RichGold

AML&CTF

1、PERIODICITY

Rich Gold Group Limited ("LBL"or "the Firm") is committed to the highest standards of Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) and other punishable criminal acts. The members of the Board and all employees are required to comply with these standards to protect LBL and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.

2、SCOPE

This Anti-Money Laundering & Counter Terrorism Financing Policy ("the Policy") sets out the requirements and supervisory perspective from relevant regulators ensuring that we have adequate policies and processes in place to identify, measure, assess, monitor, report and control and/or mitigate our risks in relation to money laundering and terrorism financing.

Rich Gold Group Limited have written this policy with the commitment of the Board of Directors to establish and put in place best sustainable practices in risk management. In preparing this policy, appropriate attention has been given to local and international regulatory environment, namely:

– Anti-Money Laundering Regulations 2008 (AMLR),
– Financial Action Task Force (FATF) (40+9 Recommendations)
– Anti-Money Laundering and Terrorist Financing Code of Practice, 2008 and;
– The requirements for better risk management practices as issued by the local regulator the Australian Securities and Investment Commission ("ASIC").

This policy is applicable to all LBL employees and any other persons engaged under a contract of service by the Firm. Failure to abide by the Policy set by the Firm to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as gross misconduct. Such cases will be referred to Human Resources (HR) for onward initiation of disciplinary

action that could lead to termination of employment and could also result in criminal prosecution and imprisonment for the concerned individual

3、OBJECTIVE

The objectives of this Policy are to:

• Ensure that the products and services of LBL are not used to launder the proceeds of crime and that all employees of LBL are aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing.
• Provide a consistent approach across the firm to the deterrence and detection of those suspected of laundering the proceeds of crime or those involved in the funding or execution of terrorism, and the disclosure to the relevant authorities
• Explain clearly the responsibility of the Board of Directors, Senior Management team, the Money Laundering Reporting Officer (MLRO) and other key colleagues

• Establish requirements for effective implementation and monitoring of compliance with this Policy.

4、DEFINITIONS

4.1.Money Laundering

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate sources through a series of transactions, so that they appear to be the proceeds from legal activities.

4.2.Terrorism Financing

Terrorism financing refers to the use of funds, or the making of available funds for the purposes of terrorism; or the acquisition, possession, concealment, conversion or transfer of funds (directly or indirectly) that will in turn be used or made available for such purposes.

It can be defined as the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

4.3.Stages of Money Laundering

Money laundering can be a diverse and often complex process. The first step in the laundering process by the criminal is to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. The funds can further be transferred to other accounts, locally or internationally or used to buy other goods or services. It eventually appears to be like legally earned money and becomes difficult to trace back to its criminal origin. The criminals can then invest or spend it or, as is often the case, use it to fund more crime/s. The laundering process is often described in three mainstages:

1. Placement
2. Layering
3. Integration

4.3.1.Placement

It is the first stage of money laundering where the 'dirty' cash or proceeds of crime enter into the financial system. There are numerous placement techniques, including the following but not limited to:
– Smurfing (or'Structuring') is a method in which small amounts of illegal cash are deposited into account(s) to avoid regulatory requirements of reporting cash transactions.

– Alternative Remittance System refers to any system used for transferring money from one location to another, and generally operating outside the banking channels.
– Electronic Fund Transfers (EFT) involve the transfer of money into and out of domestic and offshore bank accounts of fictitious individuals and shell companies.
– Asset Conversion involves the purchase of assets, such as real estate, diamonds, gold and vehicles which can then be sold and proceeds can be deposited in the account.
– Bulk Movement involves the physical transportation and smuggling of cash and monetary instrument/s such as money orders and cheques.
– Securities Dealing are illegal funds are placed with securities firm which are used for buying bearer securities and other easily transferable instruments.

4.3.2.Layering

Layering is the second stage of money laundering which involves the separation of proceeds of crime from their illegal source by using multiple complex methods to conceal the illegal origin. There are numerous techniques and institutions that facilitate layering, including the following:
– Offshore Banks accept deposits in current, savings and deposit accounts from non- resident companies, businesses with no statutory reporting requirement, thus no control on the flow of money. Without some form of control, the authorities will never be able to detect money laundering activities.
– Shell Corporation is a company that is formally established under applicable corporate laws, but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold accounts and assets to disguise their actual ownership.
– Trusts are also another example of legal arrangements set up to falsify the origin and trail of illegally gained funds. Money launderers set up offshore trust accounts and appoint irrelevant personal to head the trust, making them the trustee for the funds. The trustee in turn provides the organized crime syndicate instant access to the funds.
– Walking Accounts is where the funds are continually on the move, evading the authorities. A deposit is placed into an initial offshore account, with the instruction of an immediate transfer to another account(s). By setting up a series of walking accounts, criminals can automatically create several layers once a fund transfer occurs.
– Intermediaries is when professionals, i.e. lawyers, accountants, stock brokers, bankers and such engage in transactions on behalf of a criminal client who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.

4.3.3.Integration

Integration is the final stage of money laundering process in which the illegal funds are converted into legitimate funds. There are various integration techniques, including the following:

- Import /Export transactions is to bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well
- Business recycling involve legitimate businesses' serving as conduits for money laundering. Cash-intensive retail businesses, real estate, jewelers and restaurants are some of the most traditional methods of laundering money. This technique combines the different stages of the money laundering process.
- Asset sales & purchases is the technique which can be used directly by the criminal or in combination with shell corporations, corporate financings and other advanced means. The end result is that the criminal can treat the earnings from the transaction as legitimate profits from the sale of the real estate or other assets.
- Credit Cards are an efficient way for launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence.
- Debit Cards individuals first transfer illegal funds into an offshore account and also signs up for a debit card from the bank to utilize the funds.
- Corporate Financings are typically combined with a number of other techniques, including use of offshore banks, electronic funds transfers and shell corporations.

The three basic stages often overlap and in some cases there is even no requirement for the proceeds of crime to be 'placed'.

5.POLICY STATEMENT

The AML Policy and Procedures adopted by LBL are established in compliance with the AML Regulations 2008. The Firm aims to prevent and take measures to guard against being used as a medium for money laundering and terrorism financing activities and any other activity that facilitates money laundering or the funding of terrorist or criminal activities.

The AML/CTF Policy sets out the following minimum standards which must be complied with by the Firm:

- The Firm will establish and maintain risk-based customer due diligence, identification, verification and know your customer (KYC) procedures, including enhanced due diligence for those customers presenting higher risk, such as Politically Exposed Persons (PEPs).
- A Risk Based Approach (RBA) towards assessing and managing the money laundering and terrorist financing risks will be established and maintained.
- Risk based systems and procedures will be established to monitor ongoing customer activity.
- All staff and any individual/corporation engaged under a contract of service by the Firm shall fully comply with both the letter and the spirit of regulatory requirements and act as required by the highest standard of market conduct.
- The Firm will appoint a Money Laundering Reporting Officer (MLRO) with a responsibility for the oversight of the Firm's compliance with relevant legislation,

regulations and rules.
• The Firm will implement effective communication of all policies and procedures to raise awareness for all employees on AML/CTF issues.
• The Firm will retain the appropriate records of customer transactions for a period of at least five years, as required under AMLR 2008.
• The Firm will not continue its established relationships with customers whose conduct gives rise to suspicion of or involvement with illegal activities.
• The Firm will fully cooperate with law enforcement and regulatory authorities as required.

6.MANAGEMENT AND CONTROLS OF AML &CTF RISK

6.1.Risk Assessment

An entity shall carry out money laundering and terrorist financing risk assessments in relation to each customer, business relationship or one-off transaction in order:

• to determine the existence of any risks;
• to determine how best to manage and mitigate any identified risks;
• to develop, establish and maintain appropriate anti-money laundering and terrorist financing systems and controls to effectively respond to the identified risks; and
• to ensure that at all times there is full compliance with the requirements of the AMLR (2008) and other enactments, policies, codes, practice directions and directives mentioned above in
relation to anti-money laundering and terrorist financing activities.

A risk assessment should be proportionate to:

• the nature, size and complexity of the business, taking into account agent relationships and the range of financial products and services being offered;
• the type of products and services offered, and the extent to which the products and services offered are consistently below a given threshold;
• customers' characteristics based on developed risk profiles, including the level of customer diversity across different geographical locations;
• the conditions of the proposed transactions;
• the distribution channels

A risk-based approach assists the measurement of risks for potential laundering of illegally gained funds, identification of the risks and the appropriate means and methods for mitigating and controlling those risks. With the aim of preventing any transactions to laundering of proceeds of crime and financing of terrorism, LBL sets and develops adequate procedures in relation to monitoring the customers' transactions, related reporting, retention of records, organization of the training and internal auditing activities.

6.2.Controls

In order to prevent the laundering of proceeds of crime and financing of terrorism,

the LBL carries out a monitoring and control process in relation to:

- High-risk customers and transactions (e.g. checking the customers regularly in Blacklist provided by the Payment Service Providers we collaborate with),
- Transactions with the risky countries,
- Complex and unusual transactions,
- Transactions inconsistent with the customer's business, source of funds and profile,

The LBL carries out the following activities for monitoring of the customer services provided and transactions intermediated by the LBL.

Inquiries are carried out by:

- A Client Administration Tool (CAT) integrated with World Check (a world renowned risk intelligence system providing assistance on KYC/AML/CTF/Sanctions and frequently updated specially designated nationals lists, etc.)
- Media screening
- During account opening a customer due diligence checklist is followed for both individual and corporate customers including (but not limited to) the following:
- At least one valid government issued photo ID (e.g. a national ID or a passport or a driver's license)
- Proof of address (e.g. a utility bill or equivalent dated within the last 3 months)
- Regular KYC reviews of the existing customers are conducted depending on their risk classifications
- In case of customers' deposits and withdrawals, the Firm implements the following requirements:
- In case of bank transfer or transfer from a bank card, the name, shown during the registration must match the name of the owner of the account/bank card.
- Withdrawing funds from the trading account via the method, which is different from the depositing method, is possible solely after withdrawing the sum, which is equal to the sum of client's deposits via the method and to the same account used for depositing.
- If the account was credited in the way that cannot be used for funds withdrawal, the funds may be withdrawn to a bank account of the client or any other way may be used, as agreed with the Firm with the help of which the Firm is able to prove the identity of the account owner.
- If the account has been credited with funds through various payment systems, funds withdrawal shall be made on a pro rata basis proportionate to the size of each deposit.
- In case of depositing via Visa/MasterCard, Wire Transfer, e-Payments, the withdrawal of funds, which exceed the sum of the client's deposits, is possible via any of the following methods:
  - Visa/MasterCard,
  - Wire Transfer,
  - E-Payments
- In case of depositing via another method, the withdrawal of funds that exceed the sum of the client's deposits, is possible via any available method, by the client's

choice.

6.3.Customer Due Diligence（CDD）

The Customer Due Diligence information, as stated by the International Compliance Association （ICA), contains the facts about the prospective customer enabling the Firm to assess the extent to which the customer exposes it to a range of risks. Thus, the Firm needs to

–

6.3.1,Levels of Due Diligence

a.Simplified due diligence

Simplified due diligence is the minimum level of due diligence completed on a customer where you determine that the business relationship or transaction presents a low risk of money laundering or terrorist financing.

b.Standard Due Diligence

Standard CDD covers identifying the client, understanding the ownership and control structure and verifying the client's identity. It is required in relation to all clients and beneficial owners where neither simplified CDD nor enhanced CDD applies.

c.Enhanced due diligence(EDD)

Enhanced Due Diligence is applied in situations where the money-laundering risk associated with the business relationship is increased. These situations might include, but are not limited to:

- Customers linked to high-risk countries or business sectors; or
- Customers having unnecessarily complex ownership structures;
- Customers undertaking unusual transactions, with no evident economic or lawful purpose
- Customers who are or having close links, i.e. business partner, relative, etc., to Political Exposed Persons (PEPs)

In implementing EDD, firms gain a greater understanding of the customer(s) and the associated risk than standard due diligence. It provides more certainty that the customer and/or beneficial owner is who they claim they are and that the purposes of the business relationship are legitimate.

The examples of EDD process include, but not limited to:

- obtaining more information about the customer's or beneficial owner's business
- obtaining more robust verification of the beneficial owner's identity based on information from a reliable and independent source

- gaining a better understanding of the customer's or beneficial owner's reputation and/or role in public life and assessing how this affects the level of risk associated with the business relationship
- carrying out searches on a corporate customer's directors or other individuals exercising control to understand whether their business or integrity affects the level of risk associated with the business relationship.

The Firm can decide on the degree of EDD applied depending on the reason why the customer has been classified as 'High Risk'.

6.4 Ongoing Monitoring

Under AMLR (2008) Regulation 19, the Firm is required to conduct ongoing monitoring of the business relationships with clients on a risk-sensitive and appropriate basis. The requirement is to maintain scrutiny of transactions undertaken by the clients to ensure that the transactions are consistent with what we know of the client and the client's business and resources
Thus, the Firm shall consider the following while conducting ongoing monitoring of a business relationship which includes but not limited to:

- The knowledge of the individual (e.g. the source of the client's funds, type of business, source of wealth)
- The customer's risk profile (e.g. geography risk, product risk, etc.)

Whenever ongoing monitoring gives rise to any suspicions of money laundering, promptly report them to the MLRO.

6.5. Training

Consistent with the training obligations defined in the AMLR (2008), the Firm should provide adequate training for its staff;

- ensuring that they receive appropriate and proportionate training to the level required by the Anti-money Laundering Regulations, 2008 in relation to money laundering and terrorist financing; and
- ensuring appropriate periodic training to be given to all key staff, including front office staff, temporary and contract employees acting as third party;
- That is designed to test employee knowledge and understanding of the laws, policies and procedures, including the internal controls systems of the entity or professional, relating to AML/CFT on a periodic basis.

Depending on the new releases within regulatory environment, the MLRO should update the training material and provide additional training to the related key staff.

Records of all training activity, including completion and pass rates where applicable are maintained and retained in compliance for a period of 5 years.

– Receive and consider AML/CTF reports
– Review reportable breaches of the AML/CTF

– The Board charges the Audit & Risk Committee with the responsibility of ensuring there are adequate resources, processes and systems in place to enable this Policy function as intended.
– Ensure that the MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable her/him to carry out that responsibility. is responsible for;
– Overseeing operational risks with a concentration on regulatory risk, compliance risk and legal risk
– Reviewing the AML/CTF Program and AML/CTF reports and make recommendations to the Board
– Receiving and reviewing reports from management concerning AML/CTF, and may also make recommendations as to strategies, policies and processes for AML/CTF
– Monitor LBL's AML/CTF performance and compliance with the AML/CTF Program
– Review breach reporting of the AML/CTF Program and action as it deems fit. are responsible for;
– Ensuring adequate funding is dedicated to the operation of the risk management framework and as such, to the AML/CTF Policy.
– Assigning responsibilities to ensure the effective management of the identified money laundering/ terrorist financing risks
– Assuring that all parts of the organization comply with the AML/CTF Policy and Program
– Promoting AML/CTF awareness within the Firm to so that its cause and processes and procedures that flow becomes embedded throughout the organization is responsible for:
– Identifying the risks that the Firm confronts and providing advisory to the Senior Management
– Day-to-day oversight of the AML/CTF Program
– Providing periodical reporting, including reporting of non-compliance to the Board, Audit & Risk Committee and Managing Directors
– Acting as the contact officer for issues such as reporting suspicious matters, urgent reporting, compliance audits, Suspicious Activity Reports (SARs) or requests for information or documents to provide to third parties.
– Contributing to designing, implementing and maintaining internal AML/CTF compliance manuals, policies, procedures and systems and develop them in line with evolving regulatory framework
– Providing awareness throughout the Firm about key AML/CTF issues and AML/CTF techniques
– Ensuring that staff are adequately trained in money laundering prevention, i.e. their legal and regulatory responsibilities and their role in handling money laundering/terrorism financing and risk management.
– Carrying out regular assessments of the adequacy of the Firm's systems and controls to ensure that money laundering risks is managed effectively and advising the business on those systems and controls
– Representing the Firm to all external agencies such as Australian Financial Investigation Agency (FIA) and any other third party enquiries in relation to money laundering prevention or compliance.

7. Staff

All staff is expected to manage AML/CTF risk in their area of activity through adherence to delegated responsibilities and AML/CTF processes and procedures and by bringing to the immediate attention to the Money Laundering Office any factors identified that could place the Firm and its obligations with respect to AML/CTF at risk. All staff must:

– Remain vigilant to the possibility of money laundering/ terrorist financing.
– Comply fully with all money laundering/ terrorist financing procedures in respect of customer identification, account monitoring, record keeping, reporting and training.
– Promptly report to the MLRO where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether they are engaged in AML / CTF monitoring activities.
– Ensure that the customer is not disclosed any information related to any inquiry or filing of a SAR - Bear in mind that individuals who violate the Firm's AML/CTF policies, processes and procedures will be subject to disciplinary action.
– Be wary in not to offer, promise or provide, or to request, agree to receive, or accept any gift or entertainment to induce any customer or third party
– Avoid personal conflicts, e.g. personal account dealings

8.INDEPENDENT AUDIT FUNCTION

Every entity and professional shall establish and maintain an independent audit function that is adequately resourced to test compliance, including sample testing, with its or his written system of internal controls and the other provisions of the AMLR 2008.

LBL is committed to conduct an independent review of its AML/CTF Policy, procedures and processes. The firm's Independent Audit Function will assess the following:

- The effectiveness of this AML/CTF Policy
- Whether this AML/CTF Policy complies with the AML/CTF Rules
- Whether this AML/CTF Policy has been effectively implemented
- Whether LBL has complied with this AML/CTF Policy

Following the audit, a report regarding the results of the evaluation will be written and submitted to the Board and Audit & Risk Committee. Based on the findings on the audit report, the Board and Audit & Risk Committee will ensure that all deficiencies detected are properly addressed and redressed. The required actions to be complete the deficiencies will also be reported to the Board and Audit & Risk Committee once

9.RECORD RETENTION

The Firm shall keep business records, including records of all transactions with customers and records which enable the ASIC to monitor the compliance of the Firm

with its regulatory obligations.
All records must be readily retrievable in the Australia and must not be kept in a country where access to the records may be impeded by confidentiality or data protection restrictions. All records must be kept for at least 5 years.

10.REPORTING OF SUSPICIOUS ACTIVITY REPORTS(SARs)

The Firm must ensure that all employees (including temporary and contract employees) are aware of their personal obligations under the Proceeds of Crime Act (PCCA) 1997, to promptly report to the respective MLRO where they have knowledge or suspicion, or reasonable grounds to know or suspect money laundering or terrorist financing.

An employee who pinpoints suspicious activity or transaction must not inform the customer or any other individual regarding the existence or decision of filing a Suspicious Activity Report (SAR). "Tipping-off" a customer is a criminal offence.

The MLRO receives any internal reports and is the responsible to report to the Australian Financial Investigation Agency if he/she considers a suspicious activity report is deemed appropriate.

Below are the examples where customer identification issues have potential to indicate suspicious activity:

- The customer refuses or appears reluctant to provide information requested;
- There appears to be inconsistencies in the information provided by the customer;
- An address appears vague or unusual or, in relation to a known customer, changes frequently;
- The supporting documentation does not add validity to the other information provided by the customer;
- The customer is rushing a transaction through with promises to provide the required identification details later.

Below are the examples of activity that might suggest there could be potential terrorist activity:

- The customer is unable to satisfactorily explain the source of income or provides contradictory statements that raises doubt about his/her integrity;
- The customer's address changes frequently; and

Media reports on suspected or arrested terrorists or groups.