# ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

## AMLP1 INTRODUCTION

All employees of General Reserve of Digital Assets Limited ("GRDA") are required to comply with the policies and procedures set out in this AML Policy. When conducting fiduciary activities, reference should be made to relevant requirements stipulated in Hong Kong Ordinance Cap 615 Anti-Money Laundering and Counter Terrorist Financing Ordinance (the "AMLO").

## AMLP2 SENIOR MANAGEMENT OVERSIGHT

Senior management of GRDA should:

- be satisfied that GRDA's Anti-Money Laundering ("AML")/Counter Terrorist Financing ("CTF") systems are capable of addressing its money laundering ("ML") / terrorist financing ("TF") risks;
- appoint a director or senior manager as a Compliance Officer ("CO") who has overall responsibility for the establishment and maintenance of GRDA's AML/CFT systems; and
- appoint a senior staff as GRDA's Money Laundering Reporting Officer ("MLRO") who is the central reference point for suspicious transaction reporting.

## AMLP3 RISK ASSESSMENT AND CLIENT ACCEPTANCE

Compliance Department should assess the ML/TF risks of GRDA's clients by assigning a ML/TF risk rating to each client. It should also record its work done on a Risk Assessment Form to demonstrate (i) how the client's ML/TF risk is assessed; and (ii) the extent of Customer Due Diligence ("CDD") and ongoing monitoring that is appropriate for the client. Relevant factors to be considered by Compliance in the assessment process include the following:

### *Country Risk*

Whether the client resides in or is connected with high- risk jurisdictions for example:

- those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies (e.g. Iran, the Democratic People's Republic of Korea ("DPRK"), etc);
- countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (e.g. Afghanistan, Sudan, etc);
- countries which are vulnerable to corruption (e.g. DPRK, the Philippines, etc); or
- those countries that are believed to have strong links to terrorist activities (e.g. Iraq, Afghanistan, etc).

### *Customer Risk*

Where the client is of such a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it or the business/ industrial sector to which a client has business connections is more vulnerable to corruption. The following types of clients, by their nature or behavior, might also present a higher risk of ML/TF:

- Politically Exposed Persons ("PEPs") and/or any individuals connected with them.

A PEP is defined in the AMLO as:

(a) an individual who is or has been entrusted with a prominent public function in a place outside or within the People's Republic of China and
   i. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
   ii. but does not include a middle-ranking or more junior official of any of the categories mentioned in section (i) above.

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) PEP's close associate which is defined as:
   i. an individual who has close business relations with a person falling under section (a) above, including an individual who is a beneficial owner of a legal person or trust of which the person falling under section (a) is also a beneficial owner; or
   ii. an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under section (a) above.

- Corporate clients that use complex corporate structures, trusts or use nominee and bearer shares where there is no legitimate commercial rationale to do so;
- Clients who request to use numbered accounts or undue levels of secrecy with a transaction;
- Clients who are involved in cash-intensive businesses (e.g. casinos, money-changers, etc);
- Clients whose origin of wealth or ownership cannot be easily verified.

***Product/ Service Risk***

The characteristics of the products and services that GRDA offers and the extent to which they are vulnerable to ML/TF abuse should be considered. The risks of new products/ services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes) should therefore be assessed before they are introduced to clients, and appropriate additional measures and controls should also be implemented to mitigate and manage their associated ML/TF risks.

***Delivery/ Distribution Channel Risk***

The delivery/distribution channels (including business through internet, postal or telephone channels where a non-face-to-face account opening approach is used) and the extent to which the products and services that GRDA offers are vulnerable to ML/TF abuse should be considered. Business referred by intermediaries may also increase risk as the business relationships between the clients and GRDA become indirect.

Senior management approval is required for opening of accounts for clients associated with risky attributes. No business relationship can be established or continued with a client ascertained to be of absolute risk of money laundering and/or terrorist financing and appear on a published list of money launderers/ suspected terrorists. Compliance Departments are responsible for conducting AML checks on account applicants and related parties (e.g. beneficiary owners) before opening a client account.

## AMLP4
## SUSPICIOUS TRANSACTION REPORT ("STR")

Transactions or incidents which are identified/noted by any staff/Licensed Person of GRDA as unusual and are suspicious of ML/TF should be escalated to the MLRO. Upon receipt of an internal STR, the MLRO will provide a receipt acknowledgement to the reporter and remind him/her of his/her obligation not to tip-off the client(s) involved.

The MLRO is responsible to justify whether the transaction/ incident provides grounds for knowledge or suspicion of ML/TF, and should file a STR to the Joint Financial Intelligence Unit (the " JFIU") as soon as it is reasonable to do so if the internal STR is justified.

Under no circumstances should reports raised by any staff/Licensed Person be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/ compliance function.

Examples of unusual/ suspicious transactions are listed below:

- transactions that have no apparent economic or lawful purpose, or not in line with the Licensed Person' knowledge of the client;
- transactions that are inconsistent in amount, origin, destination, or type with a client's known, legitimate business or personal activities;
- transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
- transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
- where the transaction being requested by the client, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular client;
- where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
- where the client refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;
- where a client who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
- the extensive use of trusts or offshore structures in circumstances where the client's needs are inconsistent with the use of such services;
- transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the client's declared business dealings or interests; and
- unnecessary routing of funds or other property from/to third parties or through third party accounts.
- where a client fails to complete the identification and verification process.

The law requires the STR to be submitted to the JFIU together with any matter on which the knowledge or suspicion is based. The need for prompt reporting is especially important where a client has instructed GRDA to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, consideration may be given to contact the JFIU urgently.

Once a staff/Licensed Person has reported his/her suspicion to the MLRO, he/she has fully discharged his/her reporting obligation under the AMLO.

The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU. All staff and Licensed Person should note that tipping off is a criminal offense since it involves disclosure to any person information which might prejudice an investigation. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

However, at times when a Client Service Department/Compliance Department/Senior Management is examining suspicious transactions and need to ask the related client(s) questions which, based on common sense, a reasonable person would ask in the circumstances, such enquires, when conducted properly and in good faith, do not constitute tipping off. However, the enquiries made and the responses obtained from the client(s) should be properly documented and should be available to assist the RAs, other authorities and auditors.

## AMLP5
## RECORD RETENTION

Client, transaction and other records that are necessary and sufficient to meet the record-keeping requirements under the AMRO should be properly maintained, to ensure that:

- the audit trail for funds moving through GRDA that relates to any client and, where appropriate, the beneficial owner of the client, account or transaction is clear and complete;
- any client and, where appropriate, the beneficial owner of the client can be properly identified and verified;
- all client and transaction records and information are available on a timely basis to RAs, other authorities and auditors upon request; and
- proper records of client risk assessment, registers of suspicious transaction reports (including records of internal and external STRs) and training records are retained.

Where client identification and verification documents and records are held by a Specified Intermediary (Note) which is not an FI ("Non-FI Intermediary"), an undertaking should also be obtained from the Non-FI Intermediary that it will supply copies of all underlying CDD information to GRDA in circumstances where it is about to cease trading, or does not act as an intermediary for GRDA anymore. If GRDA has doubts on the CDD measures previously carried out by the Non-FI Intermediary, it should perform the required CDD as soon as reasonably practicable.

Note: Specified Intermediary is defined in die AMLO as:

- any of the following persons who is able to satisfy the financial institution that they have adequate procedures in place to prevent money laundering and terrorist financing -
  (a) a solicitor practicing in Hong Kong;
  (b) a certified public accountant practicing in Hong Kong;
  (c) a current member of The Hong Kong Institute of Chartered Securities practicing in Hong Kong;
  (d) a trust company registered under Part VIII of the Trustee Ordinance (Cap. 29) carrying on trust business in Hong Kong;
- a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker; or
- a lawyer, a notary public, an auditor, a professional accountant, a trust or company service provider or a tax advisor practicing in an equivalent jurisdiction, or a trust company carrying on trust business in an equivalent jurisdiction, or an institution that carries on in an equivalent

jurisdiction a business similar to that carried on by a financial institution mentioned in paragraph above, that -

(a) is required under the law of that jurisdiction to be registered or licensed or is regulated under the law of that jurisdiction;
(b) has measures in place to ensure compliance with requirements similar to those imposed under this Schedule; and
(c) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities.

**Record retention requirements**

| | |
|---|---|
| Records of transactions, data and information obtained in connection with the transaction | 6 Years after completion of a transaction (or longer if so specified) |
| Records on client identification, account files (include risk assessments of clients) and business correspondence | 6 Years after end of business relationship (or longer if so specified) |
| Original or copy of the documents, and a record of the data and information, obtained in connection with the transaction, which should be sufficient to permit reconstruction of individual transaction and establish a financial profile of any suspect account or client | 6 Years after completion of a transaction (or longer if so specified) |
| Where client identification and verification documents are held by an intermediary on which GRDA is relying to carry out CDD measures, the documents and records from that intermediary | 6 years (beginning on the date on which the transaction is completed) |