ANTI-MONEY LAUNDERING ("AML") COMPLIANCE PROGRAM:

Policies, Procedures, and Internal Controls V1.0

CRIPCOM TRADE LLC

30 N Gould STE 100

Sheridan, WY 82801

Last Update: May 1, 2025 2

Table of Contents

1. MSB Activities 3

2. Firm Policy 3

3. AML Program 3

4. M.S.B. Registration (31 C.F.R. § 1022.380) 3

5. A.M.L. Compliance Officer Designation and Duties (31 C.F.R. § 1022.210(d)(2)) 4

6. Giving AML Information to Law Enforcement Agencies and Other Financial Institutions 4

7. Know Your Customer ("KYC") 6

8. Customer Identification Program (31 CFR § 1022.210(d)) 6

9. Sanctions Screening 7

10. Agent Relationships 7

11. Monitoring Transactions for Suspicious Activity (31 C.F.R.§ 1022.320(a)) 8

12. BSA Reporting 9

13. BSA Recordkeeping 11

14. Foreign Agents and Counterparties (..... 14

15. Education and Training Program (31 C.F.R. § 1022.210 (d)(3)) 15

16. Independent Review of A.M.L. Program (31 C.F.R. § 1022.210 (d)(4)) 16

17. Senior Management Approval 16

18. Risk Assessment 17

1. MSB Activities

Headquartered in Sheridan, Wyoming ("Cripcom" or the "Firm") is a money services business. Operating via the Firm's website, Cripcom offers foreign exchange, digital virtual currency trading, and international money transfer services. In providing these services, Cripcom is classified as a dealer in foreign exchange and as a money transmitter, as those terms are defined in 31 CFR §1010.100(ff). As such, the Firm is required to implement and maintain an anti-money laundering program and is subject to other BSA/AML regulatory requirements governing money services businesses.

2. Firm Policy

It is the policy of Cripcom to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or financial institutions to separate the money from its criminal origin further. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex. 4

3. AML Program

Cripcom's anti-money laundering policies, procedures, and internal controls (collectively, our "AML Program") are reasonably designed to ensure compliance with all applicable BSA regulations and will be reviewed and updated on a regular basis.

These reviews will be conducted to address changes in regulations and in our business dealings. They will also be performed to ensure that appropriate policies, procedures, and internal controls are in place.

Our AML Program shall be kept in writing. We will make copies of our AML Program available for inspection to the Department of the Treasury upon request.

4. M.S.B. Registration (31 C.F.R. § 1022.380)

In providing money transmittal, Cripcom is obligated to register with FinCEN as an MSB.

(a) Registration

We are registered with FinCEN as an MSB. Our MSB registration number is 31000299058425.

(b) Registration Records

We shall retain a copy of the field MSB registration form and other supporting documentation at the following US address:

30 N Gould Ste 100

Sheridan, WY 82801

We shall retain these registration documents for a period of at least five years.

(c) Registration Renewal

We shall renew our registration by the end (April 30) of the second calendar year following our initial registration and by December 31 of every second calendar year thereafter.

(d) Events Requiring Re-registration 5

If any of the following events occurs during a registration period (more than 180 days before the next renewal date), we shall re-file a registration form with information different from that reported on the form originally filed:

- Change in Ownership or Control under State Law. A change in ownership or control of the MSB requires the MSB to be re-registered under State law.
- Transfer of Voting Power or Equity Interest. More than 10 percent of the voting power or equity interest of the MSB has been transferred (except MSBs that must report such a transfer to the Securities and Exchange Commission);
- Increase in the Number of Agents. The number of agents of the MSB has increased by more than 50 percent.

To re-register, we shall complete and file an RMSB no later than 180 days after the date on which the triggering event occurred.

5. A.M.L. Compliance Officer Designation and Duties (31 C.F.R. § 1022.210(d)(2))

Cripcom has designated Syed Rizvi as its Anti-Money Laundering Compliance Officer ("AML Compliance Officer"), with full responsibility for the Firm's AML Program.

Mr. Rizvi has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge, and training.

The duties of the AML Compliance Officer will include overseeing all aspects of the Firm's compliance with AML obligations. These duties shall specifically include assuring that:

- The Firm properly files reports and creates and retains records, in accordance with applicable requirements of the BSA;
- Our AML Program is updated as necessary to reflect the current requirements of the BSA, and related guidance issued by the Department of the Treasury; and
- The Firm provides appropriate training and education in accordance with 31 CFR § 1022.210(d)(3).

6. Giving AML Information to Law Enforcement Agencies and Other Financial Institutions 6

(a) FinCEN Requests under USA PATRIOT Act Section 314(a)

As of the latest update to these procedures, FinCEN did not make regular 314(a) requests of most MSBs. Should FinCEN ever make a 314(a) request of the Firm, we shall implement the following policies and procedures:

Upon receiving an information request under 31 CFR § 1010.520, we shall designate one person to be the point of contact regarding the request and to receive similar requests for information from FinCEN in the future. When requested by FinCEN, we shall provide FinCEN with the name, title, mailing address, email address,

telephone number, and facsimile number of such person, in such manner as FinCEN may prescribe. After providing FinCEN with this contact information, we shall promptly notify FinCEN of any changes to such information.

As required by 31 CFR § 1010.520(a)(3), "upon receiving an information request from FinCEN under [§ 1010.520, we shall] expeditiously search [our] records to determine whether [we maintain] or [have] maintained any account for, or [have] engaged in any transaction with, each individual, entity, or organization named in FinCEN's request." If we find a match, our AML Compliance Officer will report it to FinCEN via FinCEN's Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), our AML Compliance Officer will structure our search accordingly.

When we search our records but do not find a matching account or transaction, we will not reply to the 314(a) request. We will maintain documentation that we have performed the required search by printing a search self-verification document from FinCEN's 314(a) Secure Information Sharing System, evidencing that we have searched the 314(a) subject information against our records.

We will not disclose the fact that FinCEN has requested or obtained information from us except to the extent necessary to comply with the information request. Our AML Compliance Officer will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm- Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) request to the requesting law enforcement agency as designated in the request. Unless otherwise stated in the 314(a) request, we will not be required to treat the information request as continuing in nature, 7

and we will not be required to treat the periodic 314(a) Requests as a government-provided list of suspected terrorists for purposes of the customer identification and verification requirements.

b. Voluntary Information Sharing with Other Financial Institutions under USA PATRIOT Act, Section 314(b) (31 CFR § 1010.540)

We may share information with other financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before doing so, our AML Compliance Officer will ensure that the Firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use FinCEN's Web site to file these notices. Before sharing information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions FinCEN will make available. We understand that this requirement applies even to financial institutions with which we are affiliated. As with non-affiliated firms, we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures to ensure that only relevant information is shared and to protect the security and confidentiality of this information.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

7. Know Your Customer ("KYC")

The inadequacy or absence of KYC standards can subject an MSB to reputational, operational, legal, and financial risks. These risks are interrelated, and any one of them could result in significant costs to Cripcom (e.g., through the departure of customers, the loss of business and banking relationships, claims against the MSB, investigation costs, time and energy devoted to resolving problems, etc.). An effectively devised KYC policy is an important defense against money launderers. 8

(a) Benefits of KYC

Knowledge of Cripcom's customer base will help the MSB:

- Detect suspicious activity in a timely manner.
- Enable deeper analysis of potential and current customers.
- Promote safe business practices.
- Minimize the risk of the MSB's channels being used for illicit activities.
- Protect the MSB's reputation & image.

(b) Customer Profiling and Enhanced Due Diligence Reviews

Customer profiling is a way to create a portrait of our customer to help make decisions concerning our services. Factors such as customers' background, country of origin, public or high-profile position, source of wealth, business activities, or other risk indicators shall be considered when determining whether a customer presents a higher risk to the MSB.

Every new customer shall be profiled using judgment and information obtained through an online identity verification service. Through this service, we will check each customer against various databases for AML and KYC validation. We will use the information obtained to establish the customer's profile. Any customer with a high-risk profile must be approved by Cripcom's AML Compliance Officer before any transaction may be conducted. Ongoing reviews of high-risk customers will be conducted by our AML Compliance Officer.

8. Customer Identification Program (31 CFR § 1022.210(d))

To satisfy the Customer Identification Program ("CIP") requirements found in 31 CFR § 1022.210(d)(1), we shall collect and verify certain identifying information for each person or entity who effects a covered transaction with the Firm. We shall record customer identification information and the verification methods and results.

(a) Covered Transactions

Following is a list of covered transaction activities in which Cripcom may engage:

- Foreign exchange of more than $1,000 for any person on any day
- Money transmittals

(b) Required Customer Information – Cryptocurrency exchange, Liquidating Prepaid Cards, and Money Transmittals

Before conducting a money transmittal, we will obtain and verify, at a minimum, the name and address of the customer. 9

9. Sanctions Screening

Given the global nature of the business, cross-border payments and liquidity provider services are particularly exposed to risks related to sanctioned entities and individuals. The objective of sanctions screening is to prevent the organization from doing business with individuals, entities, or countries that are on various sanctions lists maintained by government bodies around the world.

In this process, we compare customer data against various sanctions lists. If there is a potential match, we investigate further to confirm whether it is a true match or a false positive. True matches must be reported to the relevant authorities and the business relationship is usually terminated.

The primary sanctions list that Cripcom screens against is the Specially Designated Nationals (SDN) list maintained by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury. The SDN list includes individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific.

However, sanctions are not only imposed by the U.S. but also by other countries and international bodies. Therefore, Cripcom also screen against other lists such as:

- The United Nations Security Council Sanctions List, which includes individuals and entities sanctioned under various UNSC resolutions.
- The Consolidated List of Financial Sanctions Targets and the Investment Ban List, both maintained by the UK's Office of Financial Sanctions Implementation (OFSI).
- The Consolidated List maintained by the European Union, which includes all persons, groups and entities subject to EU financial sanctions.
- The DPL (Denied Persons List), the UL (Unverified List), and the Entity List maintained by the U.S. Department of Commerce.

10. Agent Relationships

Citing 31 CFR § 1022.210(d)(1)(iii), in its March 11, 2016, Guidance, FinCEN explained that, in MSB principal-agent relationships, "each MSB remains independently and wholly responsible for implementing adequate AML program requirements." 10

FinCEN explained that, as the principal M.S.B., we must "have procedures in place to identify those agents conducting activities that appear to lack commercial purpose, lack justification, or otherwise are not supported by verifiable documentation. The principal must implement risk-based procedures to monitor the agents' transactions to ensure they are legitimate. The procedures must also ensure that, if the agents' transactions trigger reporting or recordkeeping requirements, the principal handles the information in accordance with regulatory reporting and recordkeeping obligations. In addition, the MSB principal should implement procedures for handling non-compliant agents, including agent contract terminations."

Recognizing our responsibility in each of these areas, we have implemented the following policies, procedures, and internal controls:

(a) Transaction Reviews

We recognize the risks presented to the Firm through the actions of our agents. To address these risks, we will monitor the activities of our agents.

As noted below, we will review transactions conducted through our agents. In performing these reviews, we will be attentive to agent activities that appear to lack commercial purpose or justification or are not supported by verifiable documentation.

As part of these reviews, we will confirm that we have created the required records and filed the required reports for agent transactions that trigger BSA reporting or recordkeeping requirements.

(b) AML Program Reviews

On at least an annual basis, we will also review the written AML policies and procedures of each of our agents. We will perform these reviews to ensure our agents have effective AML programs. An effective AML program will address all relevant BSA requirements, including CIP, Transaction Monitoring, BSA Reporting, and Recordkeeping.

(c) Agent Transaction – BSA Reporting and Recordkeeping

As specified in this program, Cripcom accepts full responsibility for BSA reporting and recordkeeping requirements related to Cripcom's MSB activities. Whether transactions 11

are conducted directly with us or whether they are conducted through our agents, we will file all required reports and keep all required records.

(d) Corrective Action and Termination

Agent deficiencies noted in our due-diligence activities will be reported to the agent. The agent must promptly respond to and resolve each identified deficiency. Based on our assessment of the risk presented by each identified deficiency, we shall work with the agent to set a resolution date.

Should an agent fail to respond timely or appropriately to an identified deficiency, or should our management team determine that an identified deficiency presents an unacceptable risk, we shall take immediate actions to temporarily or permanently cease all business activities with the agent. We shall take such actions should an agent ever demonstrate systemic, willful, or repeated lapses in compliance with our AML procedures or requirements.

11. Monitoring Transactions for Suspicious Activity (31 C.F.R.§ 1022.320(a))

(a) Transaction Reviews

To ensure our attentiveness to money laundering and terrorist financing activities, we will review all transactions conducted or attempted by, at, or through the Firm (including transactions conducted with agents) involving $2,000 or more of funds or assets (either individually or in the aggregate).

On a monthly basis, we will complete a transaction review form ("TRF"), on which we will document our reviews. To evidence our compliance with our requirement to identify and report suspicious transactions, we will maintain copies of our TRFs for at least five years from the date of the review.

(b) Red Flags

We will use a Transaction Review Form ("TRF") to document our reviews of transactions. With our TRF, we will consider whether or not a transaction has, at a minimum, any of the red flags identified by FinCEN in its publication: Money Laundering Prevention: A Money Services Business Guide

(https://www.fincen.gov/sites/default/files/guidance/msb_prevention_guide.pdf):

Red flags that signal possible money laundering or terrorist financing include, but are not limited to: 12

Customer ID or Information

- Customer uses a false ID.
- Two/more customers use similar IDs.
- Customer alters transaction upon learning that he/she must show ID.

- Customer alters spelling or order of his/her full name.

Transactions Below Reporting or Recordkeeping Thresholds

- Customer conducts transactions just below relevant thresholds:
- Currency exchanges are just under $1,000.

Multiple Persons

- Two or more customers work together to break one transaction into two or more transactions to evade the BSA reporting or recordkeeping requirement.

Overt Illegal Customer Conduct

- Customer offers bribes or tips.
- Customer admits to criminal conduct.

(c) Enhanced Due Diligence

For any transaction (or any combination of transactions made in a given month) of more than $10,000, Cripcom will verify the customer's source of income by reviewing documentation of the customer's funds. This documentation may include bank statements, pay stubs, and other official records which reasonably explain the source of the customer's funds. The Firm will also obtain from the customer an explanation of the purpose of the transaction. Before processing the transaction, our AML compliance officer will review the information provided by the customer and, if it is deemed satisfactory, approve the transaction.

Documentation of these activities will be maintained.

(d) Responding to Red Flags and Suspicious Activity

When an employee of the Firm detects any red flags or other activities that may be suspicious, he or she will notify our AML Compliance Officer. Under the direction of the AML Compliance Officer, the Firm will determine whether or not and how to investigate the matter further. This may include gathering additional information internally or from third-party sources, contacting the government, and/or filing a SAR.

12. BSA Reporting

(a) Use of the B.S.A. E-Filing System

We shall submit each SAR, CTR, FinCEN Form 114 (FBAR), and RMSB using the B.S.A. e-Filing System. 13

(b) Currency Transaction Report ("CTR") (31 CFR § 1010.311)

For each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to us which involves a transaction in currency of more than $10,000 and which is not between Cripcom and a commercial bank (see § 1010.315), we shall file with FinCEN a CTR. Also, we will treat multiple transactions involving currency as a single transaction to determine whether to file a CTR if they total more than $10,000 and are made by or on behalf of the same person during any one business day. We shall file a CTR within 15 days following the day on which the reportable transaction occurred. We shall retain a copy of each CTR for a period of five years from the date of the report.

(i) Identification Required (31 CFR § 1010.312)

Before concluding any transaction with respect to which the filing of a CTR is required, we shall verify and record the name and address of the individual presenting the transaction, as well as record the identity, account number, and social security or other taxpayer identification number, if any, of any person or entity

on whose behalf such transaction is to be effected. Verification of the identity of an individual who indicates that he or she is an alien or not a United States resident shall be made by passport, alien identification card, or other official documents evidencing nationality or residence.

In each instance, the specific identifying information used in verifying the identity of the customer shall be recorded on the report.

(ii) Aggregation (31 CFR § 1010.313)

In determining whether we are obligated to file a CTR, we shall aggregate activities across all of our branches.

We shall treat multiple currency transactions as a single transaction if we know that these transactions are made by or on behalf of any person and result in either cash in or cash out totaling more than $10,000 during any one business day.

(c) Report of Transportation of Currency or Monetary Instruments ("CMIR") (31 CFR § 1010.340)

As required by 31 CFR § 1010.340, we shall file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the US currency or other monetary instruments in an aggregate amount 14

exceeding $10,000 at one time. We shall file such report within 15 days after receipt of the currency or other monetary instruments.

We shall also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means currency or other monetary instruments of more than $10,000 at one time. We shall file such report at the time of departure, mailing or shipping from the United States.

(d) Report of Foreign Financial Accounts (31 CFR § 1010.350 and 420) As of the date of this program, we have no financial interest in, or signature or other authority over, a bank, securities, or other financial accounts in a foreign country.

Should we ever have a financial interest in, or signature or other authority over, a bank, securities, or other financial accounts in a foreign country, we shall report such relationship to the Commissioner of Internal Revenue for each year in which such relationship exists and shall provide such information as shall be specified in a reporting form prescribed under 31 USC 5314. The form prescribed under section 5314 is the Report of Foreign Bank and Financial Accounts (FinCEN Form 114 or "FBAR").

We shall file all FBARs with the Commissioner of Internal Revenue on or before June 30 of each calendar year with respect to foreign financial accounts exceeding $10,000 maintained during the previous calendar year. We shall retain such records for a period of five years and shall keep them at all times available for inspection as authorized by law.

(e) S.A.R. Filing (31 C.F.R. § 1022.320)

We will file a SAR with FinCEN for any transaction conducted or attempted by, at, or through the Firm involving $2,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect, or have reason to suspect that the transaction:

- involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

- is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;

15

- serves no business or apparent lawful purpose, and after examining the available facts, including the background and possible purpose of the transaction. We know of no reasonable explanation for the transaction; or

- involves the use of the Firm to facilitate criminal activity.

We may voluntarily file a SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation, but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day period begins when an appropriate review is conducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

(f) Emergency Notification to Law Enforcement by Telephone (31 FCR § 1022.320(b)(3))

In situations involving violations that require immediate attention, such as ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. In addition to local law enforcement authorities, we may also contact FinCEN's Financial Institutions Hotline (866.556.3974) to report transactions relating to terrorist activity. If we notify the appropriate law enforcement authority of such activity, we must still file a timely SAR.

(g) Joint Filing of S.A.R.s with Other Financial Institutions (31 C.F.R. § 1022.320)

If we and one or more other party have an obligation to report a transaction, we may file a single SAR jointly with the other party.

When filing jointly, we will ensure that the filed SAR contains all relevant facts, including the name of each party involved in the transaction. We will also ensure that the SAR complies with all instructions applicable to joint filings, and that we keep a copy of the report filed, along with any supporting documentation. 16

If we determine it is appropriate to file a SAR jointly, we understand that we cannot disclose that we have filed a SAR to any party except the party filing jointly. If we determine it is not appropriate to file jointly (e.g., because the SAR concerns the other party or one of its employees), we understand that we cannot disclose that we have filed a SAR to any party.

13. BSA Recordkeeping

We will keep all required records (including CIP records, SAR filings, and other required records) for at least five years.

(a) Required Records – Funds Transmittals (31 CFR § 1010.410)

In addition to the maintenance of records referenced elsewhere in this program, we shall retain either the original or a copy of each of the following:

(i) For funds transmittals under the Funds Transfer and Travel Rules (31

CFR §§ 1010.410(e) and (f)), when we are the transmittor's financial institution in funds of $3,000 or more, we will retain a record of the transmittal order. We will record the following information on the transmittal order:

- the name and address of the transmittor;
- the amount of the transmittal order;
- the execution date of the transmittal order;
- any payment instructions received from the transmittor with the transmittal order;
- any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order. and
- the identity of the recipient's financial institution.

In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order:

- the name and address of the recipient;
- the account number of the recipient;
- any other specific identifier of the recipient; and

(ii) In the case of a transmittal order of $3,000 or more from a transmittor that is not an established customer, in addition to obtaining and retaining the information required by 31 CFR § 1010.410(e)(1)(i), we will follow the criteria specified by § 1010.410(e)(2)(i) and (ii):

- Verify identity of person placing the order.
- Retain a record of the following information of the person placing the order: name, address, tax id number or alien identification number or passport number, and copy of the presented identification.
- If we know that the person placing the order is not the transmittor, we shall retain a record of the transmittor's tax id number or alien identification number or

17

passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

If the transmittal order is not made in person, we shall retain a record of the following:

- Name and address of the person placing the transmittal order, the person's tax id number, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (e.g., check or credit card transaction) for the transmittal of funds.
- If we know that the person placing the transmittal order is not the transmittor, we shall obtain and retain a record of the transmittor's tax id number or alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

(iii) For each transmittal order of $3,000 or more that we accept as a recipient's financial institution for a recipient that is not an established customer, in addition to obtaining and retaining the information

required by 31 CFR § 1010.410(e)(1)(iii), we shall also obtain the information required by 31 CFR § 1010.410(e)(3)(i) and (ii): If the proceeds are delivered in person to the recipient or its representative or agent, we shall

- Verify the identity of the person receiving the proceeds, and
- Retain a record of the name and address, the type of identification reviewed, and the number of the identification document, as well as a record of the person's tax identification number or alien identification number or passport number, and country of issuance or a notation in the record of the lack thereof.

If we have knowledge that the person receiving the proceeds is not the recipient, we shall obtain and retain the following:

- a record of the recipient's name and address, as well as the recipient's taxpayer identification number or alien identification number or passport number, and country of issuance, if known by the person receiving the proceeds, or a notation in the record of the lack thereof.

If the proceeds are delivered other than in person, we shall retain a copy of the check or other instrument used to effect payment or the information contained thereon, as well as the name and address of the person to which it was sent.

(b) Retrievability

Regarding the information that shall be retained under section "a" above:

As the transmittor's financial institution, we shall retain information in a format that shall allow us to retrieve the information by reference to the name of the transmittor. If the transmittor is an established customer and has an account used for transmittals of funds, then the information also shall be retrievable by account number. 18

As the recipient's financial institution, we shall retain information of our recipient in a format that shall allow us to retrieve the information by reference to the name of the recipient. If the recipient is an established customer and has an account used for transmittals of funds, then the information also shall be retrievable by account number.

(c) Additional Records to Be Retained by Dealers in Foreign Exchange (31 CFR § 1022.410)

We shall retain either the original or a copy of each of the following:

- Statements of accounts from banks, including paid checks, charges or other debit entry memoranda, deposit slips and other credit memoranda representing the entries reflected on such statements;
- Daily work records, including purchase and sales slips or other memoranda needed to identify and reconstruct currency transactions with customers and foreign banks;
- A record of each exchange of currency involving transactions in excess of
- $1,000, including the name and address of the customer (and passport number or taxpayer identification number unless received by mail or common carrier) date and amount of the transaction and currency name, country, and total amount of each foreign currency;
- Signature cards or other documents evidencing signature authority over each deposit or security account, containing the name of the depositor, street address, taxpayer identification number (TIN) or employer identification number (EIN) and the signature of the depositor or of a person authorized to sign on the account (if customer accounts are maintained in a code name, a record of the actual owner of the account);

- Each item, including checks, drafts, or transfers of credit, of more than
- $10,000 remitted or transferred to a person, account or place outside the United States;
- A record of each receipt of currency, other monetary instruments, investment securities and checks, and of each transfer of funds or credit, or more than $10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the United States;
- Records prepared or received by us in the ordinary course of business, that would be needed to reconstruct an account and trace a check in excess of
- $100 deposited in such account through our internal recordkeeping system to our depository institution, or to supply a description of a deposited check in excess of $100;

19

- A record maintaining the name, address, and taxpayer identification number, if available, of any person presenting a certificate of deposit for payment, as well as a description of the instrument and date of transaction;
- A system of books and records that will enable us to prepare an accurate balance sheet and income statement.

(d) SAR Maintenance and Confidentiality (31 CFR § 1022.320)

We will retain copies of all SARs filed and any supporting documentation for five years from the date of filing the SAR.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where authorized by FinCEN, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a SAR according to the provisions of Section 6(b) (above). In cases in which we file a joint SAR for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed SAR.

14. Foreign Agents and Counterparties (FinCEN Release No. 2004– 01:

https://www.fincen.gov/resources/statutes-regulations/guidance/guidance-interpretive-release-2004-1-anti-money-laundering)

Before entering into a relationship with any foreign agent or foreign counterparty, and on at least an annual basis after entering into any such relationship, we shall conduct risk-based due diligence and monitoring of activities:

(a) Review Structure and Risk Profile

- Location of agent/counterparty – check FATF guidance regarding risks posed by jurisdiction.
- Ownership of agent/counterparty – run OFAC check against owners
- Require agent/counterparty to be subject to AML requirements in its jurisdiction and that it establish internal controls.

- Use web searches to check for any reports of AML issues with agent/counterparty.

20

- Review of agent/counterparty's business, the markets it serves, and the extent to which its structure presents an increased risk for money laundering or terrorist financing.
- Review the types and purposes of services to be provided to, and anticipated activity with, the agent/counterparty.
- Consideration of the nature and duration of our relationship with the agent/counterparty.
- Identify material changes in the agent/counterparty's risk profile (ex: ownership, business, or the regulatory scrutiny to which it is subject).

(b) Monitoring

- Review of transactions to identify and, where appropriate, report suspicious transactions, including:

(1) unusual wire activity;

(2) bulk sales or purchases of sequentially numbered instruments;

(3) multiple purchases or sales that appear to be structured, and;

(4) illegible or missing customer information.

- Review of agent/counterparty AML program to discern obvious breakdowns in the implementation of the program by the agent or counterparty.
- Review of agent/counterparty activities for signs of structuring or unnecessarily complex transmissions through multiple jurisdictions that may be indicative of layering or of efforts to evade detection.

(c) Corrective Action and Termination

Agent/counterparty deficiencies noted in our due-diligence activities will be reported to the agent/counterparty. The agent/counterparty must promptly respond to and resolve each identified deficiency. Based on our assessment of the risk presented by each identified deficiency, we shall work with the agent/counterparty to set a resolution date.

Should an agent or counterparty fail to respond timely or appropriately to an identified deficiency, or should our management team determine that an identified deficiency presents an unacceptable risk, we shall take immediate actions to temporarily or permanently cease all business activities with the agent or counterparty. We shall take such actions should an agent or counterparty ever demonstrate systemic, willful, or repeated lapses in compliance with our AML procedures or requirements.

15. Education and Training Program (31 C.F.R. § 1022.210 (d)(3))

Under the direction of our AML Compliance Officer, we will provide ongoing education and training of appropriate personnel. This education and training will occur on at least 21

an annual basis. It will explain the responsibilities of Firm personnel under the Firm's AML compliance program, including education and training in the detection of suspicious transactions. If we have any branch offices or agents, we will ensure that they receive appropriate training. Newly hired personnel will complete training before they are permitted to conduct any covered transaction.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles

are in the Firm's compliance efforts and how to perform them; (4) the Firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training internally, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the names of persons trained, dates of training, and copies of training.

16. Independent Review of A.M.L. Program (31 C.F.R. § 1022.210 (d)(4))

The review of our AML compliance program will be performed annually (on a calendar year basis) by Counsellize Inc. an independent, third-party service provider, or by another, similarly qualified, service provider.

We have evaluated Counselize Consulting's qualifications to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations.

17. Senior Management Approval

Senior management of Cripcom hereby approves this AML compliance program as being reasonably designed to achieve and monitor our ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by the signature below. Signed:

Name: Diego Camacho Pulido

Title: Manager

Date May 1, 2025

18. Risk Assessment

"Although MSBs are not required by regulation to create a written risk assessment, management is encouraged to document its risk assessment in writing in order to provide a clear basis for the MSB's policies and procedures. If the MSB does not have a written risk assessment, the examiner will generally need to conduct more in depth interviews in order to determine the MSB's risk profile." (From The BSA/AML Examination Manual for Money Services Businesses,

https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf)

As a Money Services Business ("MSB"), Cripcom has conducted the following assessment of the money laundering risks present in its business activities:

Business Summary

We are registered with FinCEN to conduct business as a money transmitter and a foreign exchange dealer.

In these dealings, we most typically provide services to customers in the United States, Canada, the United Kingdom, Europe, Africa, and Asia. Our customers use our Platform for sending and receiving funds from friends, family members, and business associates worldwide. To access our services, clients can conveniently use the Cripcom mobile application or our website.

Identified Risks

In our effort to identify the risks to our firm, we have referred to the Bank Secrecy Act/Anti-money Laundering Examination Manual for MSBs

(https://www.fincen.gov/sites/default/files/shared/MSB_Exam_Manual.pdf).

Much of the following language was taken directly from this publication:

FinCEN has identified certain risks in the MSB industry. After considering these identified risks, and taking into account our particular business operations, we have identified the following risks to our firm:

Operational: Operational risk is the risk that an MSB will fail to detect or prevent money laundering or terrorist financing as a result of inadequate internal processes or systems, or as a result of human failure. Evaluation of operational risk includes:

- The MSB's systems used to process transactions that utilize transactional dollar limitations;

23

- The frequency of agent or employee turnover;
- The recordkeeping system utilized by the MSB;
- The activities of the MSB. (MSBs whose activities include both financial and non-financial products and services such as retail stores who cash checks);
- The MSB's business structure and business plan;
- The involvement of senior management in BSA matters; and
- The MSB's agent relationships.

We have identified and ranked the following operational risks to our business:

1. Cripcom's business plan: international money transmittals offered via our app and website.
2. Our use of foreign agents/counterparties.

Customer: Although any customer could conceivably be engaged in money laundering or terrorist financing, certain customers may pose heightened risk because of the nature of their business, occupation, or anticipated transactions. In assessing our customer risk, we have considered the following questions:

- Who are our customers?
- For what purpose do they use our services or products?
- How do they pay for these service or product?
- What is an average transaction?
- How frequently does the customer purchase the service or product?
- When is the customer most likely to need the service or product?
- What is the typical daily or monthly volume?

After considering these questions, we have identified and ranked the following customer risks to our business:

1. 1Most customers are foreign nationals.
2. Disbursements to beneficiaries will be handled through our agents.

Product: Offering certain products and services such as those that offer customers more anonymity or involve the handling of high dollar volumes of currency or currency equivalents, may pose greater risk of money laundering or terrorist financing to an MSB. For example, sales of traveler's checks, sales of money orders, and transmittals of funds may be particularly vulnerable to structuring. An effective AML program for an MSB significantly engaged in such activities would include the training of employees to recognize indications of structuring.

We have identified and ranked the following product risks to our business: 24

1. International money transmittals may be used to finance terrorist activities.
2. Foreign exchange transactions may be used to launder illicit funds.

Geographic: Identifying geographic locations that may pose a higher risk of money laundering or terrorist financing is essential to an MSB's risk assessment. MSBs should understand and evaluate the specific risks associated with doing business in, processing transactions for customers from, or facilitating transactions involving certain geographic locations.

High-risk geographic locations can be either international or domestic. International high-risk geographic locations generally include:

- Countries, jurisdictions and governments subject to OFAC sanctions, including state sponsors of terrorism;
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State;
- Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act;
- Countries and territories identified as non-cooperative by the Financial Action Task Force (FATF); and

- Major money laundering countries and jurisdictions identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries that are identified as jurisdictions of primary concern.

Domestic high-risk geographic locations may include, but are not limited to, a U.S. Government-designated high-risk geographic location. Domestic high-risk geographic locations include both High Intensity Drug Trafficking Areas (HIDTAs) and High Intensity Financial Crime Areas (HIFCAs).

We have identified and ranked the following geographic risks to our business:

1. Certain African countries are subject to U.S. sanctions.

2. Certain African countries have been deemed non-cooperative by FATF.

Commensurate with these risks, we have developed the policies, procedures and internal controls contained in this AML Compliance Program. Based on this risk assessment, our AML Compliance Program is effectively designed to prevent our firm from being used to facilitate money laundering or terrorist activities.