UNITED STATES OF AMERICA
FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

IN THE MATTER OF:	)	
	)	**Number 2025-02**
Paxful, Inc. and	)	
Paxful USA, Inc.	)	
	)	

CONSENT ORDER IMPOSING CIVIL MONEY PENALTY

The Financial Crimes Enforcement Network (FinCEN) conducted a civil enforcement investigation and determined grounds exist to impose a Civil Money Penalty against Paxful, Inc. and Paxful, USA Inc. (collectively, Paxful or the Company)[1] for violations of the Bank Secrecy Act (BSA) and its implementing regulations.[2] Paxful admits to the Statement of Facts and Violations set forth below, consents to the issuance of this Consent Order, agrees to pay the civil money penalty imposed in this Consent Order, and agrees to comply with the provisions of this Consent Order.

I. JURISDICTION

Overall authority for enforcement and compliance with the BSA lies with the Director of FinCEN, and the Director of FinCEN may impose civil penalties for violations of the BSA and its implementing regulations.[3]

[1] Unless otherwise indicated, all references to Paxful or the Company prior to 2019 are to Paxful, Inc. Thereafter, all references to Paxful or the Company are to both Paxful, Inc. and Paxful USA, Inc., unless otherwise indicated.
[2] The BSA is codified at 12 U.S.C. §§ 1829b, 1951-1960, 31 U.S.C. §§ 5311-5314, 5316-5336 and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 C.F.R. Chapter X.
[3] 31 U.S.C. § 5321(a); 31 C.F.R. § 1010.810(a), (d); Treasury Order 180-01 (July 1, 2014, reaff'd Jan. 14, 2020).

Paxful was a "domestic financial institution," specifically, a "money services business" (MSB), as defined by the BSA and its implementing regulations, at all times relevant to this Consent Order.[4]

The term "money services business" is defined in 31 C.F.R. §1010.100(ff) as any of the following categories of business: (1) dealers in foreign exchange; (2) check cashers; (3) issuers or sellers of traveler's checks or money orders; (4) providers of prepaid access; (5) money transmitters; (6) U.S. Postal Service; or (7) sellers of prepaid access. The regulations define the term "money transmitter" as a person that either "provides money transmission services" or who is otherwise "engaged in the transfer of funds."[5] "Money transmission services" are defined in FinCEN's regulations as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[6] Paxful's activity, as described in this Consent Order, meets the definition of a money transmitter, a type of MSB.

Registration: The BSA and its implementing regulations require an MSB, such as Paxful, to register as an MSB with FinCEN within 180 days of beginning operations and to renew that registration every two years.[7]

AML Program: The BSA and its implementing regulations require an MSB, such as Paxful, to develop, implement, and maintain an effective Anti-Money Laundering (AML) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the

[4] *See* 31 U.S.C. § 5312(b)(1) (defining domestic financial institution); 31 C.F.R. §§ 1010.100(ff) (defining "money services business") and 1010.100(ff)(5) (defining "money transmitter"). FinCEN also issued interpretive guidance explaining why CVC exchangers are money transmitters. *See* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013; *see also* FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019.
[5] 31 C.F.R. § 1010.100(ff)(5).
[6] 31 C.F.R. § 1010.100(ff)(5)(i)(A).
[7] 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(b)(2), (3).

financing of terrorist activities.[8] Paxful was required to develop, implement, and maintain an effective, written AML program that, at a minimum: (1) incorporates policies, procedures, and internal controls reasonably designed to assure ongoing compliance with the BSA and its implementing regulations; (2) designates an individual responsible to assure day-to-day compliance with the MSB's AML program and all BSA regulations; (3) provides education and/or training for appropriate personnel, including training in the detection of suspicious transactions; and (4) provides for independent review to monitor and maintain an adequate program.[9]

Suspicious Activity Reporting: The BSA and its implementing regulations require an MSB, such as Paxful, to identify and report suspicious transactions relevant to a possible violation of law or regulation in Suspicious Activity Reports (SARs) filed with FinCEN. Specifically, the BSA and its implementing regulations require MSBs to report transactions that involve or aggregate to at least $2,000, are conducted by, at, or through the MSB, and that the MSB "knows, suspects, or has reason to suspect" are suspicious.[10] A transaction is "suspicious" if an MSB "knows, suspects, or has reason to suspect" the transaction (or a pattern of transactions of which the transaction is a part): (1) involves funds derived from illegal activities, or is intended or conducted to disguise funds derived from illegal activities; (2) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; (3) has no business or apparent lawful purpose, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction; or (4) involves the use of the MSB to facilitate

[8] 31 U.S.C. § 5318(h); 31 C.F.R. § 1022.210(a).
[9] 31 U.S.C. § 5318(h)(1); 31 C.F.R. § 1022.210(d), (e) ("A [MSB] must develop and implement an [AML] program that complies with the requirements of this section on or before . . . the end of the 90-day period beginning on the day following the date the business is established.").
[10] 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320.

criminal activity.[11] An MSB is generally required to file a SAR no later than 30 calendar days after the initial detection by the MSB of the facts that may constitute a basis for filing a SAR.[12]

II. STATEMENT OF FACTS

The conduct described below took place from on or about February 3, 2015 through April 4, 2023 (the Relevant Time Period), unless otherwise indicated.[13]

A. FinCEN

FinCEN is a bureau within the U.S. Department of the Treasury and is the federal authority that enforces the BSA by investigating and imposing civil money penalties on financial institutions and individuals for willful violations of the BSA.[14] As delegated by the Secretary of the Treasury, FinCEN has "authority for the imposition of civil penalties" and "[o]verall authority for enforcement and compliance" with the BSA and its implementing regulations.[15]

B. Paxful

Throughout the Relevant Time Period, Paxful operated as an exchanger of convertible virtual currencies (CVC), and operated both a hosted CVC wallet service and a marketplace that connected peer-to-peer (P2P) buyers and sellers of CVC. Paxful is a Delaware corporation and, within the Relevant Time Period, had a physical office location in New York City. During the Relevant Time Period, Paxful conducted transactions in CVC and offered over 400 payment methods for trading

[11] 31 C.F.R. § 1022.320(a)(2)(i)-(iv).
[12] 31 C.F.R. § 1022.320(b)(3).
[13] Starting in April 2023, new owners and management took control of Paxful, replacing and removing the management and ownership who were in place during the Relevant Time Period. References herein to Paxful's "then-management or leadership" are to individuals not employed by Paxful after the Relevant Time Period.
[14] 31 U.S.C. § 5321(a). In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. Paxful admits to "willfulness" only as the term is used in civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1).
[15] 31 C.F.R. § 1010.810(a), (d).

CVC, ranging from prepaid access cards to bank transfers or cash-by-mail. Within the Relevant Time Period, Paxful conducted transactions with over 4 million users, including over 50 million successful trades on its platform worth several billion dollars in trade value across a range of products, including CVC, prepaid access cards, and various fiat currencies. Additionally, during the Relevant Time Period, Paxful's hosted wallet service had millions of users.

In addition to these transactions on Paxful's platform, FinCEN's investigation identified over 20 million external bitcoin transactions worth well over $10 billion to or from Paxful's customer accounts. On a weekly basis during the Relevant Time Period, Paxful processed tens of millions of dollars' worth of bitcoin deposits and withdrawals.

During the Relevant Time Period, Paxful willfully failed to: (1) maintain its registration with FinCEN; (2) implement an effective AML program; and (3) identify and timely report suspicious activity. These violations caused significant harm to the U.S. financial system by allowing illicit actors to use Paxful to conduct hundreds of millions of dollars' worth of transactions with suspicious counterparties, including individuals from North Korea and Iran, ransomware attackers, and the website Backpage.com—all without timely filing SARs.

C. Paxful Failed to Register as an MSB

The BSA and its implementing regulations require an MSB to register within 180 days of beginning operations and the renewal of such registration every two years.[16]

In accordance with the BSA, Paxful initially registered with FinCEN on July 27, 2015, 174 days after launching its hosted wallet and P2P exchange business. Paxful was required to re-register with FinCEN no later than December 31, 2016.[17] Paxful did not re-register with FinCEN until

[16] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(b)(2), (3).
[17] An MSB must renew its registration on or before the last day of the calendar year preceding the renewal period. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(b)(3).

September 3, 2019, despite continuing to act as a money transmitter at all times between January 1, 2017 and September 2, 2019. As such, Paxful operated as an unregistered MSB for 974 days in violation of the requirement to register. Paxful's former Chief Technology Officer later admitted to allowing Paxful's MSB registration to lapse while continuing to operate Paxful as a money transmitter during this period.[18]

D. Paxful Failed to Develop, Implement, and Maintain an Effective AML Program

Paxful willfully failed to develop, implement, and maintain an effective AML program. Paxful failed to implement ***any*** written AML program until July 2019, more than four years after it initially began business. The AML program remained deficient even after Paxful implemented one. Throughout the Relevant Time Period, Paxful's AML program violations spanned multiple pillars. Paxful's AML program did not provide for effective or timely review of transactions, failed to identify significant customer red flags, and was not appropriately implemented by Paxful staff. Illicit actors ranging from hostile nation states like Iran and North Korea to online services that facilitated child sexual abuse material (CSAM) were able to exploit Paxful's platform and the U.S. financial system as a result of these deficiencies. Paxful failed to identify, and appropriately report, numerous other types of illicit activity, including but not limited to incidents associated with the financing of terrorism.

1. Paxful Failed to Implement Policies, Procedures, and Internal Controls to Verify Customer Identity

Paxful failed to have any policies, procedures, and internal controls or a formal written AML program until early 2019. Prior to such implementation, Paxful struggled to identify significant volumes of potentially illicit activity on its platform. Failures continued after 2019, as the policies Paxful established did not sufficiently account for the risks associated with its business lines.

[18] *See* Plea Agreement at A-1, *United States of America. v. Artur Schaback*, 2:24-cr-00072-KJM (E.D. Cal. July 8, 2024).

i. Pre-February 2019

Paxful's lack of any "know your customer" (KYC)[19] processes before February 2019 contributed to the establishment and maintenance of relationships with high-risk customers that conducted significant volumes of activity without appropriate risk mitigation. For example, Paxful processed extensive transactions related to, and maintained a customer relationship with, the website Backpage.com (Backpage), a now-disbanded website that, according to the U.S. Department of Justice (DOJ), "earned hundreds of millions of dollars from facilitating prostitution and sex trafficking, placing profits over the well-being and safety of the many thousands of women and children who were victimized by its practices."[20] Backpage operated as a website that charged individuals to post advertisements that solicited customers to purchase goods and services. Many of the advertisements published on Backpage depicted children who were victims of sex trafficking.[21]

Paxful not only lacked policies, procedures, or internal controls to identify high-risk customers doing business on or through Backpage, but also actively solicited their business. Paxful's social media accounts advertised how Backpage customers could create accounts on Paxful to sell advertisements on the Backpage platform. Paxful, through its P2P marketplace, allowed vendors selling content on Backpage to receive both CVC and prepaid access cards as payments when selling their content to buyers on Backpage. Paxful made statements to the media touting this relationship as a business opportunity after credit card operators dropped Backpage.[22]

However, Paxful's own employees questioned the relationship between Paxful and Backpage as early as 2017, stating, "I've been trying to find everything about backpage.com today and now I

[19] KYC, or Know Your Customer, refers to the information that financial institutions collect from their customers to document and understand basic information about the customer and its intended relationship with the financial institution.
[20] U.S. Dep't of Justice, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment" (Apr. 9, 2018).
[21] *Id*.
[22] Brave New Coin, "Peer to Peer Bitcoin Exchange Reaps Reward of Backpage Fallout" (Aug. 12, 2015).

hope someone closes it down[.] [I]t's disgusting trafficing [*sic*] children." Paxful processed over 4 million transactions involving Backpage valued at over $24 million. Although Paxful was not requiring KYC during this time, its records included usernames, email addresses, CVC wallet addresses, and details of specific payments related to Backpage that should have raised red flags. Nevertheless, Paxful did not file a single SAR on this activity, even after the government seized Backpage in 2018. [23]

Backpage was only one of the high-risk merchants Paxful sought out. Paxful conducted over $3.5 billion in CVC transactions prior to its implementation of any KYC policies, procedures, and internal controls.

ii. Post-February 2019

On February 15, 2019, Paxful announced new mandatory KYC requirements for its users and those listing advertisements on the Company's website. However, these controls were deficient, applying only to users with activity that exceeded $1,500 without any controls to identify users who sought to evade these controls by structuring transactions. These lax policies led to customers choosing Paxful to take advantage of the inadequate KYC controls. For example, in a September 2019 exchange on a social media site, several individuals referenced Paxful as a potential P2P exchange to utilize instead of an alternate P2P trading site that had implemented more robust KYC procedures. Then-Paxful employees advertised the lax policy and offered to "port [customer's] stats" to entice customers to switch from competitor exchanges. In total, Paxful processed billions in CVC transactions alone from March 2019 through April 2023. During this same period, Paxful experienced growth that at times exceeded 20% annually.[24]

[23]U.S. Dep't of Justice, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment" (Apr. 9, 2018).
[24] *See* Newswire.com, Paxful Hits $5 Billion Volume (last visited Aug. 4, 2025).

2. Paxful Failed to Identify and Mitigate Risks Posed by Customers Conducting Unregistered MSB Activity in its P2P Product

Paxful's AML program was required to be "commensurate with the risks posed by the location and size of, and the nature and volume of the financial services" it provided.[25] However, Paxful's AML policies, procedures, and internal controls failed to cover critical elements of the services offered by its P2P trading marketplace, such as the unique risks presented by certain types of customers. For example, Paxful's written AML program included provisions to collect and retain customers' FinCEN MSB registrations but, in practice, Paxful did not implement these provisions or establish policies, procedures, and internal controls to identify unregistered MSB activity on its platform. Even though Paxful identified the risks that could flow from smaller unregistered P2P exchangers that used Paxful to engage in money transmission, Paxful did not implement policies, procedures, or internal controls to ensure Paxful was not exploited by illicit actors through these smaller exchangers. As discussed further below, Paxful also did not file SARs when required by the BSA and its implementing regulations.

3. Paxful Failed to Identify and Address Geographic Spoofing

Paxful failed to implement effective policies, procedures, and internal controls to identify when customers were using geographic spoofing (geo-spoofing) to hide the location from where they were doing business, including using virtual private networks (VPNs). Further, Paxful failed to implement any controls to review a customer's geography, including through Internet Protocol (IP) addresses.[26] Prior to January 2018, Paxful failed to implement any meaningful IP restrictions on

[25] 31 C.F.R. § 1022.210(b).

[26] "Geo-spoofing" is the act of concealing a person's true location by altering the Internet Protocol address to reflect that the person is connecting to the internet from a different location. A VPN has the effect of "masking" a user's true IP address. Financial institutions often use IP addresses to determine the jurisdiction from which a user has accessed its website or mobile application which can then be used as part of the financial institution's "geofencing controls" to identify and block or restrict access, including to support efforts by the financial institution to "ringfence" itself from certain jurisdictions (*e.g.*, higher risk jurisdictions or those in which it has elected to not obtain a license or register to do business). However, such controls can be rendered ineffective as the result of VPN masking.

customer activity, including for North Korea, Iran, Syria, and Cuba.[27] In fact, Paxful's own assessment of its activity identified over 1,500 accounts opened between May 2015 and August 2018 with Iranian, Syrian, Cuban, Crimean, or Sudanese IP addresses. Paxful's ineffective geo-spoofing controls also failed to identify tens of millions of users that logged in to its trading platform with U.S. IP addresses, even though users were not located in the United States, including significant volumes of users from Nigeria and China.

4. Paxful Failed to Implement Policies, Procedures, and Internal Controls for Transaction Monitoring

Paxful's AML program did not adequately address specific risks associated with its different products and services. Despite offering hundreds of ways to conduct transactions on Paxful, including multiple types of CVC, Paxful failed to conduct transaction monitoring on the products and services offered on the platform, which allowed the platform to be used to facilitate money laundering. Rather than implement controls, Paxful's then-senior leaders ignored employees raising potentially suspicious or fraudulent transactions. When asked about what the platform would do to address such issues, then-senior leadership told staff they were working on ways to address the issues, yet even minimal transaction monitoring was not in place until at least 2018, more than three years after Paxful began operating.

Written transaction monitoring policies, procedures, and internal controls were not in place prior to July 2019. As a result, ***all*** transactions conducted on Paxful, in fiat currency, CVC, or prepaid access cards were not appropriately reviewed for potentially suspicious activity before then. Additionally, the July 2019 procedures did not adequately address all of Paxful's products and

[27] *See, e.g.*, FinCEN, Imposition of Fifth Special Measure Against the Democratic People's Republic of Korea as a Jurisdiction of Primary Money Laundering Concern, 81 Fed. Reg. 78,715 (Nov. 9, 2016) (codified at 31 C.F.R § 1010.659); *see also* FinCEN, Imposition of Fifth Special Measure Against the Islamic Republic of Iran as a Jurisdiction of Primary Money Laundering Concern, 84 Fed. Reg. 59,302 (Nov. 4, 2019) (codified at 31 C.F.R. § 1010.661).

services, and left significant gaps in reviewing transactions made in prepaid access cards. Paxful acquired additional blockchain analytic tools in March 2020, but omitted coverage for several CVCs offered on its platform, meaning Paxful continued to fail to appropriately monitor all of the CVC offered on its platform. Paxful had no ability to identify and report suspicious activity within the significant volume of transactions in over 15 CVCs, including Dogecoin, Ripple, Ethereum, Tron, and Tether, throughout the Relevant Time Period.

5. Paxful Failed to Effectively Monitor Prepaid Access Transactions

MSBs like Paxful must implement policies, procedures, and internal controls that cover the products and services offered to customers.[28] In addition to material gaps in Paxful's ability to monitor CVC activity, Paxful further failed to implement appropriate policies, procedures, and internal controls to meaningfully monitor and report illicit activity taking place in its prepaid access sales across its platform.[29] This was a substantial portion of Paxful's overall business activity during the Relevant Time Period. For example, from May 2015 through December 2019, the top payment methods through Paxful were iTunes and Amazon prepaid access cards, constituting over $1.7 billion in value transmitted through Paxful. In 2020, trades where users converted CVC to prepaid access cards constituted over half the total bitcoin volume traded on the platform, or around $20 million worth of transactions per week. Paxful prioritized development of the prepaid access market even though it knew illicit actors were exploiting it. For example, in an exchange with an individual from Ghana who purported to offer explicit images in exchange for prepaid access cards, a then-member

[28] 31 C.F.R. § 1022.210(d)(1).
[29] 31 C.F.R. § 1022.210(d)(1)(i)(A) and (B).

of Paxful's management team told other Paxful employees that they "told her about Paxful so she could sell her scammed itunes cards lol." Paxful began to remediate these deficiencies in April 2023.

6. Paxful's North Korean, Iranian, and Terrorist Finance Transactions

Paxful's failure to implement policies, procedures, and internal controls to verify customer identity and appropriately monitor transactions directly contributed to Paxful facilitating transactions with hostile nation-states and state-sponsored cyber criminals from Iran and North Korea.

Paxful processed transactions with individuals associated with the Lazarus Group, a North Korean state-sponsored cyber-criminal group that Treasury's Office of Foreign Assets Control (OFAC) designated for malicious cyber activity on critical infrastructure.[30] Paxful took no action even after receiving law enforcement inquiries related to this activity. Yinyin Tian (Tian), a member of the Lazarus Group, conducted thousands of trades on Paxful's platform between October 2017 and November 2018. These high-risk transactions involved converting CVC sales to Apple iTunes prepaid access cards while frequently moving money between various jurisdictions on the Paxful platform, including between the United States, China, and Hong Kong. Paxful subsequently received law enforcement inquiries in December 2018 and October 2019 related to the more than $1.4 million Tian ultimately moved through his account. At the very least, such contact by law enforcement should have alerted Paxful that additional due diligence for this particular customer and his transactions was required. Nonetheless, only in May 2020—two months after Tian's bitcoin address was listed as an attribute on OFAC's Specially-Designated Nationals (SDN) list—did Paxful take any action.

In a separate example also involving Paxful's P2P marketplace, FinCEN's investigation identified several transactions taking place on Paxful's platform within a 24-hour period where a buyer and seller exchanged bitcoin for North Korean won. The offer terms advertised on Paxful

[30] U.S. Dep't of the Treasury, "Treasury Sanctions North Korean State-Sponsored Cyber Groups" (Sept. 13, 2019).

explicitly offered BTC to PayPal in North Korean won. North Korea is subject to comprehensive U.S. economic and trade sanctions and is a jurisdiction of primary money laundering concern.[31] Further, the receiving party in these transactions switched jurisdictions multiple times in the span of hours and sometimes minutes for each trade, indicating use of a VPN to obfuscate their location. Despite these clear red flags, Paxful's inadequate transaction monitoring resulted in the failure to identify or report this activity.

Paxful's ineffective policies, procedures, and controls also led to additional transactions with Iranian individuals who were eventually designated by OFAC. Paxful conducted dozens of transactions with EnExchanger and Iranvisacart.[32] Transactions with these users bore clear indicia of suspicion from taking place in Iran (including IP information and the use of the name "Iranvisacart" in advertisements), operating as unregistered P2P exchangers, and having significant exposure to CVC wallets associated with ransomware proceeds illicitly obtained by Iranian hacking groups. Paxful took no action even after OFAC's designations.

Paxful's failures also resulted in other illicit activity going unmonitored or reported. Multiple fundraisers by groups designated by the United States as Foreign Terrorist Organizations received payments from Paxful customers. For example, Paxful permitted transactions as part of a fundraising campaign for al-Qaeda in January 2019. On October 8, 1999, the United States Secretary of State designated al-Qaeda as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act and it was later designated in September 2001 as a Specially Designated Global Terrorist pursuant to Executive Order 13224.

---

[31] *See* FinCEN, Imposition of Fifth Special Measure Against the Democratic People's Republic of Korea as a Jurisdiction of Primary Money Laundering Concern, 81 Fed. Reg. 78,715 (Nov. 9, 2016) (codified at 31 C.F.R. § 1010.659); *see also* OFAC, North Korea Sanctions Program, (Nov. 2, 2016).

[32] *See* U.S. Dep't of the Treasury, "Cyber-related Designations; Publication of New Cyber-related FAQs" (Nov. 28, 2018) (designating individuals with the aliases "EnExchanger" and "Iranvisacart").

7. Compliance Officer

An MSB is required to designate a person to assure day-to-day compliance with its compliance program and the BSA. This person is responsible for assuring that the MSB files reports and creates and retains records, as well as ensuring that the compliance program is updated as necessary to reflect the current requirements of the BSA and provides appropriate training.[33]

From the beginning of its operations through 2018, Paxful operated without a qualified individual to assure day-to-day compliance with the BSA. Paxful listed its then-CEO as the chief compliance officer during this time period. However, the former CEO never received ***any*** BSA/AML-specific training or had the appropriate experience to meet the compliance obligations under the BSA. Indeed, Paxful had egregious lapses in compliance while the former CEO held this role, allowing the company's FinCEN registration to lapse, failing to implement even a rudimentary AML program that required it to conduct KYC on its users, and filing no SARs.

8. Independent Testing

An MSB must provide for independent review to monitor and maintain an adequate program.[34] The scope and frequency of the review shall be commensurate with the risk of the financial services provided by the MSB.[35] During the Relevant Time Period, Paxful conducted only a single independent test, a frequency of testing that is not even remotely commensurate with the volume of transactions processed or risks associated with the products and services offered by Paxful. Appropriate independent testing performed on a recurring basis would have identified AML program gaps and potentially suspicious transactions that went unreported.

[33] 31 C.F.R. § 1022.210(d)(2)(i)-(iii).
[34] 31 C.F.R. § 1022.210(d)(4).
[35] *Id.*

E. Paxful Failed to File Suspicious Activity Reports

FinCEN identified hundreds of suspicious transactions for which Paxful failed to timely and accurately file a SAR. Paxful facilitated transactions involving over $500 million in suspicious activity associated with ransomware attacks, darknet and other illicit marketplaces, unregistered MSBs, including unregistered CVC mixing services, CSAM, elderly financial exploitation, individuals later listed on OFAC's SDN list, terrorist financing, high-risk jurisdictions, and stolen funds or other illicit proceeds. Paxful leadership refused to improve the Company's SAR reporting for years, even instructing employees not to file SARs on suspicious activity. Paxful never filed a single SAR with FinCEN until November 2019, and even after November 2019, Paxful's SAR filing deficiencies continued.

1. Ransomware Attack Proceeds

Ransomware is malicious software that restricts the victim's access to a computer in exchange for a specified ransom, usually paid in bitcoin. If the specified ransom is not paid, the victim may be threatened with the loss or exposure of their personal data, such as account numbers and social security numbers. Ransomware perpetrators have targeted U.S. hospitals, schools, and other vital public services in addition to U.S. businesses.

Paxful CVC wallet addresses interacted directly with over 26 different strains of ransomware. These included transactions associated with SamSam, Trickbot, BitLocker, Phobos, Crysis-Dharma, and BitPaymer. Gaps in Paxful's controls and policies resulted in it interacting with hundreds of thousands of dollars of CVC addresses in hundreds of transactions associated with ransomware, on which Paxful failed to timely and accurately file SARs.

2. Child Exploitation Marketplaces

Paxful wallets facilitated hundreds of transactions with child exploitation-associated addresses. The marketplaces involved in the transactions included marketplaces dealing CSAM, such as Backpage, Welcome to Video, Dark Scandals, and several other known purveyors of CSAM. Welcome to Video was a marketplace hosted on the Darknet that exclusively advertised child sexual exploitation videos available for download by members of the site. Welcome to Video contained over 250,000 unique videos and had at least one million users. Paxful processed nearly 100 transactions with Welcome to Video related to more than 50 accounts that Paxful maintained for Welcome to Video customers over more than two years before the marketplace was shut down by law enforcement in early 2018.[36] Paxful's failure to perform basic customer verification or sufficient transaction monitoring meant that no additional scrutiny was applied to these transactions, and, therefore, Paxful failed to timely file SARs despite the obvious suspicious nature of the activity. Similarly, Paxful did not timely and accurately file SARs on several other known child exploitation-associated transactions within the required timeframe.

3. Darknet and other Illicit Markets

Paxful facilitated tens of millions of dollars with darknet or other illicit marketplace-associated addresses. Such markets facilitate the purchase and sale of illegal narcotics and controlled substances, drug paraphernalia, counterfeit and fraud-related goods and services, and other illegal contraband. This included millions of dollars' worth of value in direct transactions with prolific darknet marketplace AlphaBay, later seized by the DOJ.[37] Paxful failed to file hundreds of SARs for these and other illicit marketplace-associated transactions in a timely manner.

---

[36] U.S. Dep't of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin" (Oct. 16, 2019).
[37] U.S. Dep't of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down" (July 20, 2017).

4. Convertible Virtual Currency Mixing Services

Illicit actors can use CVC mixers—which anonymize CVC addresses and obscure CVC transactions by weaving together inflows and outflows from many different users—to launder illicit proceeds and disrupt the ability to trace CVC transactions. Darknet marketplaces actively promote mixers as the primary method for obfuscating bitcoin transactions. Paxful addresses interacted with at least 13 unregistered CVC mixing services during the Relevant Time Period, including Helix against which FinCEN assessed a $60 million civil penalty in 2020 for BSA violations.[38] Paxful did not identify and report any of the underlying transactions as suspicious despite the known red flags associated with these services. Paxful wallets facilitated the transfer of the equivalent value of over $35 million to and from unregistered CVC mixing services without filing any timely SARs.

5. Transactions with Individuals and Financial Institutions in Iran, North Korea, and Venezuela

Paxful facilitated direct transactions with parties later added to the SDN list, including EnExchanger, Iranvisacart, and Tian. Each of these entities bore indicia of suspicion even prior to their respective designations by OFAC. Paxful allowed these entities to conduct multiple transactions over extended periods in equivalent values exceeding $1 million. Paxful failed to timely file SARs on this activity, even after these entities were listed on OFAC's SDN list.

Further, Paxful failed to file SARs on large sums of value being transmitted to and from exchanges operating in high-risk jurisdictions subject to both comprehensive and specific economic sanctions by U.S. government regulations. Paxful addresses interacted with 16 virtual asset service providers that were publicly operating from Iran and Venezuela. Paxful wallets facilitated the transfer

[38] *In the matter of Larry Dean Harmon d/b/a Helix*, Number 2020-2 (FinCEN Oct. 19, 2020) (assessment of civil monetary penalty).

of over $3 million to and from these virtual asset service providers. Paxful clients were also allowed to trade in Venezuelan "Petro" CVC.[39] Paxful failed to file timely SARs on any of these transactions.

6. Alleged Stolen Funds and other Illicit Proceeds

Paxful accepted and transmitted CVC with wallets containing the proceeds of various acts of cybercrime. CVC passed through Paxful from these cybercriminal wallets holding value from large-scale elder exploitation, stolen credit card information forums, fraudulent crypto investment scams, and other criminal organizations. Paxful failed to file any timely SARs on such transactions.

Paxful maintained accounts for, and actively solicited business from, Mayrodi Mundial Moneybox (MMM) as early as 2017. MMM was a Russia-based Ponzi scheme that financially defrauded millions of people in the 1990s, and after its founder was released from Russian prison in 2011, relaunched as a CVC-only platform focused on the developing world, including in Nigeria in 2015. Paxful employees were aware of the MMM Ponzi scheme, describing it internally as a "shady" financial pyramid scheme, but nevertheless openly discussed how to drive MMM customers to Paxful. Paxful believed that if negotiations went well, "***we will have our new [B]ackpage***." Paxful failed to file timely SARs on any of this activity.

Black Axe was a fraud and money laundering ring that often used romance scams to exploit widowed or divorced elderly women financially. [40] Over more than three years—including roughly a year after the DOJ indicted one of the founders—Black Axe conducted over $620 million in transfers via bitcoin, gift cards, and wire transmissions through Paxful. The volume, location, frequency, and amount of these transactions over a significant period afforded Paxful multiple opportunities to identify and report the hundreds of millions of dollars of Black Axe transactions

[39] *See* Taking Additional Steps to Address the Situation in Venezuela (Executive Order 13827), 83 Fed. Reg. 12,469 (Mar. 21, 2018) (prohibiting transactions in "Petro").
[40] U.S. Dep't of Justice, "Organizer Of Complex Nigerian Fraud And Money Laundering Ring Sentenced" (Oct. 17, 2019).

taking place on Paxful for over three years; nevertheless, Paxful failed to file any timely SARs on this activity.

III. VIOLATIONS

FinCEN has determined that Paxful willfully violated the BSA and its implementing regulations during the Relevant Time Period.[41] Specifically, FinCEN has determined that Paxful willfully failed to register as an MSB with FinCEN in violation of 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380. Further, Paxful failed to develop, implement, and maintain an effective AML program that was reasonably designed to prevent its trading platform and hosted wallet service from being used to facilitate money laundering and the financing of terrorist activities in violation of 31 U.S.C. § 5318(h)(1) and 31 C.F.R. § 1022.210. Additionally, FinCEN has determined that Paxful willfully failed to accurately, and timely, report suspicious transactions to FinCEN, in violation of 31 U.S.C. § 5318(g)(1) and 31 C.F.R. § 1022.320.

IV. ENFORCEMENT FACTORS

As summarized below, FinCEN considered all factors outlined in the Statement on Enforcement of the Bank Secrecy Act issued August 18, 2020, when deciding whether to impose a civil money penalty in this matter.[42]

1. **Nature and seriousness of the violations, including extent of possible harm to the public and the amounts involved**: Paxful's violations of the BSA and its implementing regulations were egregious and caused extensive possible harm to the public. For a number of years, Paxful disregarded its AML obligations and took no steps to detect, deter, and report suspicious or illicit

[41] To establish that a financial institution acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose.

[42] FinCEN, "Financial Crimes Enforcement Network (FinCEN) Statement on Enforcement of the Bank Secrecy Act," (Aug. 18, 2020).

activity occurring on its platform. Paxful's subsequent efforts for the remainder of the Relevant Time Period were woefully inadequate, not based on the illicit finance risks of its business and, in some instances, could easily be circumvented by users. Paxful's failure to implement and maintain an effective AML program occurred despite the presence of numerous and repeated AML-related warning signs regarding specific customers or financial products. Personnel across various levels of the Company were complicit in these violations over the period in which the violations occurred. As a result, and based on available information, FinCEN identified thousands of potentially suspicious transactions Paxful processed that involved alleged narcotics sales, fraud, sex trafficking, child exploitation, sanctions evasion, ransomware attacks, and unregistered mixing services, none of which were timely or accurately reported to FinCEN. These substantial failures deprived law enforcement and national security agencies of crucial reporting and caused—and in some cases may have prolonged—public harm by allowing bad actors to avoid detection.

2. **Impact or harm of the violations on FinCEN's mission to safeguard the financial system from illicit use, combat money laundering, and promote national security**: From 2015 to 2019, Paxful did not have effective policies and procedures to detect and report suspicious activity. Paxful failed to conduct even minimal suspicious activity monitoring during this time, making it difficult to ascertain the complete number of specific reporting violations that exist. FinCEN identified hundreds of instances where Paxful should have filed a SAR. By denying this information to law enforcement agencies and financial regulators, Paxful had a detrimental impact on FinCEN's mission and withheld critical reporting pertaining to the DPRK, Iran, CSAM, ransomware, and other national security priorities.

3. **Pervasiveness of wrongdoing within an entity, including management's complicity in, condoning or enabling of, or knowledge of the conduct underlying the violation**: Paxful's failures to comply with FinCEN's regulations appear to have been the result of a culture of non-compliance throughout the Company for much of the Relevant Time Period. By no later than July 2015, Paxful's leadership, including the former CEO, demonstrated actual knowledge of their obligations under the BSA, including by registering with FinCEN. Nevertheless, the Company failed to comply with these obligations for more than three years, and, in several instances, solicited or engaged in business with high-risk customers and financial products. During this time, senior officials, including the former CEO, actively sought a business relationship with Backpage or acknowledged the risks of fraud associated with the gift card exchange without taking any steps to mitigate these risks or monitor and report instances of suspicious activity.
4. **History of similar violations or misconduct in general, including prior criminal, civil, and regulatory enforcement actions**: FinCEN is not aware of any prior criminal, civil, or regulatory enforcement action taken against Paxful. However, Paxful experienced significant and prolonged deficiencies in its compliance with the BSA and 31 C.F.R. Chapter X during the entire course of its operation as a financial institution, with Paxful introducing only modest and inadequate changes more than three years after its initial launch.
5. **Financial gain or other benefit resulting from, or attributable to, the violation**: For years, Paxful did not appropriately resource compliance with its AML requirements despite processing billions of dollars' worth of transactions. As a result, the Company's growth was fueled in part through facilitating transactions made by potentially suspicious activity, including transactions with high-risk jurisdictions and exposure to high-risk counterparties like darknet markets and

unregistered MSBs. Paxful operated without appropriate compliance personnel, training, and policies and procedures in place for at least four years.

6. **Presence or absence of prompt, effective action to terminate the violations upon discovery, including self-initiated remedial measures**: From its initial operations through 2019, Paxful had few, if any, controls in place to mitigate Paxful's exposure to money laundering and terrorist finance. Starting in early 2019, Paxful began taking certain steps to implement an effective AML program and comply with the BSA and FinCEN's regulations. However, even after Paxful commenced these modest efforts, it took several years to fully address many of the issues identified by FinCEN's investigation, including controls necessary for the timely and accurate filing of SARs. Many of these changes took place only after the replacement of senior leadership in April 2023. Since April 2023, Paxful has engaged with independent consultants to review a backlog of potentially suspicious transactions, resulting in the filing of thousands of SARs for transactions that took place during the Relevant Time Period.
7. **Timely and voluntary disclosure of the violations to FinCEN**: Paxful did not voluntarily self-disclose the violations described above to FinCEN.
8. **Quality and extent of cooperation with FinCEN and other relevant agencies, including as to potential wrongdoing by its directors, officers, employees, agents, and counterparties**: Paxful was forthcoming with FinCEN during its investigation, including by making complete and timely productions in response to FinCEN's information requests. Paxful also agreed to toll the statute of limitations during FinCEN's investigation. Paxful provided follow-up information to FinCEN throughout the course of negotiations on steps taken to remediate deficiencies identified during the Relevant Time Period.

9. **Systemic Nature of the Violations. Considerations include, but are not limited to, the number and extent of violations, failure rates (e.g., the number of violations out of total number of transactions), and duration of violations**: Paxful did not develop, implement, and maintain an effective AML program reasonably designed to prevent its platform from processing illicit activity. Although the Company registered as an MSB with FinCEN in 2015, it failed to implement even basic steps to comply with its AML regulations until 2019. The violations at issue continued to persist over an extended period and involved multiple products and services, rather than a specific business unit or customer group. The Company's compliance failures and shortcomings were structural in nature, and various personnel demonstrated actual knowledge of such issues, yet Paxful failed to remedy these deficiencies for many years.

10. **Whether another agency took enforcement action for related activity. FinCEN will consider the amount of any fine, penalty, forfeiture, and/or remedial action ordered**: Following a separate but parallel investigation, Paxful has agreed to pay $4 million to the DOJ.

V. CIVIL PENALTY

A. Legal Background

FinCEN may impose a Civil Money Penalty of $5,000 per day for willful violations of the requirement to register as an MSB occurring on or before November 2, 2015, and $10,556 per day for violations occurring after that date.[43]

FinCEN may impose a Civil Money Penalty of $25,000 per day for willful violations of the requirement to implement and maintain an effective AML program occurring on or before November 2, 2015, and $71,545 per day for violations occurring after that date.[44]

[43] 31 U.S.C. § 5330(e); 31 C.F.R. § 1010.821.
[44] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.821.

For each willful violation of a SAR reporting requirement, FinCEN may impose a Civil Money Penalty not to exceed the greater of the amount involved in the transaction (originally capped at $100,000) or $25,000. The former limit increased to $286,184, while the latter increased to $71,545, for violations occurring after November 2, 2015.[45]

B. Civil Penalty Determination

After considering all the facts and circumstances, as well as the enforcement factors discussed above, FinCEN has determined to impose a Civil Money Penalty of $3.5 million in this matter. FinCEN has agreed to credit against the $3.5 million Civil Penalty payment of $1.75 million to the DOJ. Accordingly, Paxful shall make a payment for the Civil Money Penalty of $1.75 million to the U.S. Department of the Treasury pursuant to the payment instructions that will be transmitted to Paxful upon execution of this Consent Order.

VI. CONSENT AND ADMISSIONS

To resolve this matter and only for that purpose, Paxful admits to the Statement of Facts and Violations set forth in this Consent Order and admits that it willfully violated the BSA and its implementing regulations. Paxful consents to the use of the Statement of Facts, and any other findings, determinations, and conclusions of law set forth in this Consent Order in any other proceeding brought by or on behalf of FinCEN, or to which FinCEN is a party or claimant, and agrees they shall be taken as true and correct and be given preclusive effect without any further proof. Paxful understands and agrees that in any administrative or judicial proceeding brought by or on behalf of FinCEN against it, including any proceeding to enforce the Civil Money Penalty imposed by this Consent Order or for any equitable remedies under the BSA, Paxful shall be precluded from disputing any fact or contesting any determinations set forth in this Consent Order.

[45] 31 U.S.C. § 5321(a)(1).

To resolve this matter, Paxful agrees to and consents to the issuance of this Consent Order and all terms herein and agrees to make a payment of $1.75 million pursuant to the payment instructions that will be transmitted to Paxful upon execution of this Consent Order. If timely payment is not made, Paxful agrees that interest, penalties, and administrative costs will accrue.[46]

Paxful understands and agrees that it must treat the Civil Money Penalty paid under this Consent Order as a penalty paid to the government and may not claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any payments made to satisfy the Civil Money Penalty. Paxful understands and agrees that any acceptance by or on behalf of FinCEN of any partial payment of the Civil Money Penalty obligation will not be deemed a waiver of Paxful's obligation to make further payments pursuant to this Consent Order, or a waiver of FinCEN's right to seek to compel payment of any amount assessed under the terms of this Consent Order, including any applicable interest, penalties, or other administrative costs.

Paxful affirms that it agrees to and approves this Consent Order and all terms herein freely and voluntarily and that no offers, promises, or inducements of any nature whatsoever have been made by FinCEN or any employee, agent, or representative of FinCEN to induce Paxful to agree to or approve this Consent Order, except as specified in this Consent Order.

Paxful understands and agrees that this Consent Order implements and embodies the entire agreement between Paxful and FinCEN, and its terms relate only to this enforcement matter and any related proceeding and the facts and determinations contained herein. Paxful further understands and agrees that there are no express or implied promises, representations, or agreements between Paxful and FinCEN other than those expressly set forth or referred to in this Consent Order and that nothing

[46] 31 U.S.C. § 3717; 31 C.F.R. § 901.9.

in this Consent Order is binding on any other law enforcement or regulatory agency or any other governmental authority, whether foreign, Federal, State, or local.

Paxful understands and agrees that nothing in this Consent Order may be construed as allowing Paxful, its subsidiaries, affiliates, Board, officers, employees, or agents to violate any law, rule, or regulation.

Paxful consents to the continued jurisdiction of the courts of the United States over it and waives any defense based on lack of personal jurisdiction or improper venue in any action to enforce the terms and conditions of this Consent Order or for any other purpose relevant to this enforcement action. Solely in connection with an action filed by or on behalf of FinCEN to enforce this Consent Order or for any other purpose relevant to this action, Paxful authorizes and agrees to accept all service of process and filings through the Notification procedures below and to waive formal service of process.

VII. COOPERATION

Paxful shall fully cooperate with FinCEN in any and all matters within the scope of or related to the Statement of Facts, including any investigation of its current or former directors, officers, employees, agents, consultants, or any other party. Paxful understands that its cooperation pursuant to this paragraph shall include, but is not limited to, truthfully disclosing all factual information with respect to its activities, and those of its present and former directors, officers, employees, agents, and consultants. This obligation includes providing to FinCEN, upon request, any document, record or other tangible evidence about which FinCEN may inquire of Paxful. Paxful's cooperation pursuant to this paragraph is subject to applicable laws and regulations, as well as valid and properly documented claims of attorney-client privilege or the attorney work product doctrine.

VIII. RELEASE

Execution of this Consent Order, and compliance with all of the terms of this Consent Order, settles all claims that FinCEN may have against Paxful for the conduct described in this Consent Order during the Relevant Time Period. Execution of this Consent Order, and compliance with the terms of this Consent Order, does not release any claim that FinCEN may have for conduct by Paxful other than the conduct described in this Consent Order during the Relevant Time Period, or any claim that FinCEN may have against any current or former director, officer, owner, or employee of Paxful, or any other individual or entity other than those named in this Consent Order. In addition, this Consent Order does not release any claim or provide any other protection in any investigation, enforcement action, penalty assessment, or injunction relating to any conduct that occurs after the Relevant Time Period as described in this Consent Order.

IX. WAIVERS

Nothing in this Consent Order shall preclude any proceedings brought by, or on behalf of, FinCEN to enforce the terms of this Consent Order, nor shall it constitute a waiver of any right, power, or authority of any other representative of the United States or agencies thereof, including but not limited to the Department of Justice.

In consenting to and approving this Consent Order, Paxful stipulates to the terms of this Consent Order and waives:

A. Any and all defenses to this Consent Order, the Civil Money Penalty imposed by this Consent Order, and any action taken by or on behalf of FinCEN that can be waived, including any statute of limitations or other defense based on the passage of time;

B. Any and all claims that FinCEN lacks jurisdiction over all matters set forth in this Consent Order, lacks the authority to issue this Consent Order or to impose the Civil Money Penalty, or lacks authority for any other action or proceeding related to the matters set forth in this Consent Order;

C. Any and all claims that this Consent Order, any term of this Consent Order, the Civil Money Penalty, or compliance with this Consent Order, or the Civil Money Penalty, is in any way unlawful or violates the Constitution of the United States of America or any provision thereof;

D. Any and all rights to judicial review, appeal or reconsideration, or to seek in any way to contest the validity of this Consent Order, any term of this Consent Order, or the Civil Money Penalty arising from this Consent Order;

E. Any and all claims that this Consent Order does not have full force and effect, or cannot be enforced in any proceeding, due to changed circumstances, including any change in law;

F. Any and all claims for fees, costs, or expenses related in any way to this enforcement matter, Consent Order, or any related administative action, whether arising under common law or under the terms of any statute, including, but not limited to, under the Equal Access to Justice Act. Paxful agrees to bear its own costs and attorneys' fees.

X. VIOLATIONS OF THIS CONSENT ORDER

Determination of whether Paxful has failed to comply with this Consent Order, or any portion thereof, and whether to pursue any further action or relief against Paxful shall be in FinCEN's sole discretion. If FinCEN determines, in its sole discretion, that a failure to comply with this Consent

Order, or any portion thereof, has occurred, or that Paxful has made any misrepresentations to FinCEN or any other government agency related to the underlying enforcement matter, FinCEN may void any and all releases or waivers contained in this Consent Order; reinstitute administrative proceedings; take any additional action that it deems appropriate; and pursue any and all violations, maximum penalties, injunctive relief, or other relief that FinCEN deems appropriate. FinCEN may take any such action even if it did not take such action against Paxful in this Consent Order and notwithstanding the releases and waivers herein. In the event FinCEN takes such action under this paragraph, Paxful specifically agrees to toll any applicable statute of limitations and to waive any defenses based on a statute of limitations or the passage of time that may be applicable to the Statement of Facts in this Consent Order, until a date 180 days following Paxful's receipt of notice of FinCEN's determination that a misrepresentation or breach of this agreement has occurred, except as to claims already time barred as of the Effective Date of this Consent Order.

In the event that FinCEN determines that Paxful has made a misrepresentation or failed to comply with this Consent Order, or any portion thereof, all statements made by or on behalf of Paxful to FinCEN, including the Statement of Facts, whether prior or subsequent to this Consent Order, will be admissible in evidence in any and all proceedings brought by or on behalf of FinCEN. Paxful agrees that it will not assert any claim under the Constitution of the United States of America, Rule 408 of the Federal Rules of Evidence, or any other law or federal rule that any such statements should be suppressed or are otherwise inadmissible. Such statements shall be treated as binding admissions, and Paxful agrees that it shall be precluded from disputing or contesting any such statements. FinCEN shall have sole discretion over the decision to impute conduct or statements of any director, officer, employee, agent, or any person or entity acting on behalf of, or at the direction of Paxful in determining whether Paxful has violated any provision of this Consent Order.

XI. PUBLIC STATEMENTS

Paxful agrees that it shall not, nor shall its attorneys, agents, partners, directors, officers, employees, affiliates, or any other person authorized to speak on its behalf or within its authority or control, take any action or make any public statement, directly or indirectly, contradicting its admissions and acceptance of responsibility or any terms of this Consent Order, including any fact finding, determination, or conclusion of law in this Consent Order.

FinCEN shall have sole discretion to determine whether any action or statement made by Paxful, or by any person under the authority, control, or speaking on behalf of Paxful contradicts this Consent Order, and whether Paxful has repudiated such statement.

XII. RECORD RETENTION

In addition to any other record retention required under applicable law, Paxful agrees to retain all documents and records required to be prepared or recorded under this Consent Order or otherwise necessary to demonstrate full compliance with each provision of this Consent Order, including supporting data and documentation. Paxful agrees to retain these records for a period of 6 years after creation of the record, unless required to retain them for a longer period of time under applicable law.

XIII. SEVERABILITY

Paxful agrees that if a court of competent jurisdiction considers any of the provisions of this Consent Order unenforceable, such unenforceability does not render the entire Consent Order unenforceable. Rather, the entire Consent Order will be construed as if not containing the particular unenforceable provision(s), and the rights and obligations of FinCEN and Paxful shall be construed and enforced accordingly.

XIV. SUCCESSORS AND ASSIGNS

Paxful agrees that the provisions of this Consent Order are binding on its owners, officers, employees, agents, representatives, affiliates, successors, assigns, and transferees to whom Paxful agrees to provide a copy of the executed Consent Order. Should Paxful seek to sell, merge, transfer, or assign its operations, or any portion thereof, that are the subject of this Consent Order, Paxful must, as a condition of sale, merger, transfer, or assignment obtain the written agreement of the buyer, merging entity, transferee, or assignee to comply with this Consent Order.

XV. MODIFICATIONS AND HEADINGS

This Consent Order can only be modified with the express written consent of FinCEN and Paxful. The headings in this Consent Order are inserted for convenience only and are not intended to affect the meaning or interpretation of this Consent Order or its individual terms.

XVI. AUTHORIZED REPRESENTATIVE

Paxful's representative, by consenting to and approving this Consent Order, hereby represents and warrants that the representative has full power and authority to consent to and approve this Consent Order for and on behalf of Paxful, and further represents and warrants that Paxful agrees to be bound by the terms and conditions of this Consent Order.

XVII. NOTIFICATION

Unless otherwise specified herein, whenever notifications, submissions, or communications are required by this Consent Order, they shall be made in writing and sent via first-class mail and simultaneous email, addressed as follows:

To FinCEN: Associate Director, Enforcement and Compliance Division, Financial Crimes Enforcement Network, P.O. Box 39, Vienna, Virginia 22183

To Paxful: Esseks Ingoglia, 350 Fifth Avenue, Suite 5200
New York, New York 10118

Notices submitted pursuant to this paragraph will be deemed effective upon receipt unless otherwise provided in this Consent Order or approved by FinCEN in writing.

XVIII. COUNTERPARTS

This Consent Order may be signed in counterpart and electronically. Each counterpart, when executed and delivered, shall be an original, and all of the counterparts together shall constitute one and the same fully executed instrument.

XIX. EFFECTIVE DATE AND CALCULATION OF TIME

This Consent Order shall be effective upon the date signed by FinCEN. Calculation of deadlines and other time limitations set forth herein shall run from the effective date (excluding the effective date in the calculation) and be based on calendar days, unless otherwise noted, including intermediate Saturdays, Sundays, and legal holidays.

By Order of the Director of the Financial Crimes Enforcement Network.

/s/
Andrea Gacki
Director

Date: December 9, 2025

Consented to and Approved By:

/s/
Roshan Dharia
Paxful, Inc.
Paxful USA, Inc.