MetaLoop Inc
Anti-Money Laundering (AML) Program:
Compliance and Supervisory Procedures

UPDATED AS OF MARCH 11, 2022

1. Preamble

This document establishes a firm-wide anti-money laundering (AML), countering the financing of terrorism (CFT), and sanctions program for MetaLoop Inc.

MetaLoop Inc, hereinafter referred to as MetaLoop or the firm, builds non-custodial Multi-Party-Computation-based multi-signature wallets with fiat on-ramp capabilities. MetaLoop allows users to buy and sell selected cryptocurrencies and interact with different blockchain networks.

It is important to note that MetaLoop does not consider itself and should not be considered as a Money Service Business because of the following reasons:

- the value belongs to the owner and is stored in his or her wallet;
- MetaLoop provides additional validation for the users via Multi-Party Computation, hereinafter referred to as MPC, but does not have total independent control over the value;
- in order to perform any transaction, the user has to initiate it and locally generate a signature;

MetaLoop does not have total independent control over funds at a user's wallet and is therefore unable to intervene for any blockchain-based transactions that a user wishes to make. MetaLoop is also unable to stop or impose any limits on users' blockchain-based transactions.

It is important to note that this policy, therefore, only applies to our fiat on-ramp service. All references to "accounts" refer to on-ramp accounts, and not the non-custodial wallets that users have created with MetaLoop.

2. Firm Policy

It is the policy of the firm 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 other financial institutions to further separate the money from its criminal origin. 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.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

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 as 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.

Our AML policies, procedures and internal controls are designed to ensure compliance with applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.

2. AML Compliance Person Designation and Duties

The firm has designated Jason Li as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm’s AML program. Jason Li has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training, including monitoring AML obligations and overseeing internal AML training and communication. The duties of the AML Compliance Person will include monitoring the firm’s compliance with AML obligations, overseeing communication and training for employees, and file any Suspicious Activity Reports(SARs). The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN)

when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

The firm will provide FINRA with contact information for the AML Compliance Person through the FINRA Contact System (FCS), including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). The firm will promptly notify FINRA of any change in this information through FCS and will review, and if necessary update, this information within 17 business days after the end of each calendar year.

The annual review of FCS information will be conducted by Jason Li and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, Jason Li will update the information promptly, but in any event not later than 30 days following the change.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310; FINRA Rule 4517.

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

o a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching 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 the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. We understand that we have 14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. We will designate through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, we are required to search those documents outlined in FinCEN's FAQ. If we find a match, MetaLoop 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), the AML Compliance Person will structure our search accordingly.

If the AML Compliance Person searches our records and does not find a matching account or transaction, then MetaLoop will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search by maintaining a log

showing the date of the request, the number of accounts searched, the name of the individual conducting the search and a notation of whether or not a match was found.

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. MetaLoop 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 federal 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, 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.

Rule: 31 C.F.R. § 1010.520.

- **b. National Security Letters**

We understand that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL by:

a) limiting access to the NSL to individuals authorized to handle the matter;
b) store the the subpoena in encrypted format;
c) limiting the knowledge and discussion of the NSL and its related matter to authorized members of the the internal compliance team and the management;
d) conduct regular training to ensure proper understanding of the internal protocol and regulatory requirements.

If we file a SAR after receiving an NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

- **c. Grand Jury Subpoenas**

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly

disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by:

e) limiting access to the subpoena to individuals authorized to handle the matter;
f) store the the subpoena in encrypted format;
g) limiting the knowledge and discussion of the subpoena and its related matter to authorized members of the the internal compliance team and the management;
h) conduct regular training to ensure proper understanding of the internal protocol and regulatory requirements.

If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

o d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

We will 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. MetaLoopwill ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. We will use the notice form found at FinCEN's website. Before we share 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 that FinCEN will make available. We understand that this requirement applies even to financial institutions *with which we are affiliated*, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both 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:

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

Rules: 31 C.F.R. § 1010.540.

o e. Joint Filing of SARs by Broker-Dealers and Other Financial Institutions

MetaLoop will not file joint SARs under any circumstances.

- **f. Sharing SARs With Parent Companies**

MetaLoop is not a subsidiary and does not have a parent company.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account or processing user transactions, and on an ongoing basis, MetaLoop will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur.

With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. MetaLoop will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated, and our compliance officer will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and file a rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Rules: 31 C.F.R. § 501.603; 31 C.F.R. § 501.604.

5. Customer Identification Program

Our CIP program should be interpreted in the context of on-ramp transaction processing where our customers purchase or sell cryptocurrency with MetaLoop.

In addition, as with other non-custodial wallet providers, MetaLoop does not have total independent control over any blockchain transactions that a wallet user may make and is therefore impossible to impose any blockchain transaction limits.

“Transaction limit” below refers to any fiat-to-crypto or crypto-to-fiat transactions.

- **a. Required Customer Information**

Prior to providing any fiat-to-crypto or crypto-to-fiat services, MetaLoop will collect the following information, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

Tier 1: Basic Information

Level 1 Account	Customer Identification Program	Transaction Limits

Personal Identity	Full name	$1000 per week in fiat-to-crypto transactions
	Email	
	Phone number	
	Date of birth	
	IP address geolocation	
Financial Identity	Card or bank account number	
	Billing address	
	Plaid provided bank account information (if applicable) including: ● personal information ○ name ○ address ○ phone number ○ email address ● account transactions ○ amount ○ date ○ type ○ description of the transaction ● account details ○ account name ○ account type ○ account and routing numbers ○ balance	

Tier 2: Full KYC

This tier is for users who wish to go above the total weekly limit of $1,000 in fiat-to-crypto transactions. Tier 2 account imposes the following additional requirements in addition to Tier 1 requirements.

Level 2 Account	**Customer Identification Program**	**Transaction Limits**
Personal Identity	Residential address	No hard limits for AML or BSA purposes. Additional transaction constraints may be imposed by
	Tax identification number (if applicable)	

Identity Document	Photo of the customer's passport or driver's license with facial recognition	MetaLoop's risk engine.

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will ask customer for further verification such as uploading required documents to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

Rule: 31 C.F.R. § 1023.220(a)(2)(i).

- **b. Customers Who Refuse to Provide Information**

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not or cease to provide any fiat-to-crypto or crypto-to-fiat services.

In either case, our AML Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN on a SAR.

- **c. Verifying Information**

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. MetaLoop will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. Based on different account risk profile, we will ask for further documentary submission and bio-metric submission such as face ID. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity if applicable:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source, government sanction list and data provider database

- Checking references with other financial institutions

- Obtaining a financial statement

We will use non-documentary methods of verification when:
(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
(2) the firm is unfamiliar with the documents the customer presents for identification verification;
(3) the customer and firm do not have face-to-face contact; and
(4) there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

Rule: 31 C.F.R. § 1023.220(a)(2)(ii).

- **d. Lack of Verification**

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify a customer's identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

Rule: 31 C.F.R. § 1023.220(a)(2)(iii).

- **e. Recordkeeping**

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date.

With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

Rule: 31 C.F.R. § 1023.220(a)(3).

- **f. Comparison with Government-Provided Lists of Terrorists**

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

Rule: 31 C.F.R. § 1023.220(a)(4).

- **g. Notice to Customers**

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law.

Rule: 31 C.F.R. § 1023.220(a)(5).

- **I. Reliance on Another Financial Institution for Identity Verification**

We will, under no circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

Rule: 31 C.F.R. § 1023.220(a)(6).

6. Corporate Customer Due Diligence Rule

In addition to the information collected under the written Customer Identification Program, FINRA Rules 2090 (Know Your Customer) and 2111 (Suitability) and the 4510 Series (Books and Records Requirements), and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts), 17a-3(a)(17) (Customer Accounts) and Regulation Best Interest, we have established, documented and maintained written policies and procedures reasonably designed to identify and verify beneficial owners of legal entity customers and comply with other aspects of the Customer Due Diligence (CDD) Rule. We will collect certain minimum CDD information from beneficial owners of legal entity customers. We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile. We will conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, maintain and update customer information.

a. Identification and Verification of Beneficial Owners

At the time of opening an account for a legal entity customer, MetaLoop INC will identify any individual that is a beneficial owner of the legal entity customer by identifying any individuals who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. The following information will be collected for each beneficial owner:

(1) the name;
(2) date of birth (for an individual);
(3) an address, which will be a residential or business street address (for an individual), or an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact

individual (for an individual who does not have a residential or business street address); and
(4) an identification number, which will be a Social Security number (for U.S. persons), or one or more of the following: a passport number and country of issuance, or other similar identification number, such as an alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).

For verification, we will describe any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration). We will also describe any non-documentary methods and the results of any measures undertaken.

b. Understanding the Nature and Purpose of Customer Relationships

We will understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile through the following methods

- The type of customer;
- The account or service being offered;
- The customer's income;
- The customer's net worth;
- The customer's domicile;
- The customer's principal occupation or business; and
- In the case of existing customers, the customer's history of activity.

c. Conducting Ongoing Monitoring to Identify and Report Suspicious Transactions

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed within Section 11 (Monitoring Accounts for Suspicious Activity).

[1] Beneficial owners and legal entity customers as defined by the CDD Rule.

7. Correspondent Accounts for Foreign Shell Banks

MetaLoop does not establish, maintain, administer or manage correspondent accounts for foreign banks.

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

11. Monitoring Accounts for Suspicious Activity

We will monitor account activities for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business.

MetaLoop runs configurable rulesets on all fiat-to-crypto and crypto-to-fiat transactions. Transactions which trigger the following rules are subject to denial or manual review:

1. **Postal codes** - numbers and higher risk postcodes associated with an account
2. **Linked/shared accounts** - attempts/linkages between accounts which look to be connected
3. **Deposit velocity (intra-hour and intra-day)** - deposits of an unusual number in certain time periods
4. **Unique linked account count** - linkages of an unusual number of unique external accounts to their MetaLoop account
5. **Total linked account count** - linkages of an unusual number of external accounts to their MetaLoop account.
6. **External fraud scores** - Customers who are scored as risky by our machine learning vendor(s)
7. **Proxy connection** - transacting from suspicious IP addresses

Customers who trigger the rules may be temporarily denied MetaLoop's on-ramp service or/and asked to provide additional documentation supporting their identity like a photo ID verification before they are allowed to transact.

MetaLoop continuously enhances its fraud risk triggers based on assessed risk and emerging trends.

The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed. Relevant information can include, but not be limited to, the following: Suspicious Activity/Transaction Reporting, Information Sharing, Letters for the purposes of the prevention and detection of crime, Blocked Transaction Reports, Recordkeeping, Customer Records and further informations adhere to MetaLoop INC AML policy.

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.

- **a. Emergency Notification to Law Enforcement by Telephone**

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use include FinCEN's Financial Institutions Hotline (866) 556-3974, to report transactions relating to terrorist activity). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR.

Although we are not required to, in cases where we have filed a SAR that may require immediate attention by the SEC, we may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. We understand that calling the SEC SAR Alert Message Line does not alleviate our obligations to file a SAR or notify an appropriate law enforcement authority.

Rule: 31 C.F.R. § 1023.320.

- **b. Red Flags**

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

- **c. Potential Red Flags in Customer Due Diligence and Interactions with Customers**

- The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is

inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.

- The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
- The customer refuses to identify a legitimate source of funds or the information provided is false, misleading or substantially incorrect.
- The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).
- The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
- The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
- The customer's background is questionable or differs from expectations based on business activities.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
- An account is opened by a politically exposed person (PEP),[9] particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company[10] beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.

- An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.[11]
- An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.[12]
- An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
- An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
- An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

d. Potential Red Flags in Money Movements

- The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
- The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
- The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
- Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.

- Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.

- The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.

- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.

- There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.

- Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

- The customer requests that certain payments be routed through nostro[14] or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.

- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

- A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).

- Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.

- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

e. Other Potential Red Flags

- The customer is reluctant to provide information needed to file reports to proceed with the transaction.

- The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.

- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.

- The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.

- The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.

- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.

- The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.

- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reasons.

- The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).

- A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.

- There is an unusual use of trust funds in business transactions or other financial activity.

o f. Responding to Red Flags and Suspicious Activity

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

12. Suspicious Transactions and BSA Reporting

o a. Filing a SAR

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving $5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

(1) 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;
(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
(3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
(4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. *See* Section 11 for contact numbers. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

We may file a voluntary 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 report suspicious transactions by completing a SAR, and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-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.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

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 disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, 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.

Rules: 31 C.F.R. § 1023.320; FINRA Rule 3310.

o b. Currency Transaction Reports

We will file with FinCEN CTRs for any on-ramp or off-ramp transactions that exceed $10,000. Also, we will treat multiple transactions involving convertible virtual currencies as a single transaction for purposes of determining 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 will use the BSA E-Filing System to file the supported CTR Form.

Rules: 31 C.F.R. §§ 1010.311, 1010.306, 1010.312.

13. AML Recordkeeping

o a. Responsibility for Required AML Records and SAR Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that SARs are filed as required.

In addition, as part of our AML program, our firm will create and maintain SARs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification *(See* Section 5 above) and funds transmittals. We will maintain SARs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods (*e.g.*, Exchange Act Rule 17a-4(a) requiring firms to preserve for a period of not less than six years, all records required to be retained by Exchange Act Rule 17a-3(a)(1)-(3), (a)(5), and (a)(21)-(22) and Exchange Act Rule 17a-4(e)(5) requiring firms to retain for six years account record information required pursuant to Exchange Act Rule 17a-3(a)(17)).

o b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Person will handle all subpoenas or other requests for SARs.

Rule: 31 C.F.R. § 1023.320(e).

14. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

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 maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

Rules: 31 CFR § 1023.210(b)(4); FINRA Rule 3310.

15. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Person.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R § 1023.210; FINRA Rule 3310.

16. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it.

Rules: 31 C.F.R. § 1023.210; FINRA Rule 3310.