Quarry Dynamics Inc.

Anti-Money Laundering / Know Your Customer Policy

1. **Company Policy**

   Quarry Dynamics Inc, along with its subsidiaries, (hereinafter collectively referred to as “the Company”) has established an Anti-Money Laundering (AML) and Know Your Customer/Client (KYC) compliance program as required by the Bank Secrecy Act (BSA), and the PCMLTFA and associated Regulations, 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 applicable requirements under the (BSA), PCMLTFA and its implementing regulations as well as the law and regulations of the countries we operate in.

   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/KYC policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and authorized body 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

2. **Person Designation and Duties**

The Company has designated a Compliance Officer as its AML/KYC Compliance Person, with full responsibility for the Company's AML/KYC program. The Compliance Officer has a working knowledge of the implementing regulations and is qualified by experience, knowledge, and training. The duties of the AML/KYC Compliance Person will include monitoring the Company's compliance with AML obligations, overseeing communication and training for employees, and any other duties decided by the director. The AML/KYC Compliance Person will also ensure that the Company keeps and maintains all the required AML records and will ensure that Suspicious Activity Reports (SARs)/ Suspicious Transaction Reports (STRs) are filed with the authorized body when appropriate. The AML/KYC Compliance Person is vested with full responsibility and authority to enforce the Company's AML/KYC program.

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

FinCEN Requests Under USA PATRIOT Act and FINTRAC Requests Under Anti-Terrorism Act

We will respond to a Financial Crimes Enforcement Network (FinCEN) or Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) request, concerning accounts and transactions 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 Request. We understand that we have 14 days (unless otherwise specified by the respective authorized body) from the transmission date of the request to respond to a Request.

If our AML/KYC Compliance Person searches our records and does not find a matching account or transaction, then our AML/KYC Compliance Person might not reply to the 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 a match was found.

We will not disclose the fact that an authorized body (FinCEN, FINTRAC) has requested or obtained information from us, except to the extent necessary to comply with the information request. The AML/KYC Compliance Person will review, maintain, and implement procedures to protect the security and confidentiality of requests from an authorized body (FinCEN, FINTRAC) similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley (GLB) Act and the AML/KYC Compliance Personal Information Protection and Electronic Documents Act (PIPEDA)with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the Request to the requesting law enforcement agency as designated in the request. Unless otherwise stated in the 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 Requests as a government provided a list of suspected terrorists for purposes of the customer identification and verification requirements.

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, RCMP or other federal government authority has sought or obtained access to any of our records. If we file a SAR/STR after receiving an NSL, the SAR/STR will not contain any reference to the receipt or existence of the NSL. The SAR/STR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

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)/Suspicious Transaction Report (STR). 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/STR in accordance with the SAR/STR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the AML/KYC Compliance Person who is the subject of the subpoena its existence, its contents, or the information we used to respond to it. If we file a SAR/STR after receiving a grand jury subpoena, the SAR/STR will not contain any reference to the receipt or existence of the subpoena. The SAR/STR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Voluntary Information Sharing

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 and will file all required notice to respective authorized authorities. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for the authorized body, by segregating it from the Company's other books and records. 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.

Sharing SAR/STRs With Parent Company

If a US Incorporated subsidiary files a SAR, we may share the SAR with our Canadian parent company, Quarry Dynamics Inc. and will have the appropriate confidentiality agreements in place. Since the parent company is a Canadian corporation, the confidentiality agreement will state that Quarry Dynamics Inc. may not disclose further any SAR/STR, or the fact that such report has been filed. The agreement will allow for Quarry Dynamics Inc. to disclose without permission underlying information (that is, information about the customers and transaction(s) reported) that forms the basis for the SAR/STR and that does not explicitly reveal that a SAR/STR was filed and that is not otherwise subject to disclosure restrictions.

3. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, the compliance officer 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 the OFAC, The Consolidated Canadian Autonomous Sanctions list and any other regulatory bodies are required. Because the 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. The compliance officer will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated, and the 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 the respective authorized body, we will reject the transaction and/or block the customer's assets

and file a blocked assets and/or rejected transaction form with authorized body within 10 days. We will pay special attention to the activities of a customer participating in a Transaction and to circumstances that refer to Money Laundering or Terrorist Financing, including to complex, high value or unusual Transactions, which do not have any reasonable economic purpose.

4. **Customer Identification Program – KYC (Know Your Customer/Know Your Client)**

In addition to the information, we must collect under the laws of the jurisdictions where the company operates, we have established, documented and maintained a written Customer Identification Program (CIP), hereinafter known as KYC. We will collect certain minimum customer identification information from each customer who opens an account for any of our projects; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide the required adequate KYC notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government or respective international authority.

a. Required Customer Information Prior to opening an account, the Company, 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:

(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), 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), or a principal place of business, local office, or other physical location (for a person other than an individual); and

(4) an identification number, which may be:

a) national or international ID (which must not expire within the next 3 months of the submission date);

b) a taxpayer identification number,

c) driver's license (national or international):

d) any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

(5) customer's contact telephone number and e-mail address;

(6) customer's Ethereum wallet address under which, in combination with the information collected above, we will be able to identify any of our customers and transactions they make within our projects.

(7) A questionnaire as well as documented evidence that an American or Canadian individual meets the criteria of accredited investor as defined by their country of residence.

(8) When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise (8) statutory documents; Where the total sum of outgoing payments relating to a transaction or a service contract exceeds 15,000 euros per calendar month and/or The AML/KYC Compliance Person is an e-resident or from a country outside the EEA or whose place of residence is in such a country, the customer can be identified by way of a digital identification system with assurance level "high" which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/20143, using an information technology means, which has a working camera, microphone, the hardware and software required for digital identification and an internet connection of adequate quality.

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 Company will not open a new account and, after considering the risks

involved, consider closing any existing account. In either case, our AML/KYC Compliance Person will be notified so that we can determine whether we should report the situation to FinCEN/FACTA on a SAR/STR.

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 identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The compliance officer will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means when appropriate documents are available. Considering 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 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/postal code, telephone number (if provided), date of birth and SSN/SIN, allow us to determine that we have a reasonable belief that we know the 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; and
- 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 identity.

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

- 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
- Checking references with other financial institutions; or
- 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 Company is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and Company do not have face-to-face contact; and

(4) there are other circumstances that increase the risk that the Company will be unable to verify the identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. 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 Company's AML/KYC Compliance Person, file a SAR/STR in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer's identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified.

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/STR in accordance with applicable laws and regulations.

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.

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 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 and other authorized body's rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers

We will provide notice to customers that the Company is requesting information from them to verify their identities, as required by law. We will use an online method of providing notice to customers.

h. Reliance on Another Financial Institution for Identity Verification.

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all the elements of our KYC 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:

- when such reliance is reasonable under the circumstances.
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements and is regulated by a functional regulator; and
- when the other financial institution has entered a contract with our Company requiring it to certify annually to us that it has implemented its anti-money laundering program

and that it will perform (or its agent will perform) specified requirements of the customer identification program.

5. Customer Due Diligence Rule

In addition to the information collected under the laws of governing authorities in the US and Canada, 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 as described above. 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, the compliance officer 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.

To establish Beneficial Ownership, the Company shall take the following actions and consider the following principles:

1) Gather information about the ownership and control structure based on information provided in pre-contractual negotiations or obtained from another reliable and independent source.

2) In situations, where no single person holds the interest or ascertained level of control to the extent of no less than 25 per cent, apply the principle of proportionality to establishing the circle of beneficiaries, which means asking information about persons, who control the operations of the legal person, or otherwise exercise dominant influence over the same;

3) If the documents used to identify a legal person, or other submitted documents do not clearly identify the Beneficial Owners, record the respective

information (i.e. whether the legal person is a part of a group, and the identifiable ownership and management structure of the group) on the basis of the statements made by the representative of the legal person, or a written document under the hand of the representative

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), a Social Insurance number (for Canadian persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, 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 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 legal methods.

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.

6. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern, or type of transactions, considering risk factors and red flags that are appropriate to our business. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML/KYC Compliance Person or his/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/KYC Compliance Person or his/ her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR/STR is filed. Relevant information can include, but not be limited to, the following:

1) The customer makes single and/or consecutive large transactions outside the schedule, if the amount of the single and/or combinations of (cash, electronic transaction or virtual currency) totaling $5,000 USD (for US persons) or exceeding $10,000 CAD (for Canadian persons) within a 24-hour window, where we know, suspect or have reason to suspect;
   (a) 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;
   (b) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the BSA regulations;
   (c) 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
   (d) the transaction involves the use of the Company to facilitate criminal activity.

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 we notify the appropriate law enforcement authority of any such activity, we must still file a timely SAR/STR.

b. Red Flags

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

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information that is false, misleading, or substantially incorrect.
- The background is questionable or differs from expectations based on business activities.
- The customer is publicly known or known to the Company 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.
- 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.

- 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
- Customer with no discernible reason for using the Company's service.
- Wire transfer activity, when viewed over a period, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions, or circuitous money movements.

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 Company's compliance with government reporting requirements and the Company's AML/KYC policies.
- The customer tries to persuade an employee not to file required reports or not to maintain the required records.

- Law enforcement has issued subpoenas or freeze letters regarding a customer or account
- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose

c. Responding to Red Flags and Suspicious Activity

When an employee of the Company detects any red flag, or other activity that may be suspicious, he or she will notify the AML/KYC Compliance Person and at least 1 C Level executive. Under the direction of the AML/KYC Compliance Person, the Company 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/STR.

7. Suspicious Transactions and Reporting

a. Filing a SAR/STR

We will file SARs with FinCEN for any transactions (cash, electronic transaction or virtual currency) conducted or attempted by, at or through the Company involving $5,000 (for US persons) or with FACTA for any transactions (cash, electronic transaction or virtual currency) conducted or attempted by, at or through the Company exceeding $10,000 CAD (for Canadian persons) within a 24 hour window, 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 law or regulation or to avoid any transaction reporting requirement under law or regulation;

(2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of BSA or PCMLTFA 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, the 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 Company to facilitate criminal activity.

We will also file a SAR/STR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

We may file a voluntary SAR/STR 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/STR rule. It is our policy that all SAR/STRs will be reported regularly to

Executive Leadership, with a clear reminder of the need to maintain the confidentiality of the SAR/STR.

We will report suspicious transactions by completing a SAR/STR, and we will collect and maintain supporting documentation as required by the authorized body regulations. We will file a SAR/STR-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/STR. If no suspect is identified on the date of initial detection, we may delay filing the SAR/STR 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/STR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

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

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by BSA or PCMLTFA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR/STR or the information contained in the SAR/STR will, except where disclosure is requested by FinCEN, FACTA, or another appropriate law enforcement or regulatory agency, decline to produce the SAR/STR or to provide any information that would disclose that a SAR/STR was prepared or filed. We will notify FinCEN/FACTA of any such request and our response.

8. AML Recordkeeping

a. Responsibility for Required AML Records and SAR/STR Filing

Our AML/KYC Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that SAR/STRs are filed as required.
In addition, as part of our AML/KYC program, our Company will create and maintain SAR/STRs and relevant documentation on customer identity and verification and funds transmittals. We will maintain SAR/STRs and their accompanying documentation for at least five years. We will keep other documents according to existing regulations and other recordkeeping requirements, including certain rules that require retention periods.

b. SAR/STR Maintenance and Confidentiality

We will hold SAR/STRs and any supporting documentation confidential. We will not inform anyone outside of FinCEN/FACTA or other appropriate law enforcement or regulatory agencies about a SAR/STR. We will refuse any subpoena requests for SAR/STRs or for information that would disclose that a SAR/STR has been prepared or filed and immediately notify FinCEN/FACTA of any such subpoena requests that we receive. We will segregate SAR/STR filings and copies of supporting documentation from other Company books and records to avoid disclosing SAR/STR filings. Our AML/KYC Compliance Person will handle all subpoenas or other requests for SAR/STRs. We may share information with another financial institution about suspicious transactions to determine whether we will jointly file a SAR/STR. In cases in which we file a joint SAR/STR 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/STR.

9. Company Relationships

We will work closely with the authorized body to detect money laundering. We will exchange information, records, data, and exception reports as necessary to comply with AML laws. The Company will have filed (and kept updated) the necessary annual certifications for such information. As a general matter, we will obtain and use the following exception reports offered by our authorized body to monitor customer activity and we will provide the authorized body with proper customer identification and due diligence information as

required to successfully monitor customer transactions. We have discussed how each Company will apportion customer and transaction functions and how we will share information and set forth our understanding in a written document. We understand that the apportionment of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the BSA and the PCMLTFA and its implementing regulations.

10. Training Programs

We will develop ongoing employee training under the leadership of the AML/KYC Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our Company'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 SAR/STRs); (3) what employees' roles are in the Company's compliance efforts and how to perform them; (4) the Company's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the regulations of the BSA and the PCMLTFA.
We will develop training in our Company, 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 AML/KYC Compliance 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.

11. Monitoring Employee Conduct and Accounts

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

performance of supervisors, as part of their annual performance review. The AML/KYC Compliance Person's accounts will be reviewed by the CFO or COO.

12. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the Company's AML/KYC Compliance Policy to the AML/KYC Compliance Person unless the violations implicate the AML/KYC Compliance Person, in which case the employee shall report to the CFO and COO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

13. Internal Review and Audit

The AML/KYC Compliance Officer is responsible for overseeing our AML/KYC Policy and presenting findings to our COO and other executives.

(a) Independent Annual Audit

Our AML/KYC Compliance Officer oversees the performance of an independent test of our AML/KYC Policy at least annually. Results are shared with the Managers.

14. Senior Manager Approval

Executive Leadership has approved this AML/KYC Compliance Policy in writing as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of the BSA, the PCMLTFA and the implementing regulations under it. This approval is indicated by signatures below.

Signed: 

Title: COO

Date:_July 25, 2022