AML/KYC POLICY

QUANTOCOIN™

AML - Policy

1. QUANTOCOIN (“QTC”) POLICY

It is the policy of Banque Duval & CIE LTD (“BD”) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. We will comply with the applicable requirements of Anti-Money Laundering/Counter-Terrorist Financing (“AML/CTF”) regulations, including, without limitation, the Money Laundering Regulations of 2007 (the “Regulations”) and the Terrorism Act 2000 (amended by the Anti-Terrorism, Crime and Security Act 2001).

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:

(i) 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 traveller’s checks, or deposited into accounts at financial institutions;

(ii) 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.

(iii) At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same 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/CFT policies, procedures and internal controls are designed to ensure compliance with all applicable regulations 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. AML/CFT COMPLIANCE PERSON DESIGNATION AND DUTIES

BD has a designated Money Laundering Reporting Officer ("MLRO"). The MLRO has full responsibility for the QTC Ecosystem, including the QTC Platform and the process of verification of participants in the QTC Token offerings organised by BC.

The duties of the MLRO will include monitoring each QTC offering for compliance with AML/CFT obligations, overseeing communication and training for employees and overseeing QTC's interaction with third-party vendors (such as with Verifyinvestor.com and/or Investready.com), where applicable. The MLRO will also ensure that BD keeps and maintains all of the required AML/CFT records and will ensure that any Suspicious Activity Reports ("SAR") generated by it or its third-party vendors are filed with, amongst other institutions, the UK Financial Intelligence Unit ("UKFIU"), when deemed by the MLRO appropriate to do so. The MLRO is vested with full responsibility and authority to enforce BD's AML/CFT program. BD will provide the company administrators, company secretary and associated financial institutions with contact information for the MLRO, including: (1) name; (2) title; (3) mailing address; (4) email address; and (5) telephone number. BD will promptly notify all parties of any change in this information and will review and update this information prior to the end of each calendar year.

3. PROVIDING AML/CFT INFORMATION THE AUTHORITIES IF REQUESTED

We will respond to a request from any authority over BD and its business (a "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 organisation named in the Request. We will designate one or more persons to be the point of contact ("POC") for Requests and will promptly update the POC information following any change in such information. Unless otherwise stated in the Request, we are required to search our files for each individual, entity or organisation named in the Request. If we find a match, the MLRO will consider any appropriate action. If the search parameters differ from searching through our entire database, for example, if limits to a geographic location apply, the MLRO will structure our search accordingly. If the MLRO searches our records and does not find a matching account or transaction, then the MLRO will not reply to the Request. We will maintain a register of Money Laundering and Financing of Terrorism Enquiries together with documentation that we have performed the required search by saving the logs, which will at all times be available on request. We will not disclose the fact that the authorities have requested or obtained information from us, except to the extent necessary to comply with the Request. The MLRO will review, maintain and implement procedures to protect the security and confidentiality of requests from the authorities with regard to the protection of customers' non-public information. We will direct any questions we have about the Request to the authorities. 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

Request as a government-provided a list of suspected terrorists for purposes of the customer identification and verification requirements.

4. LEVELS OF CDD

People who have opened an account need to provide their full contact details, prior to being allowed to participate in a QTC offering, or otherwise trade in QTC on the QTC Platform.

CUSTOMER DUE DILIGENCE ("CDD") AND KNOW YOUR CLIENT IDENTIFICATION PROGRAM ("KYC")

Whether on its own or through our third-party service providers (such as, without limitation, Verifyinvestor.com and/or Investready.com), BD will collect sufficient information from each customer who has opened an account to enable the customer to be identified. BD will: (i) utilise risk-based measures to verify the identity of each such customer, (ii) record CDD information and the verification methods and results, (ii) provide the required adequate CDD notice to customers that we will seek identification information to verify their identities; and (iv) compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

5. REQUIRED CUSTOMER INFORMATION

After opening an account, BD, directly or through its third-party service providers, will collect the following minimum information for all accounts, if applicable and as required by applicable laws and regulations, for any person, entity or organisation that is opening a new account and whose name is on the account prior to activating the account for deposits and withdrawals of FIAT currencies (deposits, trading and withdrawing digital currencies does not require CDD verification):

a. the name;

b. date and place of birth (for an individual);

c. nationality;

d. gender;

e. email;

f. phone number;

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

h. proof of identification with a photograph (selfie with passport in hand)

6. 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, QTC will deactivate the account and, after considering the risks involved, consider closing any existing account. In either case, our MLRO will be notified so that we can determine whether we should report the situation to the authorities.

7. VERIFYING INFORMATION

Based on the risk, and to the extent reasonable and practicable, we will either directly, or through a third-party service provider, 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. The MLRO will analyse the information obtained to determine whether the information is sufficient to form a reasonable belief to determine the true identity of the customer (e.g., whether the information is logical or contains inconsistencies). This process will involve the verification of customer identity through documentary means, non-documentary means or both, and documents will be used to verify customer identity when appropriate documents are available. In light of the increased instance of identity fraud, the use of documentary evidence will be supplanted by using the non-documentary means described below whenever necessary. Non-documentary means may also be utilised, if readily-available through commercially reasonable means, where uncertainty remains about whether the true identity of the customer is known. In verifying the information, consideration will be given as to whether the identifying information received (such as the customer's name, street address, postcode, email, telephone number, date of birth and photographic ID), allows a reasonable determination of the true identity of the customer (e.g., whether the information is logical or contains immediately apparent inconsistencies).

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

For an individual

a. Certified proof of identity (passport copy or provisional or full driving license or Government issued National Identity Card (picture page is sufficient))

b. Certified proof of residential address (utility bill* less than 3 months old or bank statement) *Electricity, gas, water, phone bill (not mobile phone)

For a Corporation

a. Certificate of Incorporation

b. Memorandum and articles of Association

c. Identify the Beneficial Owner

d. For at least 2 directors of a Corporation – proof of identity and proof of residential address

All of the above documents should be certified by either a lawyer, accountant, notary public or Consular Official at an Embassy or Consulate.

The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it and provide his contact details.

The certifier must state that it is a true copy of the original.

Any non-English documentation requires translation and certification as above.

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. We reserve the right to 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:

- Confirming the validity of email; and,
- Confirming the validity of telephone number.

We will verify the information within a reasonable time 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. 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 our MLRO, report the activity in accordance with applicable laws and regulations. We recognise that the risk that we may not know the customer's true 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 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. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient:

- Obtain verification of beneficial owners of corporations; and,
- Obtain additional references from financial institutions.

8. 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) deactivate the account or keep it in deactivated status; (2) close an

account after attempts to verify customer's identity fail; and (3) determine whether it is necessary to inform the FSC or UKFIU in accordance with applicable laws and regulations.

9. RECORDKEEPING

We will keep logs of 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 logs 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, unless a different period would be required or Customer made us of Its right to be "forgotten" as per the new General Data Protection Regulation (GDPR) (EU) 2016/679.

10. COMPARISON WITH GOVERNMENT-PROVIDED LISTS OF TERRORISTS

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

A. NOTICE TO CUSTOMERS

We will provide notice to customers that QTC is requesting information from them to verify their identities, as required by law. We will use the following method to provide notice to customers: Inform them by email and through the QTC Platform when the customer wants to activate their account for depositing and withdrawing FIAT currencies, by using the following text:

Important Information About Procedures for Activating a New Account

- To help the government fight the funding of terrorism and money laundering activities, QTC is required to obtain, verify, and record information that identifies each person who opens an account and wishes to deposit and withdraw FIAT currencies.

- What this means for you: When you would like to deposit and withdraw FIAT currencies, we will ask for your name, address, date of birth and other information that will allow us to identify you. We will also ask to see photographic proof of your identification and proof of address.

B. RELIANCE ON ANOTHER FINANCIAL INSTITUTION FOR IDENTITY VERIFICATION

We may, under the following circumstances, rely on the performance by another party (including an affiliate) of some or all of the elements of our CDD with respect to any customer that is opening an account or has established an account or similar business relationship with the other party to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances; and
- when the other party has entered into a contract with QTC requiring it to certify annually to us that it has implemented its anti-money laundering and counter terrorist financing program and that it will perform (or its agent will perform) specified requirements of the CDD program

11. GENERAL CUSTOMER DUE DILIGENCE

It is important to our AML and KYC reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may need to be enhanced. For each account meeting the following criteria and which could be deemed to be a higher risk:

- Corporations in off shore jurisdiction;
- Individuals from high-risk countries; and
- CDD documentation of questionable origin.

We will take steps to obtain sufficient customer information to comply with our enhanced due diligence requirements. Such information should include:

- Identification of beneficial owners of corporations;
- Reference from a financial institution; and,
- Proof of source of funds.

12. MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. The MLRO 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 MLRO or his or her designee will conduct an

appropriate investigation and review relevant information from internal or third-party sources before the authorities are notified.

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.

Red Flags

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

- 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 is false, misleading or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.
- Customer with no discernible reason for using QTC Platform.
- Efforts to Avoid Reporting and Recordkeeping
- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an employee not to file required reports or not to maintain required records.
- “Structures” deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Unusual concern with QTC’s compliance with government reporting requirements and QTC’s AML/CFT policies.
- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.
- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer’s business or history.
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.
- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account.

13. RESPONDING TO RED FLAGS AND SUSPICIOUS ACTIVITIES

When BD and/or any of its third-party service providers detects any red flag, or other activity that may be suspicious, he/she will notify the MLRO. Under the direction of the MLRO, QTC 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 informing the authorities.

14. SUSPICIOUS TRANSACTIONS REPORTING

Filing a report with the FSC or UKFIU

We will file a report with the authorities for any transactions (including deposits and transfers) conducted or attempted by, at or through QTC involving significant transactions (whether individually, or in the aggregate), as required under applicable law, where we know, suspect or have reason to suspect:

- 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;

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

- 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

- the transaction involves the use of QTC to facilitate criminal activity.

We will also file a report 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 report 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. It is our policy that all suspicious activities will be reported regularly to the senior management of BD.

Currency Transaction Reports

Unless otherwise specified and legally allowed, QTC only allows FIAT currency transactions once accounts are activated. Any transfers over a significant threshold (as determined under applicable law) may be reported to the authorities in line with applicable reporting requirements.

Currency Transportation

QTC prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us. QTC only accepts currency transactions through financial institutions and internationally recognised payment platforms.

15. AML/CFT RECORDKEEPING

Responsibility for Required AML Records

Our MLRO and his or her designee will be responsible for ensuring that AML/CFT records are maintained properly. In addition, as part of our AML/CFT program, QTC will create and maintain all relevant documentation on customer identity and verification and funds transmittals. We will maintain all documentation for at least five years.

AML/CFT Reporting Maintenance and Confidentiality

We will hold reports and any supporting documentation confidential and will comply fully with all applicable legislation, including, without limitation, the General Data Protection Regulation (GDPR) (EU) 2016/679.

We will not inform anyone outside of the authorities or other appropriate law enforcement or regulatory agency about a report. We will segregate report filings and copies of supporting documentation from other firm books and records to avoid disclosing

information. Our MLRO will handle all requests for reports. We may share information with another financial institution about suspicious transactions in order to determine whether we will jointly file a report according to the rules and regulations of the authorities. In cases in which we file a joint report for a transaction that has been handled both by us and another financial institution, both financial institutions will maintain a copy of the filed report.

Additional Records

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

- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds above a certain significant thresholder (as determined under applicable law);

- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person, regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, greater than such above-referenced threshold;

- Each document granting signature or trading authority over each customer's account;

- A record of each remittance or transfer of funds, or of currency to a person, account or place, greater than a certain threshold determined as significant by BD under applicable regulations; and

A record of each receipt of currency and of each transfer of funds which are deemed to be "significant" by BD, in consultation with the MLRO and/or a third-party service provider and subject to applicable regulations; where such transfer is received on any one occasion directly and not through a domestic financial institution, from any person, account or place.

16. TRAINING PROGRAMMES

We will develop ongoing employee training under the leadership of the MLRO 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 and/or the financing of terrorism 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 reports to the authorities; (3) what employees' roles are in QTC's compliance efforts and how to perform them; (4) QTC's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the FSC regulations. We will develop training in our firm, 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 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 specialised additional training. Our written procedures will be updated to reflect any such changes

17. PROGRAM TO INDEPENDENTLY TEST AML /CFT PROGRAM

a. Staffing

The testing of our AML/CFT program will be performed at least annually (on a calendar year basis) by the testing officer, personnel of QTC, who is not the MLRO nor does he perform the AML/CFT functions being tested nor does he report to any such persons. His qualifications include a working knowledge of applicable requirements under the FSC rules and regulations. To ensure that he remains independent, we will separate his functions from other AML/CFT activities. Independent testing will be performed more frequently if circumstances warrant.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to an internal audit committee. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved

18. MONITORING EMPLOYEE CONDUCT AND ACCOUNTS

We will subject employee accounts to the same AML/CFT procedures as customer accounts, under the supervision of the MLRO. We will also review the AML/CFT performance of supervisors, as part of their annual performance review. The MLRO's accounts will be reviewed by the testing officer.

19. CONFIDENTIAL REPORTING OF AML/CFT NON-COMPLIANCE

Employees will promptly report any potential violations of QTC's AML/CFT compliance program to the MLRO, unless the violations implicate the MLRO, in which case the employee shall report to the testing officer. Such reports will be confidential, and the employee will suffer no retaliation for making them.

QTC has reviewed all areas of its business to identify potential money laundering and/or financing of terrorism risks that may not be covered in the procedures described above. The major additional areas of risk include future changes to regulations and hacking attempts on QTC's servers. Additional procedures to address these major risks are maintaining constant contact with the FSC and performing daily security checks on QTC's server security procedures, performed by a dedicated server security specialist.

20. ADDITIONAL RISK AREAS

BD has reviewed all areas of its business to identify potential money laundering and/or financing of terrorism risks that may not be covered in the procedures described above. The major additional areas of risk include future changes to regulations and hacking attempts on QTC servers and the QTC Platform. Additional procedures to address these major risks are maintaining constant contact with the FSC and performing daily security checks on QTC's server security procedures, performed by a dedicated server security specialist.

21. SENIOR MANAGER APPROVAL

Senior management has approved this AML/CFT compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the FSC and the implementing regulations under it. This approval is indicated by signatures below.