may use a strain for their own extortion activities or lease access to the strain to other illicit actors (affiliates) for use in a “Ransomware as a Service” (RaaS) model. As a specific strain becomes less effective or more detectable, the group may develop a new strain to continue its business. For example, “Conti v2” is the second strain developed by the Conti ransomware group, the first of which is “Conti.” A ransomware actor who has used both the Conti strain and the Phobos strain in their attacks is both a Conti and a Phobos affiliate.

<sup>4</sup> As noted above, in fn. 3, Conti refers to both a criminal group, the eponymous ransomware strains it spawned, and other affiliated actors.

## II. Background

### A. Statutory Provisions

Section 9714(a) of the Combating Russian Money Laundering Act, as amended by section 6106(b) of the National Defense Authorization Act for Fiscal Year 2022 (hereafter section 9714(a)),<sup>5</sup> provides, in relevant part, that “[i]f the Secretary of the Treasury 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 of the Treasury may, by order, regulation, or otherwise as permitted by law: (1) require domestic financial institutions and domestic financial agencies to take 1 or more of the special measures described in section 5318A(b) of title 31, United States Code;<sup>6</sup> or (2) prohibit, or impose conditions upon, certain transmittals of funds (to be 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 of the Treasury (the Secretary) to administer both section 9714(a) and the Bank Secrecy Act (BSA) has been delegated to FinCEN.<sup>7</sup>

Special measures one through four of section 5318A(b), commonly known as section 311 of the USA PATRIOT Act, describe additional recordkeeping, information

---

<sup>5</sup> Section 9714 (as amended) can be found in a note to 31 U.S.C. § 5318A.

<sup>6</sup> 31 U.S.C. § 5318A of the United States Code 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.”

<sup>7</sup> Pursuant to Treasury Order 180-01 (January 14, 2020), the authority of the Secretary of the Treasury to administer the BSA, including but not limited to 31 U.S.C. § 5318A, has been delegated to the Director of FinCEN. On August 11, 2022, and in accordance with Treasury Order 101-05 (September 20, 2022) 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.

collection, and reporting requirements that the Secretary may impose on covered U.S. financial institutions. The fifth special measure, codified at 31 U.S.C. § 5318A(b)(5), allows 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, to prohibit, or impose conditions upon, the opening or maintaining in the United States of correspondent or payable-through accounts by any domestic financial institution or domestic financial agency for, or on behalf of, a foreign banking institution, if such correspondent account or payable-through account involves one or more financial institutions operating outside of the United States that the Secretary has found to be of primary money laundering concern.

**B. *Bitzlato***

According to its website, Bitzlato is a “modern company working in the field of blockchain technologies and [CVC].”<sup>8</sup> It was previously known as ChangeBot. Bitzlato is a Russian-affiliated CVC exchanger – a category of VASP – that offers exchange and P2P services, allowing users to exchange Bitcoin (BTC), Ether (ETH), Bitcoin Cash (BCH), Litecoin (LTC), Dash (DASH), Tether (USDT), Monolith Ruble (MCR) and Dogecoin (DOGE) without intermediaries and hidden commissions.

As set out on its website, Bitzlato is an online platform that provides exchange and P2P services. Through its exchange services, Bitzlato organizes “trading for digital assets, their derivatives and other market instruments” with “[t]rading conducted via

---

<sup>8</sup> Unless noted otherwise, all references to Bitzlato’s official website, webpage, or policies are sourced from pages and links accessed via <https://bitzlato.com>, including <https://bitzlato.com/terms-of-service-bitzlato/>, <https://bitzlato.com/anti-money-laundering-policy-and-know-your-client-policy>, and [https://bitzlato.com/knowledgebase/how\\_to\\_buy\\_cryptocurrency/](https://bitzlato.com/knowledgebase/how_to_buy_cryptocurrency/) (last accessed January 2023).

standard contracts or orders.”<sup>9</sup> In parallel, through its P2P services, Bitzlato operates as “an advertising board for digital assets traders” offering wallet, escrow and other related services associated with P2P exchanges.<sup>10</sup> Bitzlato further notes that its P2P services include arranging “storage of digital assets ... to ensure and guarantee the execution of transactions between registered users” and that it retains the ability to “freeze [a user’s] digital asset wallet,” indicating that Bitzlato has custody of its users’ digital wallets and the CVC held in those accounts.<sup>11</sup>

In light of those activities, Bitzlato is a financial institution within the meaning of section 9714(a). Section 9714(a) does not expressly define the term “financial institution.” However, 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.<sup>12</sup> CVC exchangers, such as Bitzlato, are “money transmitters,” and therefore, financial institutions within the meaning of section 9714(a).

Based on public and non-public information available to FinCEN, Bitzlato operates outside the United States and, although identified as “registered under the laws of Hong Kong,” Bitzlato has significant ties to and connections with Russia. Under “Section 1. Terms and Definitions” in Bitzlato’s “Terms of Service” page on its website, Bitzlato is identified as “registered under the laws of Hong Kong” and “located at Unit 617, 6/ F, 131-132 Connaught Road West, Solo workshops, Hong Kong.”<sup>13</sup> A review of

---

<sup>9</sup> Bitzlato, <https://bitzlato.com/terms-of-service-bitzlato/> (last accessed January 2023).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> See 31 U.S.C. § 5312; 31 C.F.R. §§ 1010.100(t)(3), 1010.100(ff), 1010.605(f)(iv); see also FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies” (May 9, 2019); FIN-2013-G001, “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies” (March 18, 2013).

<sup>13</sup> Bitzlato, <https://bitzlato.com/terms-of-service-bitzlato/> (last accessed January 2022).

publicly available material, however, shows that Bitzlato’s actual location of operation, its employees, and a job opening are in Russia, with job descriptions written in Russian. Indeed, a study performed by a blockchain analysis company expressly identifies Bitzlato as having a presence in Moscow City (the financial district of Moscow, Russia) during the period between 2019 and 2021,<sup>14</sup> and FinCEN has found no information on current or former employees or positions in Hong Kong.

### **III. Finding that Bitzlato is a Financial Institution Operating Outside of the United States 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 Bitzlato, a P2P CVC exchanger with significant operations in Russia, is a financial institution of primary money laundering concern in connection with Russian illicit finance, namely, through: (1) its facilitation of deposits and funds transfers by Russian ransomware groups or affiliates, such as Conti; and (2) its facilitation of transactions with Russian darknet markets on behalf of both darknet customers and darknet vendors.

#### ***A. Bitzlato is Used to Facilitate Processing and Laundering Proceeds from Ransomware Attacks***

##### ***1. Background on Ransomware***

Ransomware is a form of malicious software (malware) used by an attacker to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems. Its purpose is to extort ransom payments from victims in exchange for decrypting the information, restoring victims’ access to their

---

<sup>14</sup> Chainalysis, “The 2022 Crypto Crime Report,” at 128 (February 2022).

systems or data, and/or not disclosing or destroying data or programs on IT systems.

Ransomware payments are made most often via CVC, which are preferred by ransomware attackers for their ability to obscure the attackers' identities, thus aiding in the attackers' ability to launder their criminal proceeds and continue attacking victims.<sup>15</sup>

According to open source reporting, ransomware attacks have increased exponentially over the last several years, with an estimated 300 million attempted attacks in the first half of 2021 alone,<sup>16</sup> including attacks against U.S. entities and institutions. These attacks have destabilized private businesses, healthcare facilities, school districts, and critical infrastructure – including domestic energy distribution, such as in the 2021 Colonial Pipeline attack,<sup>17</sup> and food supply chains, such as in the 2021 JBS meatpacking plant attack.<sup>18</sup> The U.S. government has long engaged on efforts to counter the threat of ransomware, and on April 1, 2015, the President issued Executive Order (E.O.) 13694 (“Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities”), in which he declared a national emergency to deal with the threat of the “increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States [that] constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”<sup>19</sup>

---

<sup>15</sup> See, e.g., FIN-2021-A004, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments” (November 8, 2021), available at [https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory\\_FINAL\\_508\\_.pdf](https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf).

<sup>16</sup> “Mid-year Update 2021 Cyber Threat Report: Cyber threat intelligence for navigating today’s business reality,” *Sonicwall*.

<sup>17</sup> Bogage, Jacob. “Colonial Pipeline CEO says paying \$4.4 million ransom was the right thing to do for the country,” *Washington Post* (May 19, 2021).

<sup>18</sup> “Meatpacker JBS says it paid equivalent of \$11 mln in ransomware attack,” *Reuters* (June 10, 2021).

<sup>19</sup> This E.O. was amended on December 28, 2016, pursuant to E.O. 13757.

In 2021, roughly 74 percent of ransomware revenue, or over \$400 million worth of CVC, went to strains highly likely to be affiliated with Russian organizations. Blockchain analysis combined with web traffic data further revealed that most of the extorted funds from the ransomware attacks were laundered through services primarily catering to Russian users.<sup>20</sup>

The media have reported on banks and stock exchanges being targets for ransomware attacks.<sup>21</sup> Further, the U.S. financial system is being used to send significant amounts of U.S. funds as ransom payments to foreign actors – both cybercriminals and nation-state actors. Consequently, ransomware attacks are a direct threat to the U.S. economy, to its citizens, and to its national security. Moreover, the threat of ransomware is not limited to the United States, as ransomware attacks are on the rise across the globe, posing a significant threat to governments, businesses, and institutions on several continents.

Although ransomware actors and darknet markets are not always state-affiliated, the notorious ransomware group Conti has significant connections to Russia and pledged allegiance to Russia on February 25, 2022. Further, the Hydra darknet market almost entirely catered to Russian customers and illicit goods and service providers before it was shut down by law enforcement in April 2022. The illicit gains from ransomware attacks can often be traced back to Russian-affiliated exchanges and darknet markets, representing the laundering of victim payments by Russian and Russia-affiliated actors

---

<sup>20</sup> Chainalysis, “The 2022 Crypto Crime Report,” at 123 (February 2022).

<sup>21</sup> Egan, Matt. “Banks and stock exchanges are even bigger targets for ransomware attacks,” *CNN* (May 12, 2021).



through Russian and Russia-affiliated services. As such, ransomware is a conduit for Russian illicit finance.

## 2. *Bitzlato's Ransomware Connections*

Bitzlato plays a critical role in facilitating transactions for the Conti ransomware group and other global ransomware actors, including actors that operate out of Russia. As a result, FinCEN assesses that Bitzlato serves as a VASP that ultimately enables the profitability of ransomware attacks and, at least in the case of Conti, advances the political and economic destabilization interests of the Government of Russia.

### a. Conti Ransomware Group

Conti, a notorious Ransomware-as-a-Service (RaaS) group and the eponymous strains of ransomware it offers as a service to affiliated criminals for their use, emerged in December 2019.<sup>22</sup> Although most such groups take steps to obfuscate their connections to Russia and Russian illicit finance, Conti did not. To the contrary, on February 25, 2022, Conti pledged allegiance to the Government of Russia and vowed to retaliate against international state actors for their support of the Government of Ukraine amidst the Russian invasion.<sup>23</sup> Further, a cache of 60,000 leaked chat messages and files from Conti appears to link Conti to the Russian state, including the Russian Federal Security Service.<sup>24</sup>

FinCEN has documented numerous transactions between Conti-associated CVC addresses and Bitzlato.

---

<sup>22</sup> Abrams, Lawrence. "Conti ransomware shows signs of being Ryuk's successor," *Bleeping Computer* (July 9, 2020).

<sup>23</sup> Bing, Christopher. "Russia-based ransomware group Conti issues warning to Kremlin foes," *Reuters* (February 25, 2022).

<sup>24</sup> Burgess, Matt. "After Declaring Support for Russian Invasion, Conti Ransomware Gang Hit With Data Leak," *Wired* (March 18, 2022).

## b. Other Ransomware Groups

Separately, based on blockchain analysis, other ransomware groups have used Bitzlato to facilitate transactions involving ransomware, including ransomware groups based in or linked to Russia. For example, blockchain analysis has identified transactions involving Bitzlato and: (1) Chatex, a VASP designated by Treasury’s Office of Foreign Assets Control (OFAC) for facilitating financial transactions for ransomware actors; and (2) the RaaS group DarkSide, a Russian-speaking group responsible for the Colonial Pipeline Company ransomware incident in May 2021.<sup>25, 26</sup> Based on blockchain analysis, 76 Bitzlato deposit addresses received bitcoin (BTC) worth over \$300,000 attributed to Chatex. On November 8, 2021, OFAC designated Chatex, pursuant to E.O. 13694, as amended, for its part in facilitating funds transfers for ransomware actors and for providing material support to SUEX OTC, S.R.O. (SUEX). SUEX, a CVC exchanger located in Moscow City, Russia, was itself designated by OFAC on September 21, 2021, pursuant to E.O. 13694, as amended, for providing material support to the threat posed by criminal ransomware actors.<sup>27</sup> According to media reporting in 2021, the RaaS group DarkSide, a Russian-speaking group responsible for the Colonial Pipeline Company ransomware incident in May 2021, along with its clientele, also used Bitzlato.<sup>28</sup> In addition, the Phobos ransomware group and its affiliates have made at least 1,063 direct

---

<sup>25</sup> Kramer, Andrew; Schwirtz, Michael; and Troianovski, Anton. “Secret Chats Show How Cybergang Became a Ransomware Powerhouse,” *N.Y. Times* (June 3, 2021).

<sup>26</sup> Department of State, “Reward Offers for Information to Bring DarkSide Ransomware Variant Co-Conspirators to Justice,” (November 4, 2021), <https://www.state.gov/reward-offers-for-information-to-bring-darkside-ransomware-variant-co-conspirators-to-justice>.

<sup>27</sup> Department of the Treasury, “Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange” (November 8, 2021), <https://home.treasury.gov/news/press-releases/jy0471>.

<sup>28</sup> Brewster, Thomas. “As Ransomware Hackers Sit On Millions In Extorted Money, America’s Military Is Urged To Hack Back,” *Forbes* (June 5, 2021).

transfers of funds in the form of BTC to at least 76 Bitzlato deposit addresses identified as having received funds from Chatex, representing 414.84 BTC worth approximately \$3 million.

According to public reporting, a spokesperson for Bitzlato denied that it worked with any ransomware criminals and claimed it was not acquainted with an organization called DarkSide.<sup>29</sup> However, even if Bitzlato is not knowingly affiliated with DarkSide or other ransomware groups, FinCEN assesses that it provides an enabling environment for such ransomware criminals to utilize its services to cash out ransomware proceeds due to its minimal Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) protocols, solidifying its reputation as a go-to CVC exchanger for such groups.<sup>30</sup>

***B. Bitzlato is Used to Facilitate Darknet Markets and Scams***

In addition to receiving ransomware proceeds, Bitzlato's receiving and sending transactional activity shows a significant connection to counterparties associated with other suspected illicit activities, such as darknet markets and scams with ties to and operations in Russia.

Approximately two-thirds of Bitzlato's top receiving and sending counterparties are associated with darknet markets or scams. For example, Bitzlato's top three receiving counterparties, by total amount of BTC received between May 2018 and September 2022 were: (1) Binance, a VASP; (2) the Russia-connected darknet market Hydra; and (3) the alleged Russia-based Ponzi scheme "TheFiniko." Similarly, Bitzlato's top three sending counterparties, by total amount of BTC sent between May 2018 and September 2022

---

<sup>29</sup> *Id.*

<sup>30</sup> *See* Section III.C-D.

were (1) Hydra; (2) Local Bitcoins, a VASP based/incorporated in Finland; and (3) “TheFiniko.” The majority of these receiving and sending counterparties have evident ties to and/or significant operations in Russia. Moreover, FinCEN notes that Bitzlato engaged in significant transactions with each of these counterparties – all of whom are associated with illicit activities – after publishing its AML/KYC policy (further described below), demonstrating the permissive or ineffective nature of its internal controls.

As noted above, dealings with the Russia-connected darknet market Hydra represented a notable percentage of Bitzlato’s business. Bitzlato operated as a facilitator of sales and purchases of illicit goods and services on behalf of customers and vendors operating on Hydra and supported a larger proportion of business involving Hydra than comparable U.S. CVC exchangers. Prior to its designation by OFAC in April 2022 and its closure in a law enforcement operation, Russia-connected Hydra was the largest darknet market in the world, representing nearly 80 percent of all traceable darknet market transactions in 2021. Bitzlato processed over 1.46 million direct transfers with the Hydra darknet marketplace between May 2018 and early April 2022, representing transactional flows of nearly 20,000 BTC sent and received during that timeframe. Comparative analysis of Bitzlato to a large U.S.-registered CVC exchanger indicates that less than .01 percent of the U.S. exchanger’s transactions were attributed to darknet markets, whereas 6 to 8 percent of Bitzlato’s transactions were attributed to the Hydra darknet market alone. That comparison illustrates that Bitzlato either had a substantially higher appetite for engaging with this illicit darknet market than a U.S.-registered VASP

and/or that Bitzlato did not have the appropriate controls to identify and prevent Hydra's illicit activity from flowing through it.

Although Hydra has been shut down, Bitzlato continues to facilitate transactions for growing Russia-connected darknet markets. As of June 2022, Bitzlato's top counterparties by total number of transactions included three other Russian darknet markets: BlackSprut, OMG!OMG!, and Mega.<sup>31</sup> Since Hydra's closure in April 2022, these three darknet markets show notably increased transaction volumes with Bitzlato as one of their top counterparties by total sending and receiving volumes. Bitzlato's continued facilitation of Russian darknet markets further illustrates its ongoing engagement with actors connected with Russian illicit finance and raises primary money laundering concerns.

### ***C. Bitzlato Has Engaged in a Significant Volume of Russian Illicit Finance Transactions***

According to a study performed by a blockchain analysis company of seven VASPs associated with Moscow City, Russia, between 2019 and 2021, Bitzlato received CVC worth \$206 million from darknet markets, \$224 million from scams, and \$9 million from ransomware attackers, with the value of transactions involving Russian illicit finance or otherwise risky sources quantified as 48 percent of all known Bitzlato transactions.<sup>32</sup> This is the largest proportion of illicit funds received by all seven businesses analyzed during that time, with the second largest being SUEX, at 37 percent. SUEX, a CVC exchanger located in Moscow-City, Russia, was itself designated by

---

<sup>31</sup> Blockchain analysis identifies BlackSprut, OMG!OMG! and Mega as Russian darknet markets that offer narcotics and potentially other illicit goods. Open source reporting has likewise flagged that these darknet markets are Russian.

<sup>32</sup> Chainalysis, "The 2022 Crypto Crime Report," at 128 (February 2022).

OFAC on September 21, 2021, pursuant to E.O. 13694, as amended, for providing material support to the threat posed by criminal ransomware actors.

***D. Bitzlato Does Not Adequately Combat Money Laundering and Illicit Financing on its Platform***

Although Bitzlato’s homepage states that it has a “Know Your Client [(KYC)] policy,” public reporting shows that Bitzlato does not effectively implement policies and procedures designed to combat money laundering and illicit finance, and in fact, has advertised that it lacks such policies, procedures, or internal controls.

Notwithstanding its stated AML/KYC policy, Bitzlato advertises the utility of “simple registration” and does not collect the types of information typically used to conduct effective (AML/CFT).<sup>33</sup> As of March 2022, Bitzlato’s website advertised “simple registration without KYC” with “...neither selfies nor passports required. Only your email [is] needed...” for account creation and transactions on Bitzlato’s platform.<sup>34</sup> As of September 2022, Bitzlato’s advertisement had become more circumspect, offering “simple registration” with “[o]nly your email needed.”<sup>35</sup> Nevertheless, neither advertisement indicates that Bitzlato requires or collects the types of information that would be expected or needed as a part of a set of policies and procedures designed to combat money laundering and illicit finance.

Additionally, Bitzlato advertises user-privacy and anonymity, allowing one to buy and sell CVC with “a P2P fiat-to-crypto exchange,” further stating, “you exchange fiat money and cryptocurrency directly with another person.”<sup>36</sup> This exchange process allows

---

<sup>33</sup> Bitzlato, <https://bitzlato.com> (last accessed January 2023).

<sup>34</sup> Bitzlato, <https://bitzlato.com> (accessed March 2022).

<sup>35</sup> Bitzlato, <https://bitzlato.com> (accessed September 2022 and last accessed January 2023).

<sup>36</sup> “Bitzlato Review,” *CryptoNews*, (accessed March 22, 2022), available at <https://cryptonews.com/reviews/bitzlato/>.

for transfers to or from a traditional financial institution, as well as other traditional methods, and emphasizes that it does not require users to go through the sort of extensive KYC procedures that are required on other exchanges. Furthermore, publicly available information published by third parties indicates that, notwithstanding Bitzlato's public statements regarding its AML/KYC policy, verification may not be required.

On its website as of March 2022, Bitzlato purported to maintain an AML/KYC policy designed to prevent and reduce the potential risks of Bitzlato being involved in any illegal activity, stating that “in accordance with international and local regulations, Bitzlato implements effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, the proliferation of weapons of mass destruction, corruption and bribery and to respond to any form of suspicious activity on the part of its Users [sic].”<sup>37</sup> Bitzlato further states that it implements a verification procedure, and employs an official responsible for compliance with AML standards, transaction monitoring and risk assessment.

In light of its advertised “simple registration without KYC” and exchange processes, Bitzlato's previously stated AML/KYC policy and controls appear to have little impact on its actual operations. In practice, Bitzlato does not appear to be collecting the identifying information that would be necessary to facilitate meaningful KYC analysis. The significant quantity of Bitzlato transactions involving ransomware and darknet market actors provides further evidence that Bitzlato is not following its stated

---

<sup>37</sup> Bitzlato, <https://bitzlato.com/anti-moneylaundering-policy-and-know-your-client-policy> (last accessed January 2023).

AML/KYC policy or identifying suspicious transactions in a way that would allow it to identify and halt the use of its platform by illicit actors.

**IV. Analysis Regarding Finding that Bitzlato is a financial institution operating outside of the United States that is of Primary Money Laundering Concern in Connection with Russian Illicit Finance**

FinCEN was guided in its analysis by the following considerations: (1) the extent to which the institution is used to facilitate or promote money laundering in connection with Russian illicit finance, including through connections to money laundering activity by Russian organized criminal groups; (2) the extent to which the institution is used for legitimate business purposes; and (3) the extent to which action by FinCEN would guard against international money laundering and other financial crimes. While these considerations were drawn from factors identified in 31 U.S.C. § 5318A(c)(2)(B), taking into account the specific circumstances of money laundering activities in connection with Russian illicit finance and the protection of U.S. national security and the U.S. financial system, FinCEN is under no obligation pursuant to section 9714(a) 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.

***A. The extent to which Bitzlato is used to facilitate or promote money laundering in connection with Russian illicit finance, including through connections to money laundering activity by organized criminal groups***

The record amply establishes that Bitzlato has significant ties to Russia and facilitates a significant number of money laundering transactions involving Russia-related ransomware and Russia-related darknet market proceeds.



Bitzlato's significant connections to Russia are evidenced by the following:

(1) Moscow, Russia is the listed location for Bitzlato found on public websites, with a recent study performed by a blockchain analysis company expressly identifying Bitzlato as having a presence in Moscow City, Russia (during the period between 2019 and 2021);<sup>38</sup> (2) the vast majority of its customer base is located in Russia; (3) historical Bitzlato website information claimed it was created by persons in Russia; (4) a registered address in Hong Kong that is a Solo Workshops address – a shared workspace that other Russian companies use as their address of record; (5) as of May 2022, an internet job posting for Bitzlato advertised for a management position in Russia; and (6) in providing an example of a means to purchase or cash out CVC with/to fiat currency, Bitzlato cites transfers in rubles to or from bank accounts with Sberbank, a prominent Russian financial institution that is the subject of Russia-related sanctions administered and enforced by OFAC.

Furthermore, Bitzlato has significant links to Russian illicit finance and Russian criminal actors. A review of illicit actors' direct exposure to Bitzlato shows that a majority of those illicit actors were based in, or had ties to, Russia and Russia-based cybercriminal forums. Russian ransomware groups or affiliates, such as Russia-affiliated Conti, have been observed using Bitzlato. In particular, CVC wallet addresses associated with the Conti ransomware strain and its affiliates, including Trickbot, have engaged in significant BTC transactions involving Bitzlato. Additionally, Bitzlato had a significant transaction history with the Russia-connected Hydra darknet marketplace and continues to facilitate transactions for Russia-connected darknet marketplaces BlackSprut,

---

<sup>38</sup> Chainalysis, "The 2022 Crypto Crime Report," at 128 (February 2022).

OMG!OMG!, and Mega. That Bitzlato is registered in Hong Kong (or that it maintains a registered office in Hong Kong) does not alter FinCEN's assessment that Bitzlato is of money laundering concern in connection with Russian illicit finance. Section 9714(a) does not require that a foreign financial institution be registered or incorporated in Russia to fall within its scope. The statute only requires that FinCEN determine that the institution is a primary money laundering concern *in connection with* Russian illicit finance. That may occur, as it does in the case of Bitzlato, where the financial institution facilitates money laundering transactions for funds derived from illegal activity or the proceeds of illegal activity and that those activities have a nexus to Russia. Given Bitzlato's significant connections to Russia and links to Russian illicit finance and Russian criminal actors, the record demonstrates that, in this case, the statutory threshold under section 9714(a) is met.

***B. The extent to which such institutions, transactions, or types of accounts are used for legitimate business purposes***

The record further amply demonstrates that Bitzlato's services are used, to an unusually large extent, to facilitate illicit finance, particularly when compared to other CVC exchanges, and by illicit actors who seek to circumvent AML/CFT obligations and obfuscate the source of funds or their intended use. Bitzlato lacks an adequate AML/CFT program or safeguards, it has a high ratio of illicit transaction exposure relative to total transaction volume when compared to other exchanges, and it has served as the second largest attributable counterparty for the largest darknet market in the world and continues to support Russia-connected darknet markets.

Although Bitzlato offers services that could potentially be used by licit actors, those services may be found 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 Bitzlato, FinCEN believes that the need to protect U.S. financial institutions from the money laundering risks presented by Bitzlato outweighs any potential legitimate utility its services may provide.

***C. The extent to which action by FinCEN would guard against international money laundering and other financial crimes***

Finding Bitzlato to be a financial institution operating outside of the United States of primary money laundering concern in connection with Russian illicit finance, and prohibiting transmittals of funds, will help insulate the U.S. financial system from international money laundering and other financial crimes. It will further reinforce the importance of AML/CFT compliance in the virtual asset space, help protect the national security of the United States, notify financial institutions around the world of Bitzlato's illicit activity, and set an example for other international partners to follow in the fight against illicit finance and criminal actors.

**V. Considerations in Selecting the Special Measure Prohibiting Transmittals of Funds**

Section 9714(a) does not require consideration of particular factors in determining which one or more special measures to apply to address an identified primary money laundering concern. Nevertheless, although not bound by the factors, FinCEN considered, in this instance, the factors identified in 31 U.S.C. § 5318A(a)(4)(B) to help

guide its analysis in this matter and FinCEN elected to perform interagency consultations<sup>39</sup> prior to issuing this order.

Guided by the following factors, FinCEN finds reasonable grounds exist for concluding that Bitzlato is a financial institution operating outside of the United States that is of primary money laundering concern in connection with Russian illicit finance and that, pursuant to section 9714(a)(2), the imposition of a special measure prohibiting certain transmittals of funds involving Bitzlato is warranted.

***A. Whether similar action has been or is being taken by other nations or multilateral groups***

FinCEN is unaware of any action that has been taken or is being taken by other nations or multilateral groups with regard to Bitzlato. FinCEN, however, believes that the action will provide a strong signal to the international community of the risks posed by Bitzlato and urges counterpart jurisdictions to consider such risks in its supervision of VASPs.

***B. 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***

FinCEN assesses that imposing a prohibition on certain transmittals of funds involving Bitzlato will not present a significant competitive disadvantage for financial

---

<sup>39</sup> In connection with this action, FinCEN consulted with staff at the following Departments and agencies with regard to the proposed order and prohibition: 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. These 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 Bitzlato, or from an account or CVC address administered by or on behalf of Bitzlato, 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.

institutions organized or licensed in the United States given Bitzlato's relatively small size, and the relatively limited burden that compliance with this order would impose.

By U.S. and international standards, Bitzlato represents a limited percentage of daily CVC transfers. As of April 2022, Bitzlato maintained a daily BTC balance that was 0.0185 percent as large as the largest U.S.-domiciled CVC exchange, and it has 0.55 percent as many BTC transfers. Bitzlato's transaction history with this same U.S.-domiciled CVC exchange totals fewer than \$26 million in CVC over four years. By contrast, a CVC price and volume aggregator estimates that a large U.S.-domiciled exchanger processed more than \$2.7 *billion* in transfers *daily*. 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 rejection of certain transmittals of CVC that are received from or originate at Bitzlato 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 as such, compliant institutions may find themselves in receipt of CVC from Bitzlato despite a desire and effort to limit such exposure.<sup>40</sup> As such, this order allows covered financial institutions the flexibility to act

---

<sup>40</sup> 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

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 CVC originated from Bitzlato but were held for an extended period of time in an unhosted wallet, or where the covered financial institution's risk mitigation procedures would preclude returning funds to Bitzlato. 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. 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 Bitzlato***

FinCEN believes that, for the reasons described below, this action will not have an adverse systemic impact, and indeed, will have a positive systemic impact on the international payment, clearance, and settlement system, and on legitimate business activities.

Bitzlato is a small exchange and has a relatively limited presence in the international payment system. As noted above, by comparison to U.S.-domiciled CVC exchanges, Bitzlato represents a relatively limited percentage of daily CVC transfers, by volume. There is no evidence that Bitzlato is a major participant in the international payment system or relied upon by the international banking community.

Rather, given its size and limited international presence, the legitimate business services that it offers would be readily available through other regulated institutions.

---

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]. As such, a prohibition on the receipt of CVC from Bitzlato could not be feasibly implemented even by the most compliant of financial institutions and compliant institutions may find themselves in receipt of CVC from Bitzlato despite a desire and effort to limit such exposure.

Given the redundancy and availability of its services as well as its clear use for illegitimate business, this action will remove from transaction chains a VASP that facilitates illicit or otherwise unduly risky transactions that pose a risk to the international financial system, without clear adverse impact on the international payment, clearance, and settlement system or on legitimate business activities currently involving Bitzlato.

As FinCEN is not aware of timing considerations associated with such service redundancy or availability, there is also no adverse impact associated with the timing of this action.

***D. The effect of the action on U.S. national security and foreign policy***

Given Bitzlato's connection with Russian illicit finance, FinCEN believes that this action is necessary to safeguard U.S. national security and the U.S. financial system, as well as serve key U.S. national security objectives. Targeting illicit proceeds obtained by ransomware actors, especially those with a nexus to Russia, is a high priority for the United States, as evidenced by recent OFAC actions and recently established intergovernmental task forces focused on Russia-related illicit finance threats. As such, this action will complement previous actions taken by the U.S. Government and 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, and by reinforcing 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 and agencies around the world.

## **VI. Consideration of Alternative Special Measures.**

FinCEN considered the other special measures available pursuant to section 9714 prior to selecting the prohibition reflected in this order. Pursuant to section 9714, these measures included: (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. However, prohibiting the transmittal of funds involving Bitzlato is the only means of adequately addressing the threat Bitzlato poses.

In particular, none of the special measures described in 31 U.S.C. § 5318A would effectively address the threat posed by Bitzlato.<sup>41</sup> Any additional recordkeeping, information collection, or reporting requirement would be insufficient to guard against the risks posed by covered financial institutions processing transmittals of funds involving Bitzlato, as such measures may allow such transfers to continue to benefit of illicit actors connected to Russian ransomware activities, darknet markets, and scams. Furthermore, placing condition upon or prohibiting the opening or maintaining in the United States of a correspondent account or payable-through account by any domestic

---

<sup>41</sup> 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, Bitzlato 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.



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 to address the risks of a P2P VASP such as Bitzlato. The types of CVC transactions that Bitzlato facilitates do not rely on correspondent or payable-through accounts between domestic financial institutions and foreign banks, and FinCEN is unaware of such relationships between Bitzlato and U.S. or foreign financial institutions. As such, prohibiting or placing conditions upon the opening of such accounts would be ineffective at addressing the money laundering concern.

For these reasons, FinCEN assesses that the prohibition on the transmittal of funds, including CVC, involving Bitzlato is the most appropriate special measure.

## **VII. Consideration for Imposing the Special Measure Prohibiting Certain Transmittals of Funds by Order**

Section 9714(a) permits the Secretary to impose certain special measures, including the prohibition of certain transmittals of funds, “by order, regulation or otherwise as permitted by law,” and FinCEN considered both the order and regulation options. In light of the imminence of the threats posed by the illicit actors facilitated by Bitzlato, as well as the extent of the illicit transactional activity identified, an order prohibiting certain transmittals of funds is the most appropriate course of action.

In order to ensure orderly implementation, FinCEN will delay the effective date of this order until February 1, 2023.

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

## VIII. Order

### A. Definitions

#### 1. *Bitzlato*

The order defines Bitzlato, a CVC exchanger registered in Hong Kong and previously known as ChangeBot, to mean all subsidiaries, branches, and offices of Bitzlato 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. *Peer to Peer (P2P) Exchangers*

The order defines P2P exchangers to include persons engaged in the business of buying and selling CVC.

#### 6. *Recipient*

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

### *7. Successor Entity*

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

### *8. Transmittal of Funds*

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

### *9. 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 Bitzlato**

### *1. Prohibition*

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

### *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 Bitzlato or from an account or CVC address administered by or on behalf of Bitzlato, that covered financial institution rejects the transaction, preventing the intended recipient from accessing such CVC and returning the CVC to Bitzlato, or to the account or CVC address from which the CVC originated.

***C. Order Period***

The terms of this order are effective February 1, 2023, with no cessation date.

***D. Reservation of Authority***

FinCEN reserves its authority pursuant to Section 9714(a) to impose conditions on certain transmittals of funds from or to Bitzlato, or from or to any account or CVC address administered by or on behalf of Bitzlato.

***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.<sup>42</sup>

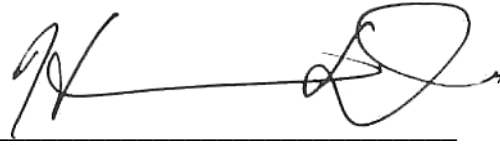
***G. Validity of Order***

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.

---

<sup>42</sup> 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.

Dated: January 18, 2023

A handwritten signature in black ink, consisting of a stylized 'H' followed by a long horizontal line and a circular flourish at the end.

---

Himamauli Das  
Acting Director  
Financial Crimes Enforcement Network