

**DEPARTMENT OF THE TREASURY**

**Financial Crimes Enforcement Network**

**31 CFR Chapter X, Part 1010**

**RIN 1506-AB68**

**Proposal of Special Measure regarding Huione Group, as a Foreign Financial  
Institution of Primary Money Laundering Concern**

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

**ACTION:** Notice of proposed rulemaking.

**SUMMARY:** FinCEN is issuing a notice of proposed rulemaking (NPRM), pursuant to section 311 of the USA PATRIOT Act, that proposes prohibiting the opening or maintaining of a correspondent account in the United States for, or on behalf of, Huione Group, a foreign financial institution based in Cambodia found to be of primary money laundering concern. The NPRM also would require covered financial institutions to apply special due diligence to their foreign correspondent accounts that is reasonably designed to guard against their use to process transactions involving Huione Group.

**DATES:** Written comments on the notice of proposed rulemaking must be submitted on or before [30 DAYS AFTER THE DATE OF PUBLICATION OF THIS DOCUMENT IN THE FEDERAL REGISTER].

**ADDRESSES:** Comments must be submitted by one of the following methods:

- *Federal E-rulemaking Portal:* <https://www.regulations.gov>. Follow the instructions for submitting comments. Refer to Docket Number FINCEN–2025–0004 in the submission.
  - *Mail:* Financial Crimes Enforcement Network, P.O. Box 39, Vienna, VA 22183. Refer to Docket Number FINCEN–2025–0004 in the submission.
- Please submit comments by one method only and note that comments submitted in response to this NPRM will become a matter of public record.

**FOR FURTHER INFORMATION CONTACT:** The FinCEN Resource Center at [www.fincen.gov/contact](http://www.fincen.gov/contact).

**SUPPLEMENTARY INFORMATION:**

**I. Statutory Provisions**

Section 311 of the USA PATRIOT Act (section 311), codified at 31 U.S.C. 5318A, grants the Secretary of the Treasury (Secretary) the authority to make a finding that “reasonable grounds exist for concluding” that any of the following “is of primary money laundering concern:

- (i) A jurisdiction outside of the United States;
- (ii) One or more financial institutions operating outside of the United States;
- (iii) One or more classes of transactions within, or involving, a jurisdiction outside of the United States; or
- (iv) One or more types of accounts.<sup>1</sup>

---

<sup>1</sup> 31 U.S.C. 5318A(a)(1).

Upon making such a finding, the Secretary is authorized to require domestic financial institutions and domestic financial agencies to take certain “special measures.”<sup>2</sup> The five special measures set out in section 311 are safeguards that may be employed to defend the U.S. financial system from money laundering and terrorist financing risks. The Secretary may impose one or more of these special measures to protect the U.S. financial system from such threats. Through special measures one through four, the Secretary may impose additional recordkeeping, information collection, and reporting requirements on covered domestic financial institutions and domestic financial agencies—collectively, “covered financial institutions.”<sup>3</sup> Through special measure five, the Secretary may “prohibit, or impose conditions upon, the opening or maintaining in the United States of a correspondent account or payable-through account” for or on behalf of a foreign banking institution, if such correspondent account or payable-through account involves the foreign financial institution found to be of primary money laundering concern.<sup>4</sup>

Before making a finding that reasonable grounds exist for concluding that a financial institution outside of the United States (or other jurisdiction, account, or class of transactions) is of primary money laundering concern, the Secretary is required to consult with both the Secretary of State and the Attorney General.<sup>5</sup> In addition, in making a finding that reasonable grounds exist for concluding that a financial institution outside of

---

<sup>2</sup> On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56 (USA PATRIOT Act). Title III of the USA PATRIOT Act amended the anti-money laundering (AML) provisions of the Bank Secrecy Act (BSA) to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. The BSA, as amended, is the popular name for a collection of statutory authorities that FinCEN administers that is codified at 12 U.S.C. 1829b, 1951-1960 and 31 U.S.C. 5311-5314, 5316-5336, and includes other authorities reflected in notes thereto. Regulations implementing the BSA appear at 31 CFR Chapter X.

<sup>3</sup> 31 U.S.C. 5318A(b)(1)–(4). The term “covered financial institution” has the same meaning as provided at 31 C.F.R. 1010.605(e)(1); *see infra* section V.A.3.

<sup>4</sup> 31 U.S.C. 5318A(b)(5).

<sup>5</sup> 31 U.S.C. 5318A(c)(1).

the United States is of primary money laundering concern, the Secretary is required to consider such information as the Secretary determines to be relevant, including the following potentially relevant institutional factors:

- The extent to which such a financial institution is used to facilitate or promote money laundering in or through a jurisdiction outside the United States, including any money laundering activity by organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction (WMD) or missiles.
- The extent to which such a financial institution is used for legitimate business purposes in the jurisdiction; and
- The extent to which such action is sufficient to ensure, with respect to transactions involving the jurisdiction and institutions operating in the jurisdiction, that the purposes of section 311 continue to be fulfilled, and to guard against international money laundering and other financial crimes.<sup>6</sup>

In selecting one or more special measures, the Secretary “shall consult with the Chairman of the Board of Governors of the Federal Reserve System, any other appropriate Federal banking agency (as defined in section 3 of the Federal Deposit Insurance Act), the Secretary of State, the Securities and Exchange Commission, the Commodity Futures Trading Commission, the National Credit Union Administration Board, and in the sole discretion of the Secretary, such other agencies and interested parties as the Secretary may find appropriate.”<sup>7</sup> When imposing special measure five, the

---

<sup>6</sup> 31 U.S.C. 5318A(c)(2)(B)(i)-(iii). In addition, in the case of a finding relating to a particular jurisdiction, section 311 sets out certain “jurisdictional factors” that the Secretary may consider, which are not relevant here. *See* 31 U.S.C. 5318A(c)(2)(A)(i)-(vii).

<sup>7</sup> 31 U.S.C. 5318A(a)(4)(A).

Secretary must do so “in consultation with the Secretary of State, the Attorney General, and the Chairman of the Board of Governors of the Federal Reserve System.”<sup>8</sup> In addition, the Secretary is required to consider the following factors:

- Whether similar action has been or is being taken by other nations or multilateral groups;
- 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;
- The extent to which the action or the timing of the action would have a significant adverse systemic impact on the international payment, clearance, and settlement system, or on legitimate business activities involving the particular jurisdiction, institution, class of transactions, or type of account; and
- The effect of the action on United States national security and foreign policy.<sup>9</sup>

The authority of the Secretary to administer the Bank Secrecy Act (BSA) and its implementing regulations, including the authority under section 311 to make such a finding and to impose special measures, has been delegated to FinCEN.<sup>10</sup>

## **II. Summary of NPRM**

Huione Group<sup>11</sup> is a financial services conglomerate based in Phnom Penh,

---

<sup>8</sup> 31 U.S.C. 5318A(b)(5).

<sup>9</sup> 31 U.S.C. 5318A(a)(4)(B)(i)-(iv).

<sup>10</sup> Pursuant to Treasury Order 180-01 (Jan. 14, 2020), the authority of the Secretary to administer the BSA, including, but not limited to, 31 U.S.C. 5318A, has been delegated to the Director of FinCEN.

<sup>11</sup> As will be discussed in greater detail in section III, Huione Group is the parent company of the following subsidiaries: Huione Crypto, Haowang Guarantee, and Huione Pay PLC. FinCEN assesses that this collective grouping of exchange services is a single organization, and for that reason, FinCEN will correspondingly refer to this collective as the Huione Group.

Cambodia.<sup>12</sup> Huione Group’s website is registered<sup>13</sup> to an individual with a listed location of Phnom Penh, Cambodia, but Huione Group, the parent entity of the conglomerate, does not appear to be registered as a business in any jurisdiction, though it was originally incorporated in Hong Kong in 2018 as Huione Group Limited.<sup>14</sup> While several of Huione Group’s subsidiaries are registered outside of Cambodia, their operations are principally carried out in Cambodia.

For years, Huione Group has laundered illicit proceeds from cybercrimes—namely, cyber heists carried out by the Lazarus Group,<sup>15</sup> an entity sanctioned by Treasury’s Office of Foreign Assets Control (OFAC)—and Convertible Virtual Currency (CVC) investment scams carried out by transnational criminal organizations (TCOs) based in Southeast Asia.<sup>16</sup>

Since its establishment, Huione Group has set up a network of businesses, each playing a different role in its money laundering enterprise. However, FinCEN’s analysis

---

<sup>12</sup> Cambodia Corporate Registry, *Huione Search*, <https://www.businessregistration.moc.gov.kh/cambodia-master/service/create.html?targetAppCode=cambodia-master&targetRegisterAppCode=cambodia-br-companies&service=registerItemSearch> (last accessed Mar. 27, 2025); Huione Pay, *Index*, <https://www.huionepay.com.kh/index/help>; Huione Group, *About*, which is no longer accessible and will be discussed later in this section, *formerly available at* <https://huione.com/html/about.jsp> (last accessed Sept. 24, 2024). Huione Crypto has numerous job announcements with a work location in Phnom Penh, Cambodia. *See* Huione Crypto, *Career Opportunities*, <https://www.huione.io/en-US/careerOpportunities> (last accessed Mar. 27, 2025). Haowang Guarantee also lists job announcements with a work location in Phnom Penh, Cambodia. *See* Haowang Guarantee, *About*, <https://www.hwdb.la/about/> (last accessed Mar. 27, 2025).

<sup>13</sup> The registration is valid through June 3, 2025. *See* ICANN, *Huione.com*, <https://lookup.icann.org/en/huione.com> (last accessed Mar. 27, 2025).

<sup>14</sup> Hong Kong Companies Registry, *Huione Group Limited*, at p. 54, [https://www.cr.gov.hk/docs/wrpt/RNC063\\_2018.12.17-2018.12.23.pdf](https://www.cr.gov.hk/docs/wrpt/RNC063_2018.12.17-2018.12.23.pdf).

<sup>15</sup> The Lazarus Group is an agency, instrumentality, or controlled entity of the government of the Democratic People’s Republic of Korea, that has stolen large volumes of Convertible Virtual Currency in numerous and often widely reported cyber heists. On September 13, 2019, the Lazarus Group was sanctioned by OFAC. *See* Department of the Treasury, Press Release, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, (Sept. 13, 2019), <https://home.treasury.gov/news/press-releases/sm774>.

<sup>16</sup> These scams are also referred to as “pig butchering.” *See* FinCEN, FIN-2023-Alert005, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”* (Sept. 8, 2023), [https://www.fincen.gov/sites/default/files/shared/FinCEN\\_Alert\\_Pig\\_Butchering\\_FINAL\\_508c.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

of Huione Group has identified the sharing of CVC infrastructure by Huione Group's constituent entities, indicating that the entities, including the parent Huione Group, are functionally operating as one and the same, despite the various branding. Because Huione Group's subsidiaries have shared CVC infrastructure with its constituent entities, the structure makes it challenging to ascertain the specific subsidiary involved in any particular transaction.

The overall Huione Group network offers unique services ranging from an online marketplace selling items useful for carrying out cyber scams to money laundering services that accept both fiat currencies and CVC. Huione Group has also created its own stablecoin, a type of CVC that is usually backed by a pre-determined quantity of fiat currency, most often the U.S. dollar (USD). The stablecoin, "USDH," which is a ticker symbol for "U.S. Dollar Huione," is pegged to the USD at a one-to-one ratio and is represented as a stablecoin that cannot be frozen. In contrast, many stablecoin issuers develop their stablecoins to retain the ability to freeze funds, which they have sometimes done in cases of known criminal activity, or at the request of law enforcement. Because Huione Group claims that USDH cannot be frozen, this service offers Huione Group's clientele a virtually risk-free ecosystem to move or store CVC without the risk of interception or "freezing" by law enforcement.

Finally, much of the illicit revenue laundered through Huione Group originates from well-documented criminal activity, and numerous publicly available reports describe the failings of Huione Group's anti-money laundering/know your customer (AML/KYC) program. Despite these reports and Huione Group's public

acknowledgments of its failings,<sup>17</sup> FinCEN assesses that Huione Group has made no meaningful steps to effectively address these AML/KYC deficiencies.

This NPRM (1) sets forth FinCEN’s finding, based on public and non-public information, that Huione Group is a financial institution operating outside of the United States of primary money laundering concern; and (2) proposes that, under special measure five, covered financial institutions be prohibited from opening or maintaining a correspondent account for, or on behalf of, Huione Group.

### **III. Finding that Huione Group is a Financial Institution Operating Outside of the United States and a Foreign Financial Institution**

As set forth above, section 311 authorizes FinCEN, through delegated authority and in pertinent part, to make a 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.”<sup>18</sup> A prerequisite to such a finding is that the relevant institution is a “financial institution operating outside of the United States.”<sup>19</sup>

---

<sup>17</sup> Following negative public reporting about Huione Group in July 2024, Huione Group provided a statement to ABC News, stating that “...because our [Huione Group’s] services are all public, covering Asia, Europe and America, and the privacy attributes of [CVC] are superimposed, our KYC [know your customer] capabilities are now seriously insufficient.” See ABC News, *Cambodian online marketplace outed as one-stop shop for scammers’ money laundering and ‘detention equipment’ needs* (July 26, 2024), <https://www.abc.net.au/news/2024-07-27/online-marketplace-for-money-laundering-and-scammers/104131624>; see also The Record, *Tether freezes \$29 million of cryptocurrency connected to Cambodian marketplace accused of fueling scams* (July 15, 2024), <https://therecord.media/tether-freezes-29-million-crypto-connected-to-scam-marketplace>; Elliptic, *Huione Guarantee: The multi-billion dollar marketplace used by online scammers* (July 9, 2024, updated Mar. 27, 2025), <https://www.elliptic.co/blog/cyber-scam-marketplace>; Elliptic, *Huione: The Company Behind the Largest Ever Illicit Online Marketplace Has Launched a Stablecoin* (Jan. 14, 2025), <https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin>; Chainalysis, *2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks on the Rise, Pig Butchering Scams Remain Lucrative* (Aug. 29, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/>.

<sup>18</sup> 31 U.S.C. 5318A(a)(1).

<sup>19</sup> 31 U.S.C. 5318A(a)(1) authorizes the imposition of special measures on, among others, “financial institutions operating outside of the United States.” Of the five special measures authorized by the statute, the fifth measure authorizes “Prohibitions or Conditions on Opening or Maintaining Certain Correspondent or Payable-Through Accounts.” The statute goes on to define the terms correspondent account and payable-through account in reference to payments made on behalf of a “foreign financial institution” – a



The BSA defines a “financial institution” to be any of several categories of entities, including money transmitters.<sup>20</sup> The BSA defines a money transmitter as including “a licensed sender of money or any other person who engages as a business in the transmission of currency funds, or value that substitutes for currency.”<sup>21</sup> A money transmitter does not require a particular license, corporate structure, or physical location.

As detailed further below, much of Huione Group’s illicit money transmitting activity occurs through transactions in CVC. This is consistent with the money transmitter definition, which includes services in CVC. FinCEN’s May 9, 2019, Guidance on CVC explains that for the purposes of the BSA’s implementing regulations, persons “may be a money transmitter ... regardless of the technology employed for the transmittal of value or the type of asset the person uses as value that substitutes for currency, or whether such asset is physical or virtual.”<sup>22</sup> For the reasons explained in the May 9, 2019, Guidance, the term “value that substitutes for currency” includes CVC.<sup>23</sup>

***A. Huione Group and its Three Identified Subsidiaries are Each a Financial Institution***

Huione Group is a parent entity that controls three subsidiaries: (i) Haowang Guarantee; (ii) Huione Pay PLC; and (iii) Huione Crypto (collectively, the “Subsidiaries”). Based on the following, FinCEN finds that reasonable grounds exist to

---

term otherwise undefined. For the purposes of this NPRM, and under these facts, FinCEN finds that Huione Group is both a foreign financial institution and a financial institution outside of the United States.

<sup>20</sup> See 31 U.S.C. 5312(a)(2).

<sup>21</sup> 31 U.S.C. 5312(a)(2)(R) (allowing “a licensed sender of money or any other person...” to constitute money transmitter). FinCEN’s implementing regulations define “person” broadly as “an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities.” 31 CFR § 1010.100(mm).

<sup>22</sup> FinCEN, FIN-2019-G001, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), at Section 1.2.3, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

<sup>23</sup> *Id.* at Sections 1.2.1, 1.3.

conclude that Huione Group and each of the Subsidiaries engages in the business of money transmission, and is thereby a financial institution under the BSA and its implementing regulations.

### 1. *Huione Group*

Huione Group is a Cambodia based, Hong Kong-registered<sup>24</sup> sole proprietorship founded in or around 2014, appears to be owned and controlled by an individual Cambodian national,<sup>25</sup> and holds itself out as the parent entity of the Subsidiaries.<sup>26</sup> By its own account, Huione Group began as a fiat currency exchange service and over the past decade, expanded its commercial interests to include finance, insurance, real estate entities,<sup>27</sup> and most recently, CVC exchange services.<sup>28</sup> The Subsidiaries operate an interconnected payment service provider, illicit online market, and a CVC exchanger (a type of virtual asset service provider or VASP).

Huione Group, as an individual entity, coordinates the Subsidiaries' activities by operating the customer service and public relations functions of the Huione Group.

---

<sup>24</sup> Hong Kong Companies Registry, *Huione Group Limited*, at p. 54, [https://www.cr.gov.hk/docs/wrpt/RNC063\\_2018.12.17-2018.12.23.pdf](https://www.cr.gov.hk/docs/wrpt/RNC063_2018.12.17-2018.12.23.pdf).

<sup>25</sup> See The Record, *Tether freezes \$29 million of cryptocurrency connected to Cambodian marketplace accused of fueling scams* (July 15, 2024), <https://therecord.media/tether-freezes-29-million-crypto-connected-to-scam-marketplace>.

<sup>26</sup> See, e.g., Elliptic, *Huione: The Company Behind the Largest Ever Illicit Online Marketplace Has Launched a Stablecoin* (Jan. 14, 2025), <https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin>; Elliptic, *Huione Guarantee: The multi-billion dollar marketplace used by online scammers* (July 9, 2024, updated Mar. 27, 2025), <https://www.elliptic.co/blog/cyber-scam-marketplace>; Chainalysis, *2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks on the Rise, Pig Butchering Scams Remain Lucrative* (Aug. 29, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/>; ABC News, *Cambodian online marketplace outed as one-stop shop for scammers' money laundering and 'detention equipment' needs* (July 26, 2024), <https://www.abc.net.au/news/2024-07-27/online-marketplace-for-money-laundering-and-scammers/104131624>; Huione Crypto, *Terms and Conditions*, <https://www.huione.io/en-US/termsAndConditions/userAgreement> (last accessed Mar. 27, 2025). The Huione Group website is no longer accessible, which FinCEN assesses is more likely than not caused by negative public attention following a series of reports by blockchain analytic firms on money laundering occurring at Huione Group.

<sup>27</sup> Huione Group, *Who We Are*, formerly available at <https://www.huione.com/html/about.jsp> (last accessed Sept. 24, 2024).

<sup>28</sup> Huione Crypto, *Introduce*, <https://www.huione.io/en-US/introduce> (last accessed Mar. 26, 2025).

Huione Group does this by hosting Telegram channels to aid customers experiencing problems with the services that the Subsidiaries provide.<sup>29</sup> One of Huione Group's Telegram channels also provides public relations commentary on behalf of the whole of the Huione Group collective. Most recently, that public relations channel responded to counter news media reports that the Cambodian government revoked Huione Pay PLC's banking license.<sup>30</sup> Lastly, Huione Group's Subsidiaries all have shared CVC infrastructure, making it challenging to ascertain the specific subsidiary involved in a particular transaction.

FinCEN finds that reasonable grounds exist to conclude that Huione Group is a money transmitter. By providing customer service and public relations services on behalf of the Subsidiaries, Huione Group is itself part of “a network of people who engage as a business in facilitating the transfer of money.” Furthermore, through Huione Group's apparent control of the Subsidiaries (each of which is itself a money transmitter, and through Huione Group's coordination of the Subsidiaries' business activities such that they form a self-contained ecosystem of exchange, payment, and market services), Huione Group is engaged as a business in the transmission of value that substitutes for currency. Accordingly, FinCEN finds that reasonable grounds exist to conclude that Huione Group is a financial institution as defined by the BSA and as that term is used in section 311.

---

<sup>29</sup> Telegram, *Huione Group Customer Service Center*, <https://t.me/huionekf/138> (last accessed Mar. 27, 2025).

<sup>30</sup> Telegram, *Huione Group Customer Service, Huione Statement* (Mar. 9, 2025), <https://t.me/huionekf/346>.

2. *Haowang Guarantee (formerly known as Huione Guarantee)*<sup>31</sup>

Haowang Guarantee describes itself as “a professional e-commerce platform that provides users with virtual digital products and transaction services...[that] does not participate in nor understand the specific business of the customer.... Huione cannot verify or guarantee the process of funds or goods.”<sup>32</sup> Multiple blockchain analytic firms have analyzed and reported on Haowang Guarantee for facilitating the sale of contraband and illicit services. For example, a public report issued by blockchain analytics company Elliptic found that Haowang Guarantee appears to operate in a manner similar to a darknet market.<sup>33</sup> This assessment is based on the fact that Haowang Guarantee offers a marketplace where third party merchants can sell goods and services, including money laundering services and equipment that can be used to detain people, which could be used for illicit purposes such as enabling human trafficking.<sup>34</sup> While FinCEN does not have evidence that Haowang Guarantee operates on the darknet, FinCEN assesses that Haowang Guarantee deals in the sale of illicit goods and services in a manner similar to a darknet market but on the open internet.<sup>35</sup>

Chainalysis, a separate blockchain analytics company, found similar results. In its

---

<sup>31</sup> On October 19, 2024, Huione Guarantee was rebranded as Haowang Guarantee, announcing the change on September 30, 2024, and offering customer discount following the rebrand to thank their long-term customers. The reason for such a rebrand is unclear, although it could be to distance itself from the recent negative public reporting about Huione Group. Telegram, *Haowang Guarantee Customer Service Channel* (Sept. 30, 2024), <https://t.me/s/kefu> (last accessed Mar. 27, 2025).

<sup>32</sup> Haowang Guarantee, *About*, <https://www.hwbd.la/about> (last accessed Mar. 27, 2025).

<sup>33</sup> Darknet Markets almost exclusively accept CVC as payment for a large range of illegal services and goods, including ransomware-as-a-service (RaaS). CVC is often the payment method of choice on darknet marketplaces because illicit actors who transact on the darknet often incorrectly believe virtual currencies to be an anonymous and untraceable means of exchange.

<sup>34</sup> Elliptic, *Huione Guarantee: The multi-billion dollar marketplace used by online scammers* (July 9, 2024, updated Mar. 27, 2025), <https://www.elliptic.co/blog/cyber-scam-marketplace>.

<sup>35</sup> See Department of the Treasury, Press Release, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (Apr. 5, 2022), <https://home.treasury.gov/news/press-releases/jy0701>.

2024 Crypto Crime Mid-year Update Report, it determined that Haowang Guarantee operates as a peer-to-peer marketplace that connects buyers and sellers and facilitates transactions.<sup>36</sup> Chainalysis reviewed blockchain data of Haowang Guarantee and determined it had processed at least USD 49 billion worth of CVC since 2021. Chainalysis also determined that merchants operating on Haowang Guarantee’s marketplace offered various illicit services, including the technology, infrastructure and resources to conduct cyber scams.<sup>37</sup>

In addition, Elliptic reports that Haowang Guarantee provides money laundering services to criminal organizations, helping them transfer the proceeds of investment frauds and other cyber scams to the legitimate banking sector undetected.<sup>38</sup> Because Haowang Guarantee offers “virtual digital products and transaction services” and facilitates CVC (digital asset) transactions, FinCEN finds that there are reasonable grounds to conclude that it is engaged as a business in the transmission of value that substitutes for currency. Accordingly, FinCEN finds that reasonable grounds exist to conclude that Haowang Guarantee is a financial institution as that term is used in the BSA and section 311.

### 3. *Huione Pay PLC*

As of January 2025, Huione Pay PLC was registered as a payment services institution with the National Bank of Cambodia.<sup>39</sup> Until December 2023, there was a

---

<sup>36</sup> Chainalysis, *2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks on the Rise, Pig Butchering Scams Remain Lucrative* (Aug. 29, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/>.

<sup>37</sup> *Id.*

<sup>38</sup> Elliptic, *Huione: The Company Behind the Largest Ever Illicit Online Marketplace Has Launched a Stablecoin* (Jan. 14, 2025), <https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin>.

<sup>39</sup> National Bank of Cambodia, *List of Payment Service Institutions* (Dec. 31, 2024), [https://www.nbc.gov.kh/download\\_files/data/english/En/EN-PSIs.pdf](https://www.nbc.gov.kh/download_files/data/english/En/EN-PSIs.pdf) (last accessed Mar. 21, 2025).

likely related entity, “Huione Pay,” registered as a money services business in Canada, which was incorporated in the country as Huione Pay Inc.<sup>40</sup> In March 2025, Huione Group advertised its plans to expand Huione Pay PLC into new markets, including in North America.<sup>41</sup>

Huione Pay PLC offers its customers the ability to trade CVC on different blockchains, and to convert CVC to or from various fiat currencies.<sup>42</sup> Huione Pay PLC is registered with the Cambodian Ministry of Commerce for “other financial service activities.”<sup>43</sup> Part of Huione Pay PLC, Huione International Payments, acts as a merchant on Haowang Guarantee’s platform and exchanging CVC to facilitate the transfer of the proceeds of cyber scams.<sup>44</sup> Huione Pay PLC holds the local equivalent of a money transmitting business license issued by the Kingdom of Cambodia and engages in the exchange of CVC in a manner consistent with the definition of a money transmitting business. Accordingly, FinCEN finds that reasonable grounds exist to conclude that

---

<sup>40</sup> Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Money Services Business Registry, *Huione Pay Inc.*, <https://fintrac-canafe.canada.ca/msb-esm/reg-eng> (last accessed Mar. 13, 2025).

<sup>41</sup> Telegram, *Huione Group Customer Service, Huione Statement* (Mar. 9, 2025), <https://t.me/huionekf/346>.

<sup>42</sup> Huione Pay website, *Index*, <https://www.huionepay.com.kh/index/help> (last accessed Mar. 27, 2025).

<sup>43</sup> See Cambodia Corporate Registry, *Huione Search*, <https://www.businessregistration.moc.gov.kh/cambodia-master/service/create.html?targetAppCode=cambodia-master&targetRegisterAppCode=cambodia-br-companies&service=registerItemSearch> (last accessed Mar. 27, 2025). On March 6, 2025, a media report indicated that Huione Pay PLC’s banking license was revoked by the Cambodian government. See Radio Free Asia, *Exclusive: World’s Largest online black market’ Loses banking license* (Mar. 6, 2025), <https://www.rfa.org/english/cambodia/2025/03/06/huione-cambodia-cyberscam-cryptocurrency/>. Huione Group responded to the allegations, refuting them by noting that Huione Pay PLC does not require a banking license for its operations. Telegram, *Huione Group Customer Service, Huione Statement* (Mar. 9, 2025), <https://t.me/huionekf/346>. However, as of March 10, 2025, Huione Pay PLC is still listed as having an active license for “other financial services activities.” See Cambodia Corporate Registry, *Huione Search*, <https://www.businessregistration.moc.gov.kh/cambodia-master/service/create.html?targetAppCode=cambodia-master&targetRegisterAppCode=cambodia-br-companies&service=registerItemSearch> (last accessed Mar. 27, 2025).

<sup>44</sup> FinCEN assesses that Huione International Payments is part of Huione Pay PLC and that the entity supports Haowang Guarantee’s facilitation of transactions connected to money laundering activities. See Elliptic, *Huione Guarantee: The multi-billion dollar marketplace used by online scammers* (July 9, 2024, updated Mar. 27, 2025), <https://www.elliptic.co/blog/cyber-scam-marketplace>; The New York Times, *How Scammers Launder Money and Get Away With It* (Mar. 23, 2025), <https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html>.

Huione Pay PLC is a financial institution as that term is used in the BSA and section 311.

#### 4. *Huione Crypto*

Huione Crypto provides CVC trading services through its “Huione Exchange” brand, which it owns and operates. Huione Exchange provides a platform for its customers to trade CVC using either its “peer to peer” or “centrali[z]ed exchange platform.”<sup>45</sup> In other words, Huione Crypto is a VASP operating under the Huione Group umbrella, and other Huione Group entities use Huione Crypto’s infrastructure to engage in CVC transactions. Separately, Huione Crypto issues the USDH stablecoin.<sup>46</sup> By facilitating CVC value exchanges for its customers through its trading platform, and by issuing a stablecoin that facilitates the transfer of money outside the conventional financial institution systems, Huione Crypto is engaged in money transmission as described at 31 U.S.C. 5312(R). Accordingly, FinCEN finds that reasonable grounds exist to conclude that Huione Crypto is a financial institution as that term is used in the BSA and section 311.

### ***B. Huione Group Operates Outside the United States***

#### 1. *Huione Group*

Based on publicly available information, Huione Group is operated by a Cambodian person, from Phnom Penh, Cambodia.<sup>47</sup> Furthermore, the Huione Group website is registered to a Cambodian address in Phnom Penh, uses a Cambodian Top-

---

<sup>45</sup> Huione Crypto, *Legal*, <https://www.huione.io/en-US/termsAndConditions/userAgreement> (last accessed Mar. 27, 2025).

<sup>46</sup> See *supra* Section II.

<sup>47</sup> The Record, *Tether freezes \$29 million of cryptocurrency connected to Cambodian marketplace accused of fueling scams* (July 15, 2024), <https://therecord.media/tether-freezes-29-million-crypto-connected-to-scam-marketplace>; see also ICANN, *Huione.com*, <https://lookup.icann.org/en/huione.com>; Elliptic, *Huione Guarantee: The multi-billion dollar marketplace used by online scammers* (July 9, 2024, updated Mar. 27, 2025), <https://www.elliptic.co/blog/cyber-scam-marketplace>.

Level Domain, and communicates predominately in the Chinese language via a Cambodian website and Telegram Channel operated from Cambodia. Accordingly, FinCEN finds that reasonable grounds exist to conclude that Huione Group is operated from and located in Cambodia and thus operates outside of the United States.

## *2. Haowang Guarantee (Formerly Huione Guarantee)*

Haowang Guarantee operates Telegram-based marketplace that allows its customers to buy and sell goods and services, relying on other Huione Group services and infrastructure to execute the exchanges. Haowang Guarantee appears to serve, in significant part, fraudsters based in Southeast Asia. FinCEN assesses that Haowang Guarantee deliberately obfuscates its location in order to shield its enterprise and customers from law enforcement. Haowang Guarantee is integrated into Huione Group's operations and is apparently subject to Huione Group's control. FinCEN assesses that it is operated from Cambodia and Haowang Guarantee advertises job opportunities based in Phnom Penh, Cambodia. Accordingly, FinCEN finds that reasonable grounds exist to conclude that Haowang Guarantee is operated from and located in Cambodia and thus operates outside of the United States.

## *3. Huione Pay PLC*

Huione Pay PLC operates eight Cambodian domestic branch locations, located in Battambang, Phnom Penh, Poipet, Siem Reap, and Sihanoukville.<sup>48</sup> Huione Pay PLC also advertises on social media that it has operated a branch in Laukkaing,<sup>49</sup> the capital of the Kokang Self-Administered Zone in northern Burma and a known center for criminal

---

<sup>48</sup> Telegram, *Huione Branch*, <https://t.me/huionestoreaddress/7> (last accessed Mar. 27, 2025).

<sup>49</sup> Telegram, *Huione Group Customer Service Center*, <https://t.me/huionekf/138> (last accessed Mar. 27, 2025).



CVC investment scams, before a 2023-2024 crackdown shuttered the majority of these operations.<sup>50</sup> Huione Pay PLC is registered as a payment services institution with the National Bank of Cambodia.<sup>51</sup> Based on the foregoing, FinCEN finds that reasonable grounds exist to conclude that Huione Pay PLC is operated from and located in Cambodia and thus operates outside of the United States.

#### 4. *Huione Crypto*

Huione Crypto, under the name Huione Crypto Spółka Z Ograniczoną Odpowiedzialnością, is registered in Poland.<sup>52</sup> Despite its Polish registration, however, FinCEN assesses that Huione Crypto operates in and from Cambodia.<sup>53</sup> Huione Crypto is registered as a Money Services Business (MSB)<sup>54</sup> with FinCEN; however, FinCEN has found no evidence consistent with activity in the United States by this entity. FinCEN assesses that the “Group” referenced in Huione Crypto’s *Standard Terms and Conditions* refers to Huione Group, and that Huione Crypto’s CVC services share infrastructure with Huione Pay PLC and Haowang Guarantee, and collectively comprise a single organization.

Regardless of this distinction, FinCEN will discuss Huione Crypto as a related, but distinct subsidiary of Huione Group. Huione Crypto advertises jobs in Phnom Penh,

---

<sup>50</sup> Recorded Future, *Myanmar rebels take control of ‘pig butchering’ scam city amid China pressure on junta* (Jan. 8, 2024), <https://therecord.media/myanmar-rebels-control-pig-butchering-scam-hub>.

<sup>51</sup> National Bank of Cambodia, *List of Payment Service Institutions* (Dec. 31, 2024), [https://www.nbc.gov.kh/download\\_files/data/english/En/EN-PSIs.pdf](https://www.nbc.gov.kh/download_files/data/english/En/EN-PSIs.pdf) (last accessed Mar. 21, 2025).

<sup>52</sup> Polish corporate registration database, *Huione Crypto SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ*, <https://www.biznes.gov.pl/en/wyszukiwarka-firm/wpis/krs/0001043802> (last accessed Mar. 27, 2025).

<sup>53</sup> Huione Crypto, *Career Opportunities*, <https://Huione.io/en-US/careerOpportunities> (last accessed Mar. 27, 2025); Huione Crypto, *Legal*, <https://www.huione.io/en-US/termsAndConditions/userAgreement> (last accessed Mar. 27, 2025); Huione Pay PLC, [www.huionepay.com.kh](http://www.huionepay.com.kh) (last accessed Mar. 27, 2025).

<sup>54</sup> For more information on what type of business or activity requires registration as a money service business, see FinCEN, *Money Services Business Definition*, <https://www.fincen.gov/money-services-business-definition>.

Cambodia indicating it is likely operated out of Cambodia, instead of Poland.

Additionally, the Standard Terms and Conditions of Huione Crypto state that the “Group provides the Services through [www.7572.com](http://www.7572.com), the Group’s mobile application or any Huione application programming interface.” The listed webpage ([www.7572.com](http://www.7572.com)) automatically redirects to the website of Huione Pay PLC ([www.huionepay.com.kh](http://www.huionepay.com.kh)).<sup>55</sup> Indeed, Huione Crypto’s terms expressly disclaim that persons inside the United States may not avail themselves of Huione Group’s services.<sup>56</sup> Accordingly, FinCEN finds that reasonable grounds exist to conclude that Huione Crypto is operated from and located in Cambodia and thus operates outside of the United States.

*5. Huione Group’s registrations with FinCEN and absence of United States operations*

The most evidence of activity in the United States by Huione Group or the Subsidiaries are three MSB registrations<sup>57</sup> with FinCEN and an address reported on two registrations.<sup>58</sup> In April 2023, Huione Crypto registered as a dealer in foreign exchange, and provided a business address in Phnom Penh, Cambodia, while noting no branches in the United States. In August 2024, Huione Pay Inc. registered to conduct multiple MSB activities, including check cashing, dealing in foreign exchange, and money transmission. Huione Pay Inc. provided an address in Denver, Colorado associated with a virtual mail forwarding service, and it also noted no branches in the United States. Finally, in February 2025, Huione LTD registered as a dealer in foreign exchange, money

---

<sup>55</sup> See FinCEN, MSB Registrant Search, *Huione*, <https://www.fincen.gov/msb-state-selector>.

<sup>56</sup> Huione Crypto, *Legal*, <https://www.huione.io/en-US/termsAndConditions/userAgreement> (last accessed Mar. 27, 2025).

<sup>57</sup> FinCEN’s MSB Registrant Search Web page reflects only what the registrant has provided to FinCEN, and FinCEN does not approve or endorse any business that has registered as an MSB.

<sup>58</sup> An examiner attempted to contact Huione Pay Inc. at the Denver, Colorado location in November 2024, but the examiner did not identify a Huione Pay representative, nor any other evidence of a physical presence by Huione Pay.

transmitter, and seller of money orders, and noted no branches in the United States. Huione LTD appears to use the same Denver, Colorado mail forwarding service as Huione Pay Inc. FinCEN has not identified any actual physical location or other information suggesting Huione Group or the Subsidiaries are actually operating in the United States.

Based on the foregoing, FinCEN assesses that Huione Group and the Subsidiaries are predominately operated from and located in Cambodia, with a limited connection—a corporate registration—to Poland. While the three MSB registrations by Huione Crypto, Huione Pay Inc., and Huione LTD suggest that Huione Group may intend to expand its business to the United States in the future, as of the date of this NPRM, FinCEN is not aware of any physical presence by Huione Group or the Subsidiaries in the United States or any substantial business with customers in the United States.

Accordingly, FinCEN finds that there are reasonable grounds to conclude that Huione Group and the Subsidiaries are foreign financial institutions that operate outside the United States.

#### **IV. Finding that Huione Group is of Primary Money Laundering Concern**

Pursuant to 31 U.S.C. 5318A(a)(1), FinCEN finds that reasonable grounds exist for concluding that Huione Group<sup>59</sup> is of primary money laundering concern. Below is a discussion of the relevant statutory institutional factors FinCEN considered in making this finding related to this Cambodia-based financial institution.

---

<sup>59</sup> As described in section III, Huione Group is a parent entity that controls three subsidiaries: (a) Haowang Guarantee; (b) Huione Pay PLC; and (c) Huione Crypto.

***A. The extent to which Huione Group is used to facilitate or promote money laundering, including any money laundering activity by organized criminal groups, international terrorist, or entities involved in the proliferation WMD or missiles***

Under section 311, in deciding to apply one or more special measures, FinCEN may consider the extent to which the financial institution is “used to facilitate or promote money laundering” including “any money laundering activity by organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction or missiles.”<sup>60</sup> FinCEN assesses that Huione Group is used to facilitate and promote money laundering, particularly in support of illicit financial activities connected to the Democratic People’s Republic of Korea (DPRK) and Southeast Asia-based TCOs. Because Huione Group has shared infrastructure with its constituent entities, the structure makes it challenging to ascertain the specific subsidiary involved in any particular transaction. FinCEN bases this assessment on information available through both public and non-public reporting, and after thorough consideration of each of the following factors: (1) Huione Group provides services that DPRK government entities use to launder the proceeds of cyber heists; (2) TCOs based in Southeast Asia have used Huione Group to launder illicit proceeds of cyber scams, including CVC investment scams; and (3) Huione Group operates an illicit online market.

***1. Huione Group facilitates transactions for DPRK actors to launder funds from sanctions evasion and cyber heists***

DPRK-affiliated actors have extensively used the Huione Group to launder stolen CVC for the benefit of the DPRK government and in support of DPRK’s WMD and ballistic missile programs, in violation of U.S. and multilateral sanctions programs,

---

<sup>60</sup> 31 U.S.C. 5318A(c)(2)(B)(i).

including United Nation Security Council Resolutions (UNSCRs). The United States has consistently taken measures to counter DPRK's abuse of CVC and protect the United States from DPRK's illicit financial activity.<sup>61</sup> However, as outlined in Treasury's 2024 National Proliferation Financing Risk Assessment, DPRK has continued to advance its illicit exploitation of new financial technology, including the theft and laundering of CVC, to raise and move money to fund its illicit weapons programs.<sup>62</sup> Indeed, a United Nations Panel of Experts (UN POE) found that the malicious cyber activities of the DPRK generates approximately 50 percent of its foreign currency income. In its March 2024 annual report, the UN POE indicated that it was investigating 17 CVC heists in 2023 for which the DPRK may be responsible, valued at more than USD 750 million.<sup>63</sup>

*a. Background on CVC heists carried out by DPRK*

In the same March 2024 report, the UN POE noted it was investigating 58 suspected cyberattacks by DPRK's Reconnaissance General Bureau (RGB),<sup>64</sup> to which the Lazarus Group<sup>65</sup> is related, on CVC companies between 2017 and 2023, valued at approximately USD 3 billion. FinCEN assesses that these funds likely bolstered DPRK's

---

<sup>61</sup> See FinCEN, *READOUT: FinCEN Hosts Public-Private Dialogue on Countering the DPRK's Illicit Cyber Activities* (Aug. 31, 2023), <https://www.fincen.gov/news/news-releases/readout-fincen-hosts-public-private-dialogue-countering-dprks-illicit-cyber>.

<sup>62</sup> Department of the Treasury, *National Proliferation Financing Risk Assessment* (Feb. 7, 2024), at pp. 2, 18, <https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf>.

<sup>63</sup> United Nations, S/2024/215, *UN Panel of Experts Letter* (Mar. 7, 2024), at p. 60, <https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf>.

<sup>64</sup> On January 2, 2015, OFAC sanctioned DPRK's RGB for being a controlled entity of the Government of North Korea. See Department of the Treasury, Press Release, *Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea* (Jan. 2, 2015), <https://home.treasury.gov/news/press-releases/j19733>. RGB was also previously listed in the annex to E.O. 13551 on August 30, 2010. Executive Order 13551, "Blocking Property of Certain Persons With Respect to North Korea," 75 FR 53837 (Aug. 30, 2010).

<sup>65</sup> This group is commonly referred to by the cybersecurity industry as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima. For the purposes of this NPRM, FinCEN will refer to this group as Lazarus Group. See Department of the Treasury, Press Release, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Group* (Sept. 13, 2019), <https://home.treasury.gov/news/press-releases/sm774>.

WMD development.<sup>66</sup> The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and Treasury issued a joint Cybersecurity Advisory to highlight the cyber threat associated with cryptocurrency thefts and tactics used by the DPRK state-sponsored advanced persistent threat group, since at least 2020.<sup>67</sup> The U.S. government has observed DPRK cyber actors targeting a variety of organizations in the blockchain technology and cryptocurrency industry, including cryptocurrency exchanges, decentralized finance protocols, play-to-earn CVC video games, CVC trading companies, venture capital funds investing in CVC, and individual holders of large amounts of cryptocurrency or valuable non-fungible tokens.<sup>68</sup> FinCEN assesses that, over time, the DPRK's money laundering processes have become more complex in order to evade OFAC sanctions, law enforcement, and BSA reporting obligations from hacked entities or CVC entities used in the laundering process. In fact, in August 2023, the FBI alerted the public to several thefts from CVC companies that it attributed to the Lazarus Group and warned that there could be another USD 40 million worth of CVC being prepared for laundering through VASPs.<sup>69</sup>

*b. Huione Group's laundering of proceeds of DPRK cyber heists*

Despite the 2023 FBI alert and other public reporting, Huione Group has continued to receive and process these illicit proceeds. There is wide reporting that Huione Group has received stolen CVC from multiple heists linked to DPRK actors,

---

<sup>66</sup> Department of the Treasury, Press Release, *Treasury Imposes Sanctions Against the Government of The Democratic People's Republic Of Korea* (Jan. 2, 2015), <https://home.treasury.gov/news/press-releases/j19733>.

<sup>67</sup> Department of the Treasury, Press Release, *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups* (Sept. 13, 2019), <https://home.treasury.gov/news/press-releases/sm774>.

<sup>68</sup> CISA, AA22-108A, *TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies* (Apr. 20, 2022), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a>.

<sup>69</sup> FBI, *FBI Identifies Cryptocurrency Funds Stolen by DPRK* (Aug. 22, 2023), <https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk>.

namely the Lazarus Group.<sup>70</sup> For example, between June 2023 and February 2024, a CVC wallet used by the Lazarus Group sent CVC valued at over USD 150,000 to Huione Group.<sup>71</sup>

FinCEN conducted blockchain analysis, using commercially available blockchain analytic software, of flows of CVC associated with several heists carried out by DPRK. This analysis identified that Huione Group received a combined total of approximately USD 2.6 million worth of CVC from the June 2, 2023 Atomic Wallet heist and the June 22, 2023 Coinspaid<sup>72</sup> and Alphapo heists.<sup>73</sup> In July 2024, Huione Group received USD 35 million worth of stolen CVC, later attributed to the Lazarus Group by the FBI, from the May 2024 heist targeting DMM, a Japanese VASP.<sup>74</sup> While the DMM heist was not initially attributed to the Lazarus Group (or any other prohibited entity or jurisdiction), the heist itself was widely reported by the time Huione Group received the CVC, and FinCEN would expect covered financial institutions to have an effective AML/KYC program to appropriately monitor transactions for red flags indicating connections to high profile heist such as this. In total, FinCEN's analysis has identified that Huione Group has received at least USD 37.6 million worth of CVC from DPRK cyber actors stemming from DPRK-attributed heists.

---

<sup>70</sup> The U.S. government has previously issued advisories to publicly highlight the Lazarus Group's threat and tactics associated with CVC theft targeting organizations in the blockchain and CVC industry. See CISA, AA22-108A, *TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies* (Apr. 20, 2022), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-108a>.

<sup>71</sup> Reuters, *Exclusive: North Korean hackers sent stolen crypto to wallet used by Asian payment firm* (July 15, 2024), <https://www.reuters.com/technology/cybersecurity/north-korean-hackers-sent-stolen-crypto-wallet-used-by-asian-payment-firm-2024-07-15/>.

<sup>72</sup> FBI, *FBI Identifies Cryptocurrency Funds Stolen by DPRK* (Aug. 22, 2023), <https://www.fbi.gov/news/press-releases/fbi-identifies-cryptocurrency-funds-stolen-by-dprk>.

<sup>73</sup> *Id.*

<sup>74</sup> FBI, *FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of \$308 Million USD from Bitcoin.DMM.com* (Dec. 23, 2024), <https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom>.

On multiple occasions between 2022 and 2024, a DPRK national with deep ties to the RGB, DPRK's primary foreign intelligence organization, worked with Huione Pay PLC officials to transfer CVC and fiat currency. FinCEN assesses that senior Huione Pay PLC leadership was aware of the individual's affiliation with DPRK. This DPRK national maintained personal relationships with multiple Huione Pay PLC officials and regularly met in person with at least one of these officials. In late 2023, the DPRK national worked with Huione Pay PLC officials to convert CVC into fiat currency and subsequently transfer fiat currency to an associate. In total, the DPRK national transferred CVC values at tens of thousands USD to the Huione Pay PLC official. In mid-2023, the DPRK national also planned to remit USD internationally to Hong Kong and sought Huione Pay PLC officials help to do so.

Given the opacity of Huione Group and the inherent limitation of blockchain analytics, FinCEN is largely unable to determine what DPRK actors do with the CVC after they send it to Huione Group. However, given the close connection between Huione Pay PLC officials and DPRK nationals with close ties to DPRK's RGB, FinCEN assesses DPRK most likely uses Huione Group to convert CVC to fiat currencies.

*2. Huione Group's laundering of proceeds of organized criminal groups' cyber scams*

Huione Group also has significant exposure to, and has facilitated transactions associated with suspected fraud activity, including CVC investment scams, also referred to as pig-butcher. FinCEN assesses that Huione Group's extensive CVC services and its online marketplace, Haowang Guarantee, has made Huione Group, a "one stop shop" for criminals to launder CVC obtained through illicit activities, and ultimately convert it to fiat currency.



a. *Background on CVC investment scams*

In 2023, FinCEN published an alert on the “Pig Butchering” CVC investment scams.<sup>75</sup> These scams are largely perpetrated by criminal organizations based in Southeast Asia, who use victims of human trafficking to conduct outreach to millions of unsuspecting individuals around the world. The frontline scammers in these schemes are themselves often victims of trafficking, including forced labor, and are subjected to physical and mental abuse. The traffickers also force victims to work up to 15 hours a day and, in some cases, “resell” victims to other scam operations or subject them to sex trafficking.<sup>76</sup>

Once trust or a relationship has been established, the scammer will introduce the victim to a supposedly lucrative investment opportunity in CVC and direct them to use CVC investment websites or applications designed to appear legitimate, but are instead fraudulent and ultimately controlled or manipulated by the scammer. When a victim’s pace of investment slows or stops, the scammer will use even more aggressive tactics to extract any final payments. The scammer may present the victim with supposed losses on the investment and encourage them to make up the difference through additional deposits. If the victim attempts to withdraw their investment, the scammer may demand that the victim pay purported taxes or early withdrawal fees. Once the victim is unable or

---

<sup>75</sup> FinCEN, FIN-2023-Alert005, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering”* (Sept. 8, 2023), [https://www.fincen.gov/sites/default/files/shared/FinCEN\\_Alert\\_Pig\\_Butchering\\_FINAL\\_508c.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

<sup>76</sup> Department of the Treasury, Press Release, *Treasury Sanctions Cambodian Tycoon and Businesses Linked to Human Trafficking and Forced Labor in Furtherance of Cyber and Virtual Currency Scams* (Sept. 12, 2024), <https://home.treasury.gov/news/press-releases/jy2576>.

unwilling to pay more into the scam, the scammer will abruptly cease communication with the victim, taking the victim's entire investment with them.<sup>77</sup>

*b. Huione Group's laundering of proceeds of cyber scams, including CVC investment scams*

Based on FinCEN analysis of non-public information, Huione Group received at least USD 36 million worth of CVC investment scam proceeds since at least August 2021. More broadly, the analysis identified that in the aggregate, inclusive of the cyber scam proceeds, Huione Group received approximately USD 300 million worth of CVC relating to other cyber scams. Despite the limitations noted above, FinCEN assesses that, after illicit actors send CVC to Huione Group, CVC is then converted to fiat currency or different CVC, or withdrawn at a later point to move to a different VASP, as part of the money laundering process.

*3. Huione Group's lax anti-money laundering policies and procedures*

The risks presented by Huione Group's association with illicit actors and transactions linked to illicit activity are compounded by either an absence of, or ineffective, AML/KYC policies and procedures among Huione Group's components, as well as recent changes that have served to obfuscate Huione Group's involvement in illicit activity. For example, in July 2024, Huione Group was the subject of reporting by several blockchain analytic firms describing the use of its various services by TCOs for scam activity, including those offered by Haowang Guarantee.<sup>78</sup> Elliptic reported that

---

<sup>77</sup> FinCEN, FIN-2023-Alert005, *FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (Sept. 8, 2023), at p. 4, [https://www.fincen.gov/sites/default/files/shared/FinCEN\\_Alert\\_Pig\\_Butchering\\_FINAL\\_508c.pdf](https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf).

<sup>78</sup> See Chainalysis, *2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks on the Rise, Pig Butchering Scams Remain Lucrative* (Aug. 29, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/>; Elliptic, *Huione: The Company Behind the Largest Ever Illicit Online Marketplace Has Launched a Stablecoin* (Jan. 14, 2025), <https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin>.

Haowang Guarantee offered scam-enabling products and services used by scam compound operators to imprison and torture their workers. The products included tear gas, electric batons, and electronic shackles, among other related devices. The same month, in a post to its website in response to the adverse media reporting, Haowang Guarantee confirmed that “detention equipment” is not necessarily human trafficking.”<sup>79</sup> Subsequent to these events, Huione Group, namely Huione Pay PLC, removed all references to Haowang Guarantee from its websites.<sup>80</sup>

Neither Huione Pay PLC nor Haowang Guarantee have published AML/KYC policies.<sup>81</sup> Huione Crypto does not have a published AML/KYC policy either. Rather, it maintains a “standard terms and conditions” on its website governing the use of its services. In relevant part, the agreement prohibits the use of Huione Crypto’s platform by citizens, nationals or residents of particular countries, including the United States, Iran or North Korea, as well as individuals sanctioned under various national regimes, including those of the United States and United Nations. The agreement also states that “the [u]ser may not use the interface or services to disguise the origin or nature of illicit proceeds.”<sup>82</sup> However, the extent of the criminal and money laundering activity on Huione Crypto’s platforms that violate its terms and conditions agreement reflects that its AML/KYC program is either ineffective or unenforced.

---

<sup>79</sup> Haowang Guarantee, *To all public friends on social media* (July 17, 2024), <https://www.yu444.com/gonggao/detail/2237>.

<sup>80</sup> Elliptic, *Huione: The Company Behind the Largest Ever Illicit Online Marketplace Has Launched a Stablecoin* (Jan. 14, 2025), <https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin>.

<sup>81</sup> Repeated searches of their respective websites, including most recently on March 27, 2025, failed to yield any evidence of a policy. Haowang Guarantee’s website did contain cursory fraud indicators available to customers, however, in FinCEN’s assessment, this falls short of reasonable policies and procedures aimed at combatting money laundering. See Haowang Guarantee, *Fangpian*, <https://hwdb.la/fangpian> (last accessed Mar. 27, 2025).

<sup>82</sup> Huione Crypto, *Legal*, <https://www.huione.io/en-US/termsAndConditions/userAgreement> (last accessed Mar. 27, 2025).

Despite this, and as described in greater detail in section IV. A.1–2, since at least August 2021, FinCEN identified—through analysis of non-public information—that Huione Group received at least USD 37 million worth of illicit proceeds from sanctioned entities—including DPRK entities—and at least USD 300 million worth of CVC from various cyber and CVC scam activity. FinCEN’s analysis identified that, in the aggregate, Huione Group has received at least USD 4 *billion* worth of illicit proceeds, between August 2021 and January 2025.<sup>83</sup> This large-scale, persistent use of Huione Group by DPRK actors and TCO-driven CVC investment scams to launder their illicit proceeds belies the adequacy or effectiveness of Huione Group’s AML/KYC procedures.

Huione Group itself has conceded the deficiencies in its AML regime. In a July 2024 media statement, for example, Huione Group stated “our [Know Your Customer] capabilities are now seriously insufficient.”<sup>84</sup> This statement was made after previously claiming earlier that month—in response to public identification of one heist, the proceeds of which were transmitted to Huione Pay PLC—that it had not known that Huione Pay PLC “received funds indirectly” from the heist, due to the layers of transactions between the source of the heist and the Huione Group-owned wallets that ultimately received the funds.<sup>85</sup>

---

<sup>83</sup> By illicit category, Huione Group has received the following proceeds in CVC, denominated in equivalent USD value: USD 1,363 from child sexual abuse material; USD 618,861 from Darknet Markets/Illicit Cyber Vendors; USD 3,246 from FinCEN Primary Money Laundering Concerns; USD 3,248,510,440 from Identified Illicit Cyber actors; USD 47,393,602 from VASPs without KYC policies; USD 407,129,792 from OFAC Specially Designated Nationals (U.S. sanctioned entities); USD 347,549,705 from Scams; USD 22,133,556 from seized and/or stolen funds; and 2,627,009 from terrorist financing.

<sup>84</sup> See ABC News, *Cambodian online marketplace outed as one-stop shop for scammers’ money laundering and ‘detention equipment’ needs* (July 26, 2024), <https://www.abc.net.au/news/2024-07-27/online-marketplace-for-money-laundering-and-scammers/104131624>.

<sup>85</sup> Reuters, *Exclusive: North Korean hackers sent stolen crypto to wallet used by Asian payment firm* (July 15, 2024), <https://www.reuters.com/technology/cybersecurity/north-korean-hackers-sent-stolen-crypto-wallet-used-by-asian-payment-firm-2024-07-15/>.

4. *Huione Group is expanding problematic CVC-related operations despite regulatory prohibition*

Further illustrating the money laundering risk posed by Huione Group is the fact that a significant portion of its assessed illicit transactional activity involves CVC, which the National Bank of Cambodia, Huione Group’s primary regulator, expressly prohibits. In a 2024 public statement, the National Bank of Cambodia stated that payment firms are “not allowed to deal or trade any cryptocurrencies and digital assets.”<sup>86</sup> Despite this prohibition, Huione Group has continued to develop its CVC services and has even expanded its CVC offerings in recent months. In September 2024, Huione Group launched USDH, a stablecoin it explicitly advertised as “unfreezable” and “not restricted by traditional regulatory agencies.”<sup>87</sup> FinCEN assesses that Huione Group is likely taking this unusual step to hamper compliance with applicable anti-money laundering laws. Huione Group’s intentional launching of this “unfreezable” stablecoin differs from other stablecoin issuers that generally respond to law enforcement requests to freeze CVC tied to illicit activity. One particular example of this contrast occurred in July 2024, when one stablecoin issuer froze CVC valued at over USD 29 million that was located in a Huione Group CVC wallet because it was “associated with activities allegedly linked to fraudulent and transnational criminal operations.”<sup>88</sup> By offering USDH, which is “unfreezable,” even upon a lawful request from law enforcement, Huione Group facilitates and profits from money laundering, benefiting TCOs and DPRK actors exfiltrating the proceeds of their crimes.

---

<sup>86</sup> *Id.*

<sup>87</sup> Huione Crypto, *USDH is a stable currency in one word!*, <https://huione.io/en-us/introduce> (last accessed Mar. 27, 2025).

<sup>88</sup> The Record, *Tether freezes \$29 million of cryptocurrency connected to Cambodian marketplace accused of fueling scams* (July 15, 2024), <https://therecord.media/tether-freezes-29-million-crypto-connected-to-scam-marketplace>.

Given the various aggravating factors described above, FinCEN finds that the Huione Group—with its weak and ineffective AML policies, procedures, and controls, provision of services that offer anonymity and an ability to evade sanctions, and development of a stablecoin designed to hinder the ability of law enforcement to recover the proceeds of crime—is being used extensively to facilitate or promote money laundering, in particular by organized criminal groups and entities involved in the proliferation WMD or missiles.

***B. The extent to which Huione Group is used for legitimate business purposes***

Under section 311 and FinCEN’s delegated authority, in deciding to apply one or more special measure, FinCEN may consider the extent to which the financial institutions “are used for legitimate business purposes.”<sup>89</sup> In addition to the payment and CVC exchange services outlined in this NPRM, the Huione Group advertises ostensibly legitimate business services, such as systems for telephone, water, and electricity bill payments. Huione Group also offers a point-of-sale system for Cambodian businesses, though there is no indication such a system is operational in the United States.<sup>90</sup> Huione Group’s payment services are also ubiquitous in Cambodia, most often in the form of “quick response” codes, generally referred to as “QR” codes. These QR codes are common across Cambodia, and are used to pay hotel, restaurant, and supermarket bills, among other general purchases. While FinCEN does not know the full extent of Huione Group’s legitimate business activity, Huione Group’s transactional volume since

---

<sup>89</sup> 31 U.S.C. 5318A(c)(2)(B)(ii).

<sup>90</sup> Huione Pay, *Service Items: Omni-Directional Service*, <https://www.huionepay.com.kh/index/service?lang=en> (last accessed Mar. 27, 2025).

inception is believed to be at least USD 49 billion worth of CVC since 2021,<sup>91</sup> including licit and illicit volume. While FinCEN lacks insight into most of Huione Groups fiat currency transaction activity, additional FinCEN analysis revealed that Huione Group engaged in at least USD 41 million in cleared international transactions through U.S. correspondent bank accounts, between December 2020 and December 2024.

Huione Group's activity, through these constituent services, indicates some legitimate business transiting the financial institution. However, under the totality of circumstances, FinCEN assesses that the benefits of any legitimate business activities Huione Group conducts are outweighed by the substantial money laundering risks it poses.

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

Under section 311 and FinCEN's delegated authority, in deciding to apply one or more special measures, FinCEN may consider the extent to such action is "sufficient to ensure," that the purpose of section 311 "continue[s] to be fulfilled, and to guard against international money laundering and other financial crimes."<sup>92</sup> A finding that Huione Group is of primary money laundering concern would make clear the illicit finance risk it poses to domestic financial institutions, and by extension, to their foreign correspondents. This awareness is likely to cause those financial institutions, or their regulators, to take their own action to mitigate the risks posed by Huione Group. Moreover, such a finding and subsequent imposition of special measure five, as proposed here, would protect the

---

<sup>91</sup> Chainalysis, *2024 Crypto Crime Mid-year Update Part 2: China-based CSAM and Cybercrime Networks on the Rise, Pig Butchering Scams Remain Lucrative* (Aug. 29, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/>; The New York Times, *How Scammers Launder Money and Get Away With It* (Mar. 23, 2025), <https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html>.

<sup>92</sup> 31 U.S.C. 5318A(c)(2)(B)(iii).

U.S. financial system from money laundering and other financial crimes by severing Huione Group's access to the U.S. financial system.

## **V. Proposed Special Measure**

Having found that Huione Group is a financial institution operating outside of the United States and is of primary money laundering concern (particularly regarding its laundering of illicit proceeds from DPRK-affiliated cyber heists and CVC investment scams carried out by TCOs based in Southeast Asia), FinCEN proposes imposing a prohibition on covered financial institutions under special measure five. Special measure five authorizes the Secretary to impose conditions upon the opening or maintaining in the United States of a correspondent account or payable-through account, if such account “involves” a financial institution of primary money laundering concern.<sup>93</sup> Although Huione Group does not have correspondent accounts with U.S. financial institutions, it has accounts with foreign financial institutions that maintain U.S. correspondent accounts. Those U.S. correspondent accounts involve Huione Group when transactions involving the financial institution are processed through those accounts. Thus, FinCEN has determined that special measure five will most effectively mitigate the risks posed by Huione Group.

FinCEN considered the other special measures available under section 311. As discussed further in section IV.E. below, it determined that none of them would appropriately address the risks posed by Huione Group.

In proposing this special measure, FinCEN consulted with representatives and staff of the Board of Governors of the Federal Reserve System, the Office of the

---

<sup>93</sup> 31 U.S.C. 5318A(b)(5).



Comptroller of the Currency, the Secretary of State, the staff of the Securities and Exchange Commission, the Commodity Futures Trading Commission, staff of the National Credit Union Administration, the Federal Deposit Insurance Corporation, and the Attorney General.<sup>94</sup> These consultations involved obtaining interagency views on the imposition of special measure five and the effects that such a prohibition would have on the U.S. domestic and international financial systems.

In addition, FinCEN considered the factors set forth in section 311, as set forth below.<sup>95</sup>

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

In March 2025, at least one news outlet reported that the National Bank of Cambodia stripped Huione Pay PLC of its banking license.<sup>96</sup> FinCEN is not otherwise aware of any other nation or multilateral group that has imposed, or is currently imposing, similar action against Huione Group.

***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***

While FinCEN assesses that the prohibition proposed in this NPRM would place some cost and burden on covered financial institutions, these burdens are neither undue nor inappropriate in view of the threat posed by the illicit activity facilitated by Huione Group. As described above and according to public and non-public information, Huione Group has no direct USD correspondent relationships with U.S. financial institutions and

---

<sup>94</sup> See 31 U.S.C 5318A(b)(5).

<sup>95</sup> 31 U.S.C. 5318A(a)(4)(B)(i)-(iv).

<sup>96</sup> Radio Free Asia, *Exclusive: World's Largest online black market' Loses banking license* (Mar. 6, 2025), <https://www.rfa.org/english/cambodia/2025/03/06/huione-cambodia-cyberscam-cryptocurrency/>.

instead, accesses USD through nested corresponding relationships, outside the United States. These accounts may be used for commercial payments, as well as foreign exchange and money markets. Covered financial institutions and transaction partners have ample opportunity to arrange for alternative payment mechanisms in the absence of correspondent banking relationships with Huione Group.

As such, a prohibition on correspondent banking with Huione Group is expected to impose minimal additional compliance costs for covered financial institutions, which would most commonly involve adding Huione Group to existing sanctions and money laundering screening tools. FinCEN assesses that given the risks posed by Huione Group's facilitation of money laundering, the additional burden on covered financial institutions in preventing the opening of correspondent accounts with Huione Group, as well as conducting due diligence on foreign correspondent account holders and notifying them of the prohibition, will be minimal and not undue.

***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 of Huione Group***

FinCEN assesses that imposing the proposed special measure would have minimal impact upon the international payment, clearance, and settlement system. As a comparatively small financial institution responsible for a nominal amount of transaction volume in the region, Huione Group is not a systemically important financial institution in Cambodia, regionally, or globally. FinCEN views that prohibiting Huione Group's access to U.S. correspondent banking channels would not affect overall cross-border transaction volumes. Further, a prohibition under special measure five would not prevent Huione Group from conducting legitimate business activities in other foreign currencies.

***D. The effect of the proposed action on United States national security and foreign policy***

As described above, evidence available to FinCEN demonstrates that Huione Group serves as a significant conduit for money laundering by TCOs engaged in CVC investment scams and DPRK-related actors engaging in CVC heists. Imposing special measure five will: (1) close Huione Group's access to USD; (2) inhibit Huione Group's ability to act as an illicit finance facilitator for DPRK and TCOs engaged in CVC investment scams; and (3) raise awareness of the way illicit actors exploit weaknesses in vulnerable jurisdictions to circumvent sanctions and finance WMD and ballistic missile proliferation.

***E. Consideration of alternative special measures***

In assessing the appropriate special measure to impose, FinCEN considered alternatives to a prohibition on the opening or maintaining in the United States of correspondent accounts or payable-through accounts, including the imposition of one or more of the first four special measures, or imposing conditions on the opening or maintaining of correspondent accounts under special measure five. Having considered these alternatives and for the reasons set out below, FinCEN assesses that none of the other special measures available under section 311 would appropriately address the risks posed by Huione Group and the urgent need to prevent it from accessing USD through correspondent banking.

With its public acknowledgements of its failure to address significant AML/KYC deficiencies, Huione Group continues to present a significant money laundering risk, particularly related to DPRK cyber heists and TCO-run scams. Taken as a whole, Huione Group's history of involvement in laundering proceeds of illicit activities, and its creation

of an unfreezable stablecoin, presents a heightened risk that Huione Group will continue to be used by illicit actors. A key feature of Huione Group's service offerings includes a marketplace to sell items that enable CVC investment scams, and money laundering services to launder the proceeds of the scams. Huione Group serves as a significant node of the money laundering ecosystem that enables criminals to both obtain necessary items to carry out various crimes, and the services to launder the proceeds of those crimes.

Because of the nature, extent, and purpose of the obfuscation engaged in by Huione Group, any special measure intended to mandate additional information collection would likely be ineffective and insufficient to determine the true identity of illicit finance actors who transact with the group. For example, the provision under special measure one, that "the identity and address of the participants in a transaction or relationship, including the identity of the originator of any funds transfer" be collected in records and reports, could be circumvented by the operations of shell companies, wherein the reported identity of the originator serves to obscure the true beneficial owner or originator.<sup>97</sup> This would be ineffective in preventing illicit transactions. Huione Group's record of such circumvention suggests that special measure one would not adequately protect the U.S. financial system from the threats posed by the financial institution. Further, the requirements under special measures three and four, that domestic financial institutions obtain "with respect to each customer (and each such representative), information that is substantially comparable to that which the depository institution obtains in the ordinary course of business with respect to its customers residing in the United States," are also likely to be ineffective.<sup>98</sup> Huione Group's use of nested

---

<sup>97</sup> 31 U.S.C. 5318A(b)(1)(B)(i).

<sup>98</sup> 31 U.S.C 5318A(b)(3)(B).

correspondent account access through layers of payment systems would render these alternative measures ineffective. Only significant effort and expense by U.S. institutions could fill this gap, which would impose a disproportionate compliance burden, with no guarantee that the money laundering threat would be addressed through customer due diligence research. FinCEN also considered special measure two, which may require domestic financial institutions to “obtain and retain information concerning the beneficial ownership of any account opened or maintained in the United States by a foreign person.”<sup>99</sup> The agency determined that this special measure would likely be ineffective since the concerns involving Huione Group do not involve the opening or maintaining of accounts in the U.S. by foreign persons.

FinCEN similarly assesses that merely imposing conditions under special measure five would be inadequate to address the risks posed by Huione Group’s activities. Special measure five enables FinCEN to impose conditions as an alternative to a prohibition on the opening or maintaining of correspondent accounts.<sup>100</sup> Given Huione Group’s longstanding ties to DPRK proliferation finance, coupled with money laundering tied to CVC investment scams, and public acknowledgment of failures of its AML/KYC program, FinCEN determined that imposing any condition would not be an effective measure to safeguard the U.S. financial system. FinCEN assesses that the billions of dollars’ worth of CVC and fiat laundered through Huione Group’s exploitation of its access to USD, and the exposure of U.S. financial institutions to Huione Group’s illicit activity, outweigh the value in providing conditioned access to the U.S. financial system for any purportedly legitimate business activity. Conditions on the opening or

---

<sup>99</sup> 31 U.S.C. 5318A(b)(2).

<sup>100</sup> 31 U.S.C. 5318A(b)(5).

maintaining of correspondent accounts would likely be insufficient to prevent illicit financial flows through the U.S. financial system, given Huione Group's inadequate AML/KYC program.

In sum, FinCEN assesses that any condition or additional recordkeeping or reporting requirement would be an ineffective measure to safeguard the U.S. financial system from the illicit behavior facilitated by Huione Group. Such measures would not prevent Huione Group from accessing the correspondent accounts of U.S. financial institutions, thus leaving the U.S. financial system vulnerable to processing illicit transfers that are likely to finance DPRK's nuclear proliferation, or CVC investment scams, resulting in significant national security and money laundering risk. In addition, no recordkeeping or reporting requirements or conditions would be sufficient to guard against the risks posed by a financial institution that processes transactions that are designed to obscure the transactions' true nature and are ultimately for the benefit of DPRK and TCOs. Therefore, FinCEN has determined that a prohibition on opening or maintaining correspondent banking relationships is the only available special measure available under section 311 that can adequately protect the U.S. financial system from the illicit finance risk posed by Huione Group. For these reasons, and after thorough consideration of alternate measures, FinCEN assesses that no measures short of full prohibition on correspondent or payable-through banking access would be sufficient to address the money laundering risks posed by Huione Group.

## **VI. Section-by-Section Analysis**

The goal of this proposed rule is to combat and deter DPRK-affiliated money laundering and the laundering of proceeds from cyber scams including, CVC investment

scams carried out by TCOs through Huione Group, and to prevent Huione Group from using the U.S. financial system to enable its illicit finance behavior.

**A. 1010.664(a)—Definitions**

**1. Definition of Huione Group**

The term “Huione Group” means all subsidiaries, branches, and offices of Huione Group operating as a financial institution in any jurisdiction outside of the United States, including Haowang Guarantee (formerly known as Huione Guarantee), Huione Pay PLC, and Huione Crypto Spółka Z Ograniczoną Odpowiedzialnością (d/b/a Huione Crypto).

**2. Definition of Correspondent Account**

The term “correspondent account” has the same meaning as the definition contained in 31 CFR 1010.605(c)(1)(ii). In the case of a U.S. depository institution, this broad definition includes most types of banking relationships between a U.S. depository institution and a foreign bank that are established to provide regular services, dealings, and other financial transactions, including a demand deposit, savings deposit, or other transaction or asset account, and a credit account or other extension of credit. FinCEN is using the same definition of “account” for purposes of this proposed rule as is established for depository institutions in the final rule implementing the provisions of section 312 of the USA PATRIOT Act, requiring enhanced due diligence for correspondent accounts maintained for certain foreign banks.<sup>101</sup> Under this definition, “payable-through accounts” are a type of correspondent account.

In the case of securities broker-dealers, futures commission merchants, introducing brokers in commodities, and investment companies that are open-end

---

<sup>101</sup> See 31 CFR 1010.605(c)(2)(i).

companies (mutual funds), FinCEN is also using the same definition of “account” for purposes of this proposed rule as was established for these entities in the final rule implementing the provisions of section 312 of the USA PATRIOT Act, requiring due diligence for correspondent accounts maintained for certain foreign banks.<sup>102</sup>

### *3. Definition of Covered Financial Institution*

The term “covered financial institution” is defined by reference to [31 CFR 1010.605\(e\)\(1\)](#), the same definition used in the BSA rule ([31 CFR 1010.610](#)) requiring the establishment of due diligence programs for correspondent accounts for financial institutions. In general, this definition includes the following:

- a bank;
- a broker or dealer in securities;
- a futures commission merchant or an introducing broker in commodities; and
- a mutual fund.

### *4. Definition of Foreign Banking Institution.*

The term “foreign banking institution” means a bank organized under foreign law, or an agency, branch, or office located outside the United States of a bank. The term does not include an agent, agency, branch, or office within the United States of a bank organized under foreign law.

### *5. Definition of Subsidiary*

The term “subsidiary” means a company of which more than 50 percent of the voting stock or an otherwise controlling interest is owned by another company.

---

<sup>104</sup> See 31 CFR 1010.605(c)(2)(ii)-(iv).



**B. 1010.664(b)—*Prohibition on Accounts and Due Diligence Requirements for Covered Financial Institutions***

**1. *Prohibition on Opening or Maintaining Correspondent Accounts***

Section 1010.664(b)(1) of the proposed rule would prohibit covered financial institutions from opening or maintaining in the United States a correspondent account for, or on behalf of, Huione Group.

**2. *Prohibition on Use of Correspondent Accounts Involving Huione Group***

Section 1010.664(b)(2) of the proposed rule would require covered financial institutions to take reasonable steps to not process a transaction for the correspondent account of a foreign banking institution in the United States if such a transaction involves Huione Group. Such reasonable steps are described in 1010.664(b)(3), which sets forth the special due diligence requirements a covered financial institution would be required to take when it knows or has reason to believe that a transaction involves Huione Group.

**3. *Special Due Diligence for Correspondent Accounts***

As a corollary to the prohibition set forth in section 1010.664(b)(1) and (2), section 1010.664(b)(3) of the proposed rule would require covered financial institutions to apply special due diligence to all of their foreign correspondent accounts that is reasonably designed to guard against such accounts being used to process transactions involving Huione Group. As part of that special due diligence, covered financial institutions would be required to notify those foreign correspondent account holders that the covered financial institutions know or have reason to believe provide services to Huione Group, that such correspondents may not provide Huione Group with access to the correspondent account maintained at the covered financial institution. A covered financial institution may satisfy this notification requirement using the following notice:

Notice: Pursuant to U.S. regulations issued under Section 311 of the USA PATRIOT Act, see 31 CFR 1010.664, we are prohibited from opening or maintaining in the United States a correspondent account for, or on behalf of, Huione Group. The regulations also require us to notify you that you may not provide Huione Group, including any of its subsidiaries, branches, and offices access to the correspondent account you hold at our financial institution. If we become aware that the correspondent account you hold at our financial institution has processed any transactions involving Huione Group, including any of its subsidiaries, branches, and offices, we will be required to take appropriate steps to prevent such access, including terminating your account.

The purpose of the notice requirement is to aid cooperation with correspondent account holders in preventing transactions involving Huione Group from accessing the U.S. financial system. FinCEN does not require or expect a covered financial institution to obtain a certification from any of its correspondent account holders that access will not be provided to comply with this notice requirement.

Methods of compliance with the notice requirement could include, for example, transmitting a notice by mail, fax, or e-mail. The notice should be transmitted whenever a covered financial institution knows or has reason to believe that a foreign correspondent account holder provides services to Huione Group.

Special due diligence also includes implementing risk-based procedures designed to identify any use of correspondent accounts to process transactions involving Huione Group. A covered financial institution would be expected to apply an appropriate screening mechanism to identify a funds transfer order that on its face listed Huione Group as the financial institution of the originator or beneficiary, or otherwise referenced Huione Group in a manner detectable under the financial institution's normal screening mechanisms. An appropriate screening mechanism could be the mechanisms used by a covered financial institution to comply with various legal requirements, such as

commercially available software programs used to comply with the economic sanctions programs administered by the U.S. Department of the Treasury's OFAC.

#### **4. *Recordkeeping and Reporting***

Section 1010.664(b)(4) of the proposed rule would clarify that the proposed rule does not impose any reporting requirement upon any covered financial institution that is not otherwise required by applicable law or regulation. A covered financial institution must, however, document its compliance with the notification requirement described above in section 1010.664(b)(3).

### **VII. Request for Comments**

FinCEN is requesting comments for 30 days after the publication of this NPRM. Given Huione Group's consistent and longstanding ties to facilitating transactions for DPRK proliferation finance and cyber scams including CVC investment scams, and its track record of facilitating and promoting money laundering in support of DPRK and TCOs' illicit activity, FinCEN assesses that a 30-day comment period for this NPRM strikes an appropriate balance between ensuring sufficient time for notice to the public and opportunity for comment on the proposed rule, while minimizing undue risk posed to the U.S. financial system in processing illicit transfers that are likely to finance DPRK WMD proliferation, funds derived from cyber scams, including CVC investment scams carried out by TCOs, and other illicit activity. FinCEN invites comments on all aspects of the proposed rule, including the following specific matters:

1. FinCEN's proposal of a prohibition under the fifth special measure under 31 U.S.C. 5318A(b), as opposed to imposing special measures one through four or imposing conditions under the fifth special measure;

2. The form and scope of the notice to certain correspondent account holders that would be required under the rule; and
3. The appropriate scope of the due diligence requirements in this proposed rule.

## **VIII. Regulatory Impact Analysis**

FinCEN has analyzed this proposed rule under Executive Orders 12866, 13563, the Regulatory Flexibility Act,<sup>103</sup> the Unfunded Mandates Reform Act,<sup>104</sup> and the Paperwork Reduction Act.<sup>105</sup>

As discussed above, the intended effects of the imposition of special measure five to Huione Group are twofold. The rule is expected to: (1) combat and deter money laundering in facilitation of proliferation financing associate with Huione Group; and (2) prevent Huione Group from using the U.S. financial system to enable its illicit finance behavior. In the analysis below, FinCEN discusses the economic effects that are expected to accompany adoption of the rule as proposed and assesses such expectations in more granular detail. This discussion includes an explanation of how FinCEN's assumptions and methodological choices have influenced FinCEN's conclusions. The public is invited to comment on all aspects of FinCEN's practice.<sup>106</sup>

### ***A. Executive Orders***

Executive Orders 12866 and 13563 direct agencies to assess costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563

---

<sup>103</sup> 5 U.S.C. 603.

<sup>104</sup> 12 U.S.C. 1532, Public Law 104–4 (Mar. 22, 1995).

<sup>105</sup> 44 U.S.C. 3507(a)(1)(D).

<sup>106</sup> See Section VII; see also Section VIII.D.

emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility.

It has been determined that this proposed rule is not a significant regulatory action under section 3(f) of Executive Order 12866. Accordingly, a regulatory impact analysis is not required.

#### ***B. Regulatory Flexibility Act***

When an agency issues a rulemaking proposal, the Regulatory Flexibility Act (RFA) requires the agency to “prepare and make available for public comment an initial regulatory flexibility analysis” (IRFA) that will “describe the impact of the proposed rule on small entities.”<sup>107</sup> However, section 605 of the RFA allows an agency to certify a rule, in lieu of preparing an analysis, if the proposed rulemaking is not expected to have a significant economic impact on a substantial number of small entities. This proposed rule would apply to all covered financial institutions and would affect a substantial number of small entities. Nevertheless, for the reasons described below, FinCEN assesses that these changes would be unlikely to have a significant economic impact on such entities.

Covered financial institutions would also be required to take reasonable measures to detect use of their correspondent accounts to process transactions involving Huione Group. All U.S. persons, including U.S. financial institutions, currently must comply with OFAC sanctions, and U.S. financial institutions generally have suspicious activity reporting requirements and systems in place to screen transactions to comply with OFAC sanctions and section 311 special measures administered by FinCEN. The systems that U.S. financial institutions have in place to comply with these requirements can easily be

---

<sup>107</sup> 5 U.S.C. 603(a).

modified to adapt to this proposed rule. Thus, the special due diligence that would be required under the proposed rule—*i.e.*, preventing the processing of transactions involving Huione Group and the transmittal of notification to certain correspondent account holders—would not impose a significant additional economic burden upon small U.S. financial institutions. For these reasons, FinCEN certifies that the proposals contained in this rulemaking would not have a significant impact on a substantial number of small businesses.

FinCEN invites comments from members of the public who believe there would be a significant economic impact on small entities from the imposition of a prohibition under the fifth special measure regarding Huione Group.

### ***C. Unfunded Mandates Reform Act***

Section 202 of the Unfunded Mandates Reform Act of 1995<sup>108</sup> (Unfunded Mandates Reform Act), requires that an agency prepare a budgetary impact statement before promulgating a rule that may result in expenditure by the state, local, and tribal governments, in the aggregate, or by the private sector, of USD 100 million or more in any one year, adjusted for inflation.<sup>109</sup> If a budgetary impact statement is required, section 202 of the Unfunded Mandates Reform Act also requires an agency to identify and consider a reasonable number of regulatory alternatives before promulgating a rule.<sup>110</sup>

FinCEN has determined that this proposed rule will not result in expenditures by state, local, and tribal governments in the aggregate, or by the private sector, of an annual

---

<sup>108</sup> 12 U.S.C. 1532, Public Law 104–4 (Mar. 22, 1995).

<sup>109</sup> *Id.*

<sup>110</sup> *Id.*

USD 100 million or more, adjusted for inflation (USD 188.9 million).<sup>111</sup> Accordingly, FinCEN has not prepared a budgetary impact statement or specifically addressed the regulatory alternatives considered.

#### ***D. Paperwork Reduction Act***

The recordkeeping and reporting requirements, referred to by the Office of Management and Budget (OMB) as a collection of information, contained in this proposed rule will be submitted by FinCEN to the OMB for review in accordance with the Paperwork Reduction Act of 1995 (PRA).<sup>112</sup> Under the PRA, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by the OMB. Written comments and recommendations for the proposed prohibition can be submitted by visiting [www.reginfo.gov/public/do/PRAMain](http://www.reginfo.gov/public/do/PRAMain). Find this particular document by selecting “Currently under Review—Open for Public Comments” or by using the search function. Comments are welcome and must be received by [30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. In accordance with requirements of the PRA and its implementing regulations, 5 CFR part 1320, the following information concerning the collection of information as required by 31 CFR 1010.664 is presented to assist those persons wishing to comment on the information collections.

---

<sup>111</sup> The Unfunded Mandates Reform Act requires an assessment of mandates that will result in an annual expenditure of USD 100 million or more, adjusted for inflation. The U.S. Bureau of Economic Analysis reports the annual value of the gross domestic product (GDP) deflator in the first quarter of 1995, the year of the Unfunded Mandates Reform Act, as 66.452, and as 125.532 in the third quarter of 2024, the most recent available. See U.S. Bureau of Economic Analysis, “Table 1.1.9. Implicit Price Deflators for Gross Domestic Product,” <https://www.bea.gov/itable/> (last accessed Jan. 17, 2025). Thus, the inflation adjusted estimate for USD 100 million is  $125.532/66.452 \times 100 = \text{USD } 188.9 \text{ million}$ .

<sup>112</sup> 44 U.S.C. 3507(a)(1)(D).

The provisions in this proposed rule pertaining to the collection of information can be found in sections 1010.664(b)(3)(i)(A) and 1010.664(b)(4). The notification requirement in section 1010.664(b)(3)(i)(A) is intended to aid cooperation from foreign correspondent account holders in preventing transactions involving Huione Group from being processed by the U.S. financial system. The information required to be maintained by section 664(b)(4) will be used by federal agencies and certain self-regulatory organizations to verify compliance by covered financial institutions with the notification requirement in section 1010.664(b)(3)(i)(A). The collection of information would be mandatory.

*Frequency:* As required.

*Description of Affected Financial Institutions:* Only those covered financial institutions defined in section 1010.664(a)(3) that are engaged in correspondent banking with, or processing transactions potentially involving, Huione Group as defined in section 1010.664(b)(1) and (2) would be affected.



*Estimated Number of Potential Respondents: Approximately 15,710.*<sup>113</sup>

**Table 1. Estimates of Covered Financial Institutions by Type**

| <b>FINANCIAL INSTITUTION TYPE</b>               | <b>NUMBER OF ENTITIES</b> |
|---|---------------------------|
| Banks with an FFR <sup>a</sup>                  | 8,995 <sup>b</sup>        |
| Banks without an FFR <sup>c</sup>               | 395 <sup>d</sup>          |
| Broker-dealers in securities <sup>e</sup>       | 3,320 <sup>f</sup>        |
| Open end mutual funds <sup>g</sup>              | 2,036 <sup>h</sup>        |
| Futures commission merchants <sup>i</sup>       | 65 <sup>j</sup>           |
| Introducing brokers in commodities <sup>k</sup> | 899 <sup>l</sup>          |

<sup>a</sup> See 31 CFR 1010.100(t)(1); *see also* 31 CFR 1010.100(d).

<sup>b</sup> Bank data is as of Jan. 17, 2025, from Federal Deposit Insurance Corporation BankFind (<https://banks.data.fdic.gov/bankfind-suite/bankfind>). Credit union data is as of Sept. 2024 from the National Credit Union Administration Quarterly Data Summary Reports (<https://ncua.gov/analysis/credit-union-corporate-call-report-data/quarterly-data-summary-reports>).

<sup>c</sup> 31 CFR 1020.210(b).

<sup>d</sup> The Board of Governors of the Federal Reserve System Master Account and Services Database contains data on financial institutions that utilize Reserve Bank financial services, including those with no federal regulator. FinCEN used this data to identify 395 banks and credit unions utilizing Reserve Bank financial services with no federal regulator. (<https://www.federalreserve.gov/paymentsystems/master-account-and-services-database-existing-access.htm>)

<sup>e</sup> 31 CFR 1010.100(t)(2).

<sup>f</sup> According to the Securities and Exchange Commission (SEC), there are 3,320 broker-dealers in securities as of Mar. 2025 from website “Company Information About Active Broker-Dealers” (<https://www.sec.gov/foia-services/frequently-requested-documents/company-information-about-active-broker-dealers>).

<sup>g</sup> See 31 CFR 1010.100(t)(10); *see also* 31 CFR 1010.100(gg).

<sup>h</sup> According to the SEC, in 2024 there were 2,036 open-end registered investment companies that report on Form N-CEN. (<https://www.sec.gov/dera/data/form-ncen-data-sets>).

<sup>i</sup> 31 CFR 1010.100(t)(8).

<sup>j</sup> According to the Commodity Futures Trading Commission (CFTC), there are 65 futures commission merchants as of November 30, 2024. See *Financial Data for FCMs*, <https://www.cftc.gov/MarketReports/financialfcmdata/index.htm>.

<sup>k</sup> 31 CFR 1010.100(t)(9).

<sup>l</sup> According to the National Futures Association, there are 899 introducing brokers in commodities as of Dec. 31, 2024 from website “NFA Membership Totals” (<https://www.nfa.futures.org/registration-membership/membership-and-directories.html>).

<sup>113</sup> This estimate is informed by public and non-public data sources regarding both an expected maximum number of entities that may be affected and the number of active, or currently reporting, registered financial institutions.

*Estimated Number of Expected Respondents: Approximately 127.<sup>114</sup>*

**Table 2. Estimates of Affected Financial Institutions by Type**

| <b>FINANCIAL INSTITUTION TYPE</b>  | <b>NUMBER OF ENTITIES</b> |
|------------------------------------|---------------------------|
| Banks with an FFR                  | 60 <sup>a</sup>           |
| Banks without an FFR               | 17 <sup>b</sup>           |
| Broker-dealers in securities       | 26 <sup>c</sup>           |
| Open end mutual funds              | 16 <sup>d</sup>           |
| Futures commission merchants       | 1 <sup>e</sup>            |
| Introducing brokers in commodities | 7 <sup>f</sup>            |

<sup>a</sup> Data are from the FFIEC Central Data Repository for Reports of Condition and Income (Call Reports) and Uniform Bank Performance Reports (UBPRs), available for most FDIC-insured institutions. Using this source of data, FinCEN determines that as of Q3 2024, approximately 60 banks (as defined by FinCEN regulations, *see* 31 CFR 1010.100(d)) will be affected by this rule on any given year. Specifically, we determine that there are approximately 60 banks that report non-zero values for deposit liabilities of banks in foreign countries. Deposit liabilities in a foreign country is an indication that a bank maintains correspondent accounts with a foreign financial institution.

<sup>b</sup> The Board of Governors of the Federal Reserve System Master Account and Services Database contains data on financial institutions that utilize Reserve Bank financial services, including those with no federal regulator. FinCEN used this data to identify an additional 17 international banking entities with no federal regulator and that do not file Call Reports, but that are also likely to maintain correspondent accounts with a foreign financial institution.

<sup>c</sup> Broker dealers, unless they are publicly traded, are not required to make reports indicating whether or not they have foreign correspondent accounts or hold foreign deposits. FinCEN reviewed financial statement data from 10-Q and 6-K filings with the SEC, and identified nine publicly traded broker dealers with US operations that reported foreign deposits. FinCEN also examined Suspicious Activity Reports (SARs) filed by broker dealers in 2024 to identify another two non-publicly traded broker dealers who appeared likely to be maintaining foreign deposits. However, because many broker dealers are not publicly traded and did not file SARs, FinCEN conservatively estimates that the proportion of broker dealers with foreign correspondent accounts will be similar to the proportion for banks (approximately 0.8%). 0.8% of 3,320 active broker dealers is approximately 26 broker dealers assumed to have foreign correspondent accounts.

<sup>d</sup> Mutual funds, futures commission merchants, and introducing brokers in commodities generally use intermediary US banks to move and maintain client deposits and funds for investment. Therefore, it is unlikely that many of these institutions will maintain direct correspondent accounts with foreign financial institutions outside of their existing upstream banking relationships. However, because these institutions may in some cases receive deposits from, make payments or other disbursements, or otherwise transact directly with foreign financial institutions, FinCEN conservatively estimates that the proportion of mutual funds with foreign correspondent accounts will be similar to the proportion for banks (approximately 0.8%). 0.8% of 2,036 active mutual funds is approximately 16 mutual funds assumed to have foreign correspondent accounts.

<sup>e</sup> 0.8% of 65 active futures commission merchants is approximately one futures commission merchants assumed to have foreign correspondent accounts.

<sup>f</sup> 0.8% of 899 active introducing brokers in commodities is approximately seven introducing brokers in commodities assumed to have foreign correspondent accounts.

<sup>114</sup> While this regulation applies to all covered institutions described in Table 1, in practice the burden will only be imposed on select institutions that maintain correspondent accounts for foreign banks. Table 2 below presents an estimate of this subpopulation of banks, brokers or dealers in securities, mutual funds, futures commission merchants, and introducing brokers in commodities based on data from the most recent calendar year end.

*Estimated Average Annual Burden in Hours per Affected Financial Institution:*

Imposing special measure five requirements as described in this proposed rule is expected to result in a new, incremental recordkeeping burden on certain covered financial institutions as described above. Each anticipated component of this is outlined below.

Each affected covered financial institution is expected to incur a recordkeeping burden associated with preparing and retaining the materials necessary to demonstrate compliance with the proposed requirements. This is expected to include records related to:

- B.** Documenting the reasonable steps the financial institution undertakes to ensure no transactions involving Huione Group are processed for a foreign correspondent account, including:
  - 1. Any investigative activities undertaken when the financial institution knows or has reason to believe that a foreign bank's correspondent account has been or is being used to process transactions involving Huione Group.
  - 2. Any subsequent activities undertaken to prevent such access, including, where necessary, termination of the correspondent account.
- C.** Notifying, and documenting that the financial institution has provided notice to, foreign correspondent account holders that the financial institution knows or has reason to believe provide services to Huione Group, that such correspondents may not provide Huione Group with access to the correspondent account maintained at the financial institution.

**D.** Documenting the reasonable steps it took with respect to special due diligence requirements, including but not limited to, the reasoning that informed decisions to adopt (or not adopt) new measures adding to its existing risk-based approach, and those new measures, if adopted.

The estimated average annual burden associated with the collection of information in this proposed rule is, in total, one business day, or eight hours per affected financial institution.

*Estimated Total Annual Burden:* Approximately 1,016 hours.<sup>115</sup>

*Estimated Total Annual Cost:* Approximately \$121,920.<sup>116</sup>

*FinCEN invites comments on:* (a) whether the proposed collection of information found in section 1010.664(b)(4) is necessary for the proper performance of the mission of FinCEN, including whether the information would have practical utility; (b) the accuracy of FinCEN's estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information required to be maintained; (d) ways to minimize the burden of the required collection of information, including through the use of automated collection techniques or other forms of information technology; and

---

<sup>115</sup> 127 expected respondents multiplied by eight hours per respondent equals 1,016 total annual burden hours.

<sup>116</sup> The wage rate applied here is a general composite hourly wage (\$85.55), scaled by a private-sector benefits factor of 1.42 ( $\$120.07 = \$85.55 \times 1.42$ ), that incorporates the mean wage data (available for download at <https://www.bls.gov/oes/tables.htm>, "May 2023 - National industry-specific and by ownership") associated with the six occupational codes (11-1010: Chief Executives; 11-3021: Computer and Information Systems Managers; 11-3031: Financial Managers; 13-1041: Compliance Officers; 23-1010: Lawyers and Judicial Law Clerks; 43-3099: Financial Clerks, All Other) for each of the nine groupings of NAICS industry codes that FinCEN determined are most directly comparable to its eleven categories of covered financial institutions as delineated in 31 CFR parts 1020 to 1030. The benefit factor is 1 plus the benefit/wages ratio, where as of June 2023, Total Benefits = 29.4 and Wages and salaries = 70.6 ( $29.4/70.6 = 0.42$ ) based on the private industry workers series data downloaded from [https://www.bls.gov/news.release/archives/ecec\\_09122023.pdf](https://www.bls.gov/news.release/archives/ecec_09122023.pdf) (accessed Dec. 22, 2024). Given that many occupations provide benefits beyond cash wages (e.g., insurance, paid leave, etc.), the private sector benefit is applied to reflect the total cost to the employer. 1,016 total annual burden hours multiplied by \$120 per hour equals a total annual cost of \$121,920.

(e) estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to report the information.

## **IX. Regulatory Text**

### **List of Subjects in 31 C.F.R. Part 1010**

Administrative practice and procedure, Banks, Banking, Brokers, Crime, Foreign banking, Terrorism.

### **Authority and Issuance**

For the reasons set forth in the preamble, FinCEN proposes amending 31 C.F.R. part 1010 as follows:

### **Part 1010-GENERAL PROVISIONS**

1. The authority citation for part 1010 continues to read as follows:

“Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C. 5311-5314, 5316-5336; title III, sec. 314, Pub. L. 107-56, 115 Stat. 307; sec. 2006, Pub. L. 114-41, 129 Stat. 458-459; sec. 701 Pub. L. 114-74, 129 Stat. 599; sec. 6403, Pub. L. 116-283, 134 Stat. 3388.”

2. Add 1010.664 to read as follows:

#### **1010.664 Special measures regarding Huione Group.**

- (a) *Definitions.* For purposes of this section, the following terms have the following meanings.

(1) *Huione Group.* The term “Huione Group” means all subsidiaries, branches, and offices of Huione Group operating as a financial institution in any jurisdiction outside of the United States, including Haowang Guarantee (formerly known as Huione Guarantee), Huione Pay PLC, and Huione Crypto Spółka Z Ograniczoną Odpowiedzialnością (d/b/a Huione Crypto).

(2) *Correspondent account.* The term “correspondent account” has the same meaning as provided in 1010.605(c)(1)(ii).

(3) *Covered financial institution.* The term “covered financial institution” has the same meaning as provided in 1010.605(e)(1).

(4) *Foreign banking institution.* The term “foreign banking institution” means a bank organized under foreign law, or an agency, branch, or office located outside the United States of a bank. The term does not include an agent, agency, branch, or office within the United States of a bank organized under foreign law.

(5) *Subsidiary.* The term “subsidiary” means a company of which more than 50 percent of the voting stock or an otherwise controlling interest is owned by another company.

(b) *Prohibition on accounts and due diligence requirements for covered financial institutions.*

(1) *Prohibition on opening or maintaining correspondent accounts for Huione Group.* A covered financial institution shall not open or maintain in the United States a correspondent account for, or on behalf of, Huione Group.

(2) *Prohibition on processing transactions involving Huione Group.* A covered financial institution shall take reasonable steps not to process a transaction for the correspondent account in the United States of a foreign banking institution if such a transaction involves Huione Group.

(3) *Special due diligence of correspondent accounts to prohibit transactions.*

(i) A covered financial institution shall apply special due diligence to its foreign correspondent accounts that is reasonably designed to guard against their use to process

transactions involving Huione Group. At a minimum, that special due diligence must include:

(A) Notifying those foreign correspondent account holders that the covered financial institution knows or has reason to believe provide services to Huione Group that such correspondents may not provide Huione Group with access to the correspondent account maintained at the covered financial institution; and

(B) Taking reasonable steps to identify any use of its foreign correspondent accounts by Huione Group, to the extent that such use can be determined from transactional records maintained in the covered financial institution's normal course of business.

(ii) A covered financial institution shall take a risk-based approach when deciding what, if any, other due diligence measures it reasonably must adopt to guard against the use of its foreign correspondent accounts to process transactions involving Huione Group.

(iii) A covered financial institution that knows or has reason to believe that a foreign bank's correspondent account has been or is being used to process transactions involving Huione Group shall take all appropriate steps to further investigate and prevent such access, including the notification of its correspondent account holder under paragraph (b)(3)(i)(A) of this section and, where necessary, termination of the correspondent account.

*(4) Recordkeeping and reporting.*

(i) A covered financial institution is required to document its compliance with the notification requirement set forth in this section.

(ii) Nothing in paragraph (b) of this section shall require a covered financial institution to report any information not otherwise required to be reported by law or regulation.

Dated: May 1, 2025

Andrea M. Gacki  
Director  
Financial Crimes Enforcement Network