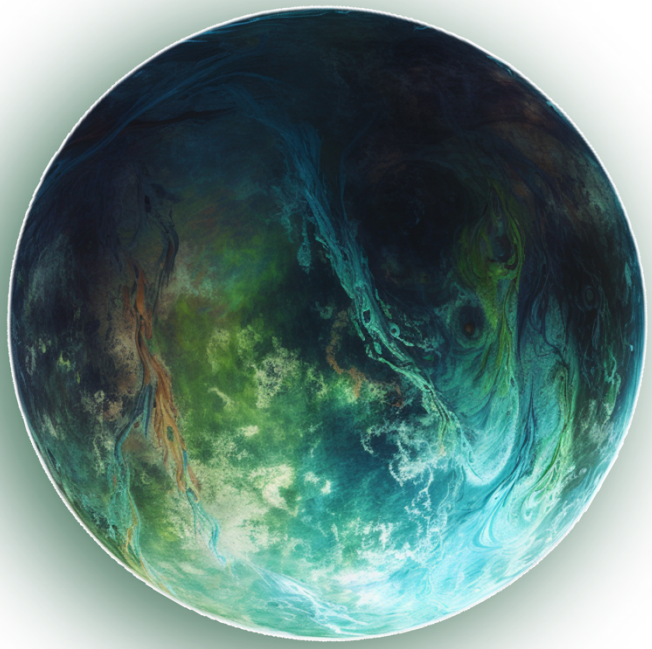
RMG FZC

Anti Money Laundering Policy



RMG FZC LIMITED
Hong Kong SAR, China

Company Incorporation & Business Registration No.: 76874833
Registered Address: 9/F Amtel Building, 148 Des Voeux Rd Central, Central, Hong Kong
Email: welcome@rmgfzc.co
Website: www.RMGFZC.co

6 August 2024
Version 1.1

Table of Contents

1. Introduction

The Anti-Money Laundering and Counter Financing of Terrorism Ordinance (Cap. 615) of Hong Kong SAR requires firms to apply risk-sensitive client due diligence measures (including identification and verification of identity) so that they know and understand who the client and/or client's beneficial owners are and the nature of activity to expect.

It is a criminal offence to make funds and financial services available to countries, persons, and organisations prescribed by international sanctions legislation. Therefore, the first element of client due diligence is to ascertain whether RMG FZC LIMITED (the Firm) can act for a potential client at all.

RMG FZC LIMITED is committed to maintaining effective prevention and detection measures to assist the law enforcement authorities to deter, detect, and disrupt financial crime. This policy sets out the minimum standards established to protect RMG FZC LIMITED from being used to launder money or to finance terrorism and to ensure that all employees and long-term contractors conduct business in accordance with applicable Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) regulations.

2. Document purpose

The purpose of this policy document is to lay down RMG FZC LIMITED's AML/CTF policies and create awareness among employees on the means to prevent, recognise, and resolve any possible breach.

3. Objectives

The objective of this document is to prescribe an effective system for combating money laundering and terrorism financing activity within or through RMG FZC LIMITED. It will also ensure that the firm, its employees, and present or future subsidiaries are not complicit, whether willfully or inadvertently, in any form of activity that supports money laundering or terrorism financing. This document has been prepared in compliance with all statutory provisions currently in force in Hong Kong SAR and conforms to international AML & CTF standards.

4. Scope

This policy is applicable to RMG FZC LIMITED's provision of gold bullion trading business activities, including those outsourced. RMG FZC LIMITED may share this policy with selected clients and partners, and in some instances, they may also be contractually obliged to adhere to it.

5. Non-Compliance with this Policy

Non-Compliance with AML rules and regulations can expose RMG FZC LIMITED to substantial risks, including civil and criminal penalties. Non-compliance or violation of the policy requirements by employees may result in:

- Disciplinary action, including termination of employment in appropriate cases
- Civil/criminal penalties.
- Public censure or penalties by the regulators

6. Governance and Review of this Policy

The Risk and Compliance Committee has the ultimate responsibility of approving this policy document and ensuring its implementation.

RMG FZC senior management will be responsible for enforcing compliance with these guidelines while consistently advising the Compliance Committee and the company's employees will be expected to strictly abide by these policy guidelines and support the implementation of this policy.

The custodian of this policy document will be the Money Laundering Reporting Officer("MLRO") of RMG FZC who reports to the Compliance Committee and is responsible for the AML program.

This policy will be subject to periodic reviews taking into account various factors including regulatory changes, adjustments to RMG FZC's business model, market intelligence and industry standards.

7. Regulations

1. The following regulations have been used to formulate this policy:
   - - Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)
   - - Organized and Serious Crimes Ordinance (Cap. 455)
   - - United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)
   - - Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615)

8. Policy Statement

1. RMG FZC LIMITED acknowledges that money laundering, terrorism financing, and other financial crime have become a worldwide concern due to their negative societal and economic effects. The firm has resolved to enhance its participation in the global push for accountability by adopting this Anti-Money Laundering Know and Countering Terrorism Finance policy document.

2. We therefore recognise the likelihood of serious risks with respect to personal, stakeholder and reputational interests in the event RMG FZC fails to adequately design, develop and implement appropriate training, processes and procedures to prevent the facilitation of money laundering or terrorist financing.

9. Scope and Purpose

1. The objective of this document is to prescribe an effective system for combating money laundering and terrorism financing activity within or through RMG FZC. It will also ensure that the firm, its employees and present orfuture subsidiaries are not complicit, whether willfully or inadvertently in any form of activity that supports moneylaundering or terrorism financing.

2. This document has been prepared in compliance with all statutory provisions currently in force in the United Kingdom and HMRC Guidance for Payment Service Businesses and it also conforms to international AML & CTF standards.

3. The purpose of this policy document is to lay down RMG FZC's AML/CTF policies and create awareness among employees on the means to prevent, recognise and resolve any possible scenarios that present money laundering and terrorism financing risks.

10. Money Laundering regulations 2017

1. The Money Laundering Regulations 2017 presents law enforcement, regulatory and supervisory agencies with a great opportunity to collect financial intelligence necessary in combating money laundering and terrorism financing.

2. There are risks for non-compliance with the requirements of the regulations including but not limited to:

   - Revocation of license
   - Fines and penalties
   - Imprisonment
   - Negative publicity and reputational damage

3. This policy document will explore and recommend appropriate and prudent approaches to ensure RMG FZCcomplies with the law while exploiting the opportunities presented under the regulation.

11. What is money laundering?

11.1. Money laundering is the processing of criminal proceeds or illegally acquired funds with an intention of disguising their origin and integrating these funds into the financial system or legitimate economic activity.

11.2 As such - even payment services firms with what might seem to be only an ancillary or a minor part to play in the overall transaction or flow of funds need to be aware of the potential scope for either exploitation, or their playing an inadvertent or indirect part in criminal activities. Full awareness of all AML protocols empowers RMG FZC and its employees to mitigate risk.

12. What is Terrorism Financing?

Terrorist financing refers to the processing of funds to sponsor or facilitate terrorist activity. These funds could be from legitimate or illegitimate sources but their main goal is to provide for the sourcing of materials used in terrorist activity and operations of a terrorist group.

13. Money laundering cycle

1. Money laundering occurs through three distinct stages as demonstrated below;

    1. Placement – Funds acquired from illegal activity enter the financial system. This is mainly through deposits into personal or business accounts. It is important to note that funds from what looks like legitimate business activity could be a front for a money laundering syndicate.

    2. Layering – At this stage, criminals create a complex web of transactions through various accounts, instructions, or geographical locations (often extending across borders) aimed at obfuscating the source and/or beneficiaries of these funds.

    3. Integration – The laundered funds that by now have been "processed" to appear to come from legitimate sources are then integrated into the legitimate economy through the purchase of high value goods, mutual funds, investment companies, listed stocks, household and industrial property, real estate, business ventures, and other activities usually engaged in using legitimately acquired funds. The proceeds are used to further criminal activities where funds are commingled with legitimate business proceeds.

14. Structuring

14.1. Structuring is the act of altering a financial transaction to avoid detection.

14.2.For example, a launderer who would like to launder £10,000 might split it into several deposits instead of one single deposit to stay under a regulatory reporting threshold.

15. Smurfing

15.1. Smurfing on the other hand is the act of using individuals or runners to perform multiple financial transactions to avoid the currency reporting requirements.

15.2 In the above example, the criminal who wants to launder £10,000 will now recruit several people to make deposits below the regulatory reporting threshold.

16. Refining

1. Refining is a money laundering method that involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different firms or branches in order not to raise suspicion. This serves to decrease the bulk of large amounts of cash.

For example, a drug dealer who sells small amounts of drugs on the streets collects many small value denominations. Making such deposits would raise suspicion and therefore they move around payments businesses or branches requesting 'exchange' into higher value denominations that are easier to carry around without attracting a lot of attention.

2. All customers and non-customers of RMG FZC requesting transfers or movement of funds will be subject to appropriate identification and due diligence procedures as spelt out in the KYC section of this document. Suspicious Transaction reports should also be raised once transactions of this nature meeting threshold limits are identified.

17. Risk & Compliance Committee Responsibilities

- Ownership of RMG FZC LIMITED's risk-based money laundering prevention strategies and policies.
- Accountability for the establishment and maintenance of effective risk-based systems and controls including (but not limited to) product and service development, client take-on, and changes in business profile.
- Ensuring adequate controls and implementation of anti-money laundering risk management policies.
- Considering the extent to which cultural barriers to compliance exist and taking effective measures to address these.
- Ensuring that any material outsourcing in respect of AML systems and controls is properly assessed, controlled, and monitored in line with any relevant requirements of RMG FZC LIMITED's regulator.
- Clear allocation of the roles, responsibilities, and duties involved in managing RMG FZC LIMITED's money laundering risks.
- Ensuring that an appropriately qualified Money Laundering Reporting Officer (MLRO) is appointed and that the function is adequately resourced including coverage for absences.
- Ensuring that the MLRO is provided promptly with reports of suspicious activities and unfettered access to client and business information held by RMG FZC LIMITED.
- Seeking management information from the MLRO at least on an annual basis as to the effectiveness of RMG FZC LIMITED's systems and controls compliance with policies and procedures and applicable laws.
- Ensuring that any regulatory notification concerning a material failure in RMG FZC LIMITED's systems and controls or compliance with applicable laws and regulations is duly filed.
- Ensuring overall responsibility for the establishment and maintenance of effective systems and controls under Hong Kong SAR rules has been allocated to the MLRO.

18. Business Risk Assessment

1. Financial crime strategy and risk-based systems and controls should be comprehensive and proportionate to the nature and scope of RMG FZC LIMITED's activities and enable the company to identify, assess, monitor, and manage its money laundering risk. Regular assessments of the effectiveness of the systems and controls must be carried out to ensure on-going compliance and all stages of this process must be documented.
2.
3. In assessing its money laundering risk, RMG FZC LIMITED must take account of several factors including:

3.1.- Customer, product, and activity profiles
3.2.- Distribution channels
3.3.- Complexity and volume of transactions
3.4.- Processes and systems
3.5.- Operating environment
3.6.- Geographical risk.

4. RMG FZC LIMITED's business risk assessment comprises a profile for the company, its regulated entities and activities, an assessment of business risk, and a matrix of identified risk and mitigating measures. On an on-going basis, there is a review of controls by the MLRO and Senior management with any adjustments agreed and an action for change drawn up. This Business risk assessment is reviewed by the MLRO on an annual basis and findings reported to the Risk & Compliance Committee.
5. The Company has a product roadmap that will introduce new customer products and offerings. A financial crime risk assessment is performed for all new products and service offerings as part of RMG FZC LIMITED's product governance process.

19. Internal Controls - Employee Vetting

1. An employer will commit a criminal offence if it engages or supplies a barred person to undertake a regulated activity . The safeguarding schemes impose a duty on employers to check information on

individuals carrying out regulated activities where this may affect their suitability to perform such a role. Checks must be made with the Disclosure and Barring Service to ensure an individual is not barred from regulated employment and any offers of employment must make clear they are subject to this check.

2. Regulators have expressed concern about the use of insiders to facilitate crime or launder the proceeds of crime. RMG FZC has therefore decided to take a rigorous employee vetting process through hiring a specialised third-party provider to carry out the employee vetting process, which involves:

- Checking CVs and dealing with any discrepancies at the interview stage.
- Conducting background screening of all recruits The level of screening applied depends on the riskrating applied to the relevant role from a financial crime perspective.
- On-going screening of employees will focus on financial and reputation issues.
- Employees must also complete satisfactory probationary periods, which may be extended at the discretion of their manager.

20. Money Laundering Reporting Officer

1. The key person responsible for comprehensive and ongoing KYC compliance is RMG FZC's MoneyLaundering Reporting Officer ("MLRO").

Among the key responsibilities of MLRO are:

- Co-ordinating customer facing activity to ensure that all existing customers comply with standard documentary requirements,
- Track and report on key updates of to AML policies and procedures, ensuring they meet requirements at all times,
- Ensure customer-facing staff are well trained and comply with AML/KYC/CTF requirements for new relationships as set out in this policy and others,
- To be in charge of escalated document verification to ensure that customers and staff meet the requirements outlined in this policy,
- To act as the repository of KYC best practice and advise the Risk & Compliance Committee and management on any implementation challenges or similar,
- To advise the Compliance Committee and senior management on regulatory trends and industry best practice.
- To establish an an AML compliance program and operational procedures
- Receive and vet suspicious activity reports from staff and file these with the appropriate authority when deemed necessary
- To ensure that the AML compliance programme is followed and enforced
- Co-ordination of staff training and AML awareness
- Developing and deploying methods of detecting suspicious activity
- To maintain close co-operation & liaison with our regulator and other relevant authorities.

21. Roles and Responsibilities of Employees

All employees of RMG FZC LIMITED will be expected to fully support all the requirements of this policy in their day-to-day work. They also have an express obligation:

Not to knowingly support individuals, corporate bodies, or any other parties with an intention of laundering funds or channelling terrorist financing funds through RMG FZC LIMITED.

Not to tip off customers who are under investigation or whose transactions are being monitored or on whose transaction(s) an STR/SAR has been filed.

Not to offer any solicited information about internal controls and safeguards against money laundering to external parties without the express permission of the MLRO.

RMG FZC employees (and long-term contractors) are required to:

- Conduct themselves in accordance with the highest ethical standards
- Comply with all applicable AML and sanctions laws and regulations
- Comply with the firm's AML and sanctions policies and procedures
- Prevent, detect and report money laundering, terrorist financing or other unusual orsuspicious activity
- Protect RMG FZC reputation for integrity and fair dealing, by ensuring that our clients and the transactions they are engaged in on their behalf are legitimate.

- RMG FZC employees are not permitted to:
  - Knowingly provide advice or assistance to individuals or entities who breach or attempt to breach or avoid AML laws or the company's policies or procedures
  - Establish client relationships or conduct transactions with prohibited individuals/entities
  - Deliberately, recklessly or negligently ignore indications that a client is seeking to engage in a relationship or transaction for anything other than a lawful purpose.

  - Employee responsibilities are to:
  - Be alert to the possibility of money laundering/terrorist financing and unusual activities,
  - Comply fully with all AML policies and procedures including client due diligence and verification of identity, monitoring, record keeping, plus detection and reporting of suspicious activity,
  - Promptly report to the Money Laundering Reporting Officer all occasions where there are reasonable grounds to suspect money laundering; and
  - Attend or otherwise complete any required AML training

1. Acquisition, possession, and assistance - It is an offence to acquire the proceeds of crime or to assist anyone whom you know, or suspect has committed or benefited from criminal conduct. The offence of money laundering has a maximum tariff, of up to 14 years imprisonment.
2. Failure to report - It is an offence for any member of management or staff who acquires knowledge or has reasonable grounds to know or suspect that benefit has been gained from criminal conduct or proceeds of crime are being laundered, not to report their concerns as soon as possible. Staff who are negligent in this respect may be liable to prosecution and there is a maximum of up to 5 years

imprisonment.

3. Tipping Off - It is an offence for anyone to prejudice an investigation by informing the subject, or any third party, of a suspicion, that a disclosure has been made either internally or externally, or that the authorities are acting or proposing to act or investigate. The offence of tipping off has a maximum tariff, of up to 5 years imprisonment.

4. Disclosure of a SAR - It is an offence to disclose to a third person that a SAR has been to the police, HM Revenue and Customs, the NCA or any other authority, if that disclosure might prejudice any investigation that might be carried out as a result of the SAR.

5. Disciplinary Processes:

1. RMG FZC has in place disciplinary arrangements for circumstances where a member of staff fails without reasonable excuse to make an internal suspicious activity report ("SAR").

2. RMG FZC will also consider disciplinary action when a member of staff acts in a way that puts the firm at risk of breaching a legal or regulatory obligation.

2. Our internal disciplinary processes are separate from any disciplinary action that may be initiated by the FCA if a breach of their principles or rules is found to have been caused..

22. AML Compliance

1. Risk Based Approach for AML Compliance

1.1. RMG FZC will adopt a risk-based approach to its AML/KYC/CTF compliance program and all related matters. We seek to mitigate all money laundering and terrorist financing risks before they present themselves.

1.2. In collaboration with staff, the Board will spearhead an enterprise-wide compliance culture by setting the right tone from the top. They will also be responsible for evaluating overall organisational compliance levels through quantitative and qualitative measures.

1.3. In enforcing compliance to policies as set out in this document, the Risk & Compliance Committee will ensure that:

- This AML policy document is distributed and available to all) employees
- All employees are aware of RMG FZC's KYC policies, know what money laundering is and their responsibilities and obligations in relation to the company's Anti-Money Laundering programme.
- All employees are aware of the reporting procedures regarding suspicious activity reports(SAR),
- Training programs are conducted and amended by all employees
- The identities of the new customers are properly verified with respect to the account opening checklist and against original documents. In instances when this is outsourced assurance must be

provided by the third party that their procedures meet the requirements of RMG FZC and formal agreements ensuring this must be put in place.

23. Customer Due Diligence ("CDD")

The goal of CDD is to access client information and understand the types of behaviours and transactions the customer is likely to undertake. CDD processes should be risk-based and information collected should be commensurate with the AML risk profile of each client.

Customer Identification and Identity Verification Procedures

The firm will adhere to the following procedure for identifying and verifying client identity before commencing any relationship:

- Identification and Verification should be completed for:

- The client legal entity (Merchant)

- Ultimate Beneficial Owner

- Officers - Directors, Partners, etc.

- Authorised Signatories / Legal representatives

24. Customer Identification and Identity Verification Procedures

1. The firm will adhere to the following procedure for identifying and verifying client identity before commencing any relationship;

Identification and Verification should be completed for;

- The client legal entity (Merchant)
- Ultimate Beneficial Owner
- Officers - Directors, Partners, etc
- Authorised Signatories / Legal representatives

2. Engage the customer through the onboarding portal capturing as much detail about the customer as possible.

3. Establish a four-eye principle during review. The first operation team checks the completeness of documents., with the MLRO conducting a sanity check on quality of work.

4. Final approval to establish the account/initiate the relationship should be documented and keep an audit trail for record keeping purposes.

5. The firm should verify documents and information by use of one or more of the following methods:

- Confirming the details on KYC requirements from official documents supplied;
- Confirming the validity of the official documentation through certification by an authorised person (e.g., embassy official, notary public, registrar of companies etc);
- Undertaking a company search or other commercial inquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated;
- Using an independent information verification process, such as by accessing public and privatedatabases;
- Visiting the corporate entity where practical.

25. Verification of documents

RMG FZC will verify identity documents electronically using third party tools that leverage on technology and official databases to verify ID docs.

25.1. KYC Deficiencies

25.1.1. In the event of any KYC information being found deficient for lack of information / insufficient document quality or availability, the client's account must not be allowed to operate, only unless an exception is granted by the MLRO.

2. Identification & Verification of Ultimate beneficial ownership (UBO)

2.1. A UBO is defined as each individual (natural person) who directly or indirectly owns 25% or more equity interest of a legal entity or a single individual with significant responsibility to control, manage or direct a legal entity (e.g. its Chief Executive Officer, Chief Financial Officer, Chief Operating Officer etc.)

26. PEP, Sanctions & Adverse Media Screening

26.1. Before establishing a business relationship, RMG FZC will run a negative news search. The purpose of this is to identify any negative references to the professional reputation of a new or an existing client and

uncover any allegations of criminal activity. Any links to negative news uncovered should be clearly explained & documented and taken into account when risk rating the client.

27. Watch List Screening

1. RMG FZC deploys screening engine LexisNexis to capture name variance and spelling from those provided on screening lists. The compliance team will follow the four- eye principle to conduct sanction and other review upon a positive hit.

2. Based on the risk appetite of the company, the following lists will be used for daily customer screening:

   - The United NaCon Match List
   - US Office of Foreign Assets Control List ("OFAC") Specially Designated Nationals ("SDN") list. The maintenance of the list is managed by LexisNexis and it is updated on a daily basis. The MLRO and compliance team members will screen existing and new clients plus suppliers to ensure none of them are on the lists.
   - The MLRO is in addition responsible to maintain an entity-specific list, such lists as required by banks, local regulators, internal blacklist, card BIN list etc and conduct periodic screening against this list.

3. RMG FZC adopts a rigorous process to review all the hits generated. Reviewers will check the client's name, address and identify information to review the hits. RMG FZC will reject any persons or entities that are designated or blocked on the lists.

If there is a positive match, we will verify additional data elements such as Date of Birth and full identification information to decide whether the hit is true or not.

4. If after investigation it's decided to be a true positive hit, it will be escalated to the MRLO. If a true hit is identified during a transaction, the transaction won't be completed, and the client reported within 7 working days.

If after investigation, the hit is a false positive, the compliance team will document their decision and keep a record of it on file.

28. Sanction reporting

28.1. RMG FZC will help coordinate the freezing and reporting of any sanctioned transactions or accounts under its control, according to our regulatory obligations. Once the MRLO identifies a hit, the correspondent transaction and account will be reported within 7 business days.

29. Enhanced Due Diligence

Where necessary following a risk assessment RMG FZC LIMITED will conduct Enhanced Due Diligence (EDD) on medium/high-risk clients to understand and verify their identity and detect instances of suspicious activity. EDD is required for new and existing customers which pose high risk or represent specific AML risks/aspects. Our EDD activities include but are not limited to the following:

A check using public information or a third-party service provider (e.g. LexisNexis) to validate corporate information provided by the client.

Requesting original or certified documents to verify the identity of the client and key associated parties - Officers, Authorised Signatories, UBOs, etc.

Collection of information to understand the source of funds and source of wealth.

Negative news: An open search in Google to check if there is negative news about the client using a defined search string as well as within a third-party tool.

30. Periodic Reviews

1. The Board will conduct a quarterly review of KYC exception reports, unresolved SARs, and other monitoring reports.

2. During these reviews they will make decisions on retention or exiting of relationships for all pending cases.

31. High Risk Accounts & PEP Accounts

1. Relationships with PEPs may represent increased risks due to the possibility that individuals holding political or other public offices may misuse their power and influence for personal gain and advantage or for the personal gain or advantage of family and close associates. Such individuals may also use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position or resulting from bribery and corruption. Additionally they may also seek to use their power and influence to gain representation and/or access to, or control of legal entities for similar purposes.

2. It is however important to understand that the majority of PEPs do not abuse their position and will not represent any undue additional risk to RMG FZC solely by virtue of that categorisation. PEPs may be categorised as such in their own right or by association.

PEPs include but are not limited to the following:

- Heads of state;
- Heads of government;
- Government ministers (including assistants and or deputy ministers);
- Members of parliament;
- Senior government officials;
- Officials and equivalent of the above or other international organisations and ambassadors;

3. A business entity formed by or on behalf of any of the above-mentioned persons is considered the equivalent of PEP. Once a PEP has been identified, the compliance team should follow KYC procedures andidentify the source of funds, along with reporting the PEP to the Risk & Compliance Committee for approval.

4. Close family includes a PEP's direct family members including spouses, children, parents and siblings. In any of these cases there may be circumstances which mitigate against categorising a family member themselves as a PEP, including separation and estrangement although these facts should be investigated and recorded.

- Close associates: include a PEP's widely and publicly known close business colleagues and/or personal advisors, in particular financial advisors or persons acting in a financial fiduciary capacity. Such associates should be categorised as a PEP themselves and treated accordingly.

5. Recognising that PEPs can provide legitimate business, but also fully cognisant of the risks inherent in some of these relationships, RMG FZC:

- Will treat clients falling under the PEP category alongside other High Risk clients and carry out EDD measures both at on-boarding and through the relationship with the client,
- Shall have reasonable procedures designed to try to identify PEPs before the relationship is established,
- Will ensure that PEPs as with any other client of ours are recognised and respected, with clearinstructions on how to handle such clients developed,
- Ensure that final authority for establishment of relationships with PEPs will be sought from the Risk & Compliance Committee.
- Will ensure that PEPs are closely monitored to ensure their ongoing behaviour is aligned with the business activities proposed at the start of the relationship.

32. Money Laundering Risk Assessment

1. Product Risk

1.1. RMG FZC will establish clear rules for the assessment of all existing products/services and incorporate the same rules for new and future products to ensure that the company's products do not present opportunity for money laundering or terrorism financing, either due to limited controls or design that makes it difficult to fulfill legal requirements

2. Payment Partners Risk

2.1. RMG FZC has established rules to evaluate risk from external payment partners to ensure the partner does not present a money laundering or terrorism financing risk. We will evaluate their core management qualifications, compliance and risk management capabilities and check for any negative news on them before establishing a relationship.

3. Merchant Risk

3.1. The firm has developed a process to evaluate a client's risk based on the following factors:

- Completeness of KYC and AML Risk Profile
- Years in business

- Business categories - Industry Type (card scheme Merchant Category Code)
- Operational risk e.g. source of funds
- Product value
- Average Ticket Value
- Credit risk

33. Customer Risk Assessment

1. The Risk & Compliance Committee will lead in the implementation of an ongoing customer and transaction risk assessment program for all existing and new clients, to support an effective monitoring and reporting framework.

2. The risk rating exercise will be based on the following key parameters:

- Client Type - Client occupation/profession or business
- Nature of transactions e.g. cash intensive, wire transfers, forex transactions etc
- Means to entering business relationship with the client (on-site visit or rely on third party due diligence)
- Presence of any Politically Exposed Persons
- Geographic origin of the client and related parties or operation
- Results of adverse media screening against regulatory warning lists, HM Treasury, OFAC and United Nations sanctions lists
- Non-compliance with information recording requirements
- When client transactions are inconsistent with stated business or activities
- The client suddenly experiencing significant transaction fluctuations
- Significant changes being made to the client's information, such as business licence, office location etc.

- Clients frequently having large-value transactions or suspicious transactions;

- Client who receive frequently complaints

3. The MLRO will develop a risk assessment methodology for transactions emanating from or received by RMG FZC or conducted through specific products. The risk-rating exercise will be ongoing and will be informed byrespective business developments, but a comprehensive review should be conducted by the Risk & Compliance Committee every 12 months.

34. Customer Due Diligence (CDD)

1. Having sufficient information about clients and making use of that information underpins all the other anti-money laundering procedures and is the most effective weapon against being used to launder the proceeds of crime. It additionally provides protection against fraud, enables the compliance team to recognise and report suspicious activity in accordance with their personal legal obligations, and protects RMG FZC against reputational and financial risk.

Client due diligence measures comprise of the following:

1. Identifying clients and verifying their identity,

2. Identifying beneficial owners of clients (where applicable) and verifying their identity,

3. Obtaining information about the purpose and intended nature of the intended business relationship, and;

4. On-going monitoring of business relationships.

Due Diligence is be conducted as described below:

35. Collecting KYC information

35.1.RMG FZC will deploy a digital onboarding KYC platform where the customer uploads documents and information via our website or app. Publicly available information will be extracted from official registries tosupplement information provided by the client.

36. Document Verification

36.1.Uploaded images of identity documents are reviewed for data integrity, visual authenticity and against a police record check. The image on a document is matched with a selfie photo taken by the client at the time ofsubmission, to check they are the true owner of the document.

Where discrepancies are identified with regards to these documents, EDD is required and further documentation may be requested to verify the prospective client.

37. Facial Similarity photo

37.1.The Facial Similarity Photo checks uses a live photo taken at the time of submission, so that an assessment may be performed to assess whether the holder of the identity document is the same actual person as appears on the document. Checks carried out include face comparison, image integrity, visual authenticity (spoofing detection).

37.2.Where discrepancies are identified with regards to these documents, EDD is required and further documentation may be requested to verify the prospective client.

38. Enhanced Due Diligence ("EDD")

38.1.All clients that present a high risk of money laundering and terrorist financing activity will be subject toEDD. Such clients include but are not limited to:

- PEPs
- Companies in the travel industry
- Financial service providers
- High-value goods dealers e.g. precious stone dealers, high value art dealers etc.

38.2.The purpose of EDD is to understand and verify the customer's identity and to detect, report instances of suspicious activity. EDD should include identifying any negative reference to the professional reputation of the individual or entity by where relevant;

- Collecting information to understand the source of funds and/or purpose of transaction;
- Collecting information on the ownership structure, beneficial owners, controllers and account signatories;
- Obtaining additional information about the client such as financial statement; description of business operation, anticipated total sales and list of end clients;
- Comparing information collected against what's known of the client to ensure the information presented is logical and consistent.
- Reviewing any transaction history to ensure it's aligned with expected behaviour.
- Visiting business sites in person if needed.
- Requiring original or certified copies of documents to verify the identity of the clients or its ultimatebeneficial owners.
- Anticipated future business volumes;
- The type of business relationship and purpose of the relationship;
- Requiring completion of prescribed KYC/Due Diligence forms;

39. Transaction Monitoring and Reporting

39.1.As part of ongoing CDD and EDD measures, RMG FZC will implement a manual and automated transaction monitoring program. This will mainly support identification of threshold limits and reporting of SARs. Reporting procedures are outlined in subsequent sections.

39.2.RMG FZC will not conduct business with Shell Companies or Numbered Accounts, nor clients with no known operating address, assets or visible operations nor remit/receive money from accounts or clients whose identity is kept secret, anonymous or do not provide full disclosure of their ultimate beneficiary(ies).

39.3.The firm will implement a robust transaction monitoring program that will be able to detect complex, unusual large transactions and unusual patterns which have no apparent economic or lawful purpose, or which are inconsistent with the client's known activity.

40. Investigation and Monitoring Co-ordination

40.1.The compliance team will be responsible for coordinating internal investigations on all suspicious customer activity and coordinating discussion with regulators and supervisory agencies.

41. Technology (Core System and Outsourced AML Compliance Services)

41.1.RMG FZC will continue to invest in and optimise our core transaction monitoring capabilities to ensure that the system generates reports and information in an effective way that is relevant to the identification of trends, suspicious transactions/activities and other prescribed monitoring requirements.

41.2.RMG FZC will also invest in other outsourced services e.g. training, screening, systems review and audit that it deems would be best handled by an external party, without prejudice to the requirement that the company bears ultimate responsibility for all outsourced services.

42. Employee Training and Audit

42.1.The Risk & Compliance Committee will identify the frequency with which to upgrade staff skills in recognising and preventing money laundering activity through a structured training program.

42.2.They will also ensure that all staff are up to date with most recent legal and regulatory developments and that they are aware of their obligations relating to AML/KYC/CTF compliance at all times. RMG FZC will develop a training program for all of the RMG FZCs's employees, which is tailored to the nature of our business. The training will;

1. Describe the nature and processes of money laundering and terrorist financing;

23. Explain AML/KYC/CTF laws, regulatory requirements and related laws with regard to threshold transactions and record keeping

24. Explain RMG FZC's policies and systems with regard to reporting regulations on suspicioustransactions/acclivity with emphasis on client identification and verification of identity,

25. Outline appropriate due diligence and reporting procedures and requirements.

42.3.RMG FZC may periodically engage external/independent & comprehensive review and audit of AML/KYC/CTF frameworks, policies and systems to assure that they conform to evolving regulatory requirements. This exercise will in any event be conducted at least once every three years.

43. Suspicious Transaction/Activity Reports

The MLRO is responsible for creating a Suspicious Transaction/Activities Report and following the standard reporting procedure to the Financial Services and the Treasury Bureau (FSTB). A suspicious transaction is one that involves potential money laundering or terrorist financing or one that violates the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) and existing statutory provisions. It is any transaction conducted or attempted by, at, or through RMG FZC LIMITED which we know, suspect, or have reason to suspect:

- Involves funds derived from illegal activities or is intended to be conducted in order to hide or disguise funds or assets derived from illegal activities (including without limitation the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement;
- Is designed to evade any regulations promulgated under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance or has no business or apparent lawful purpose or is not the sort in which the particular client would normally be expected to engage and we know of no reasonable explanation for it.

44. Retention of Documents and Record Keeping

44.1.RMG FZC will retain all records of the customer for 5 years, as required by law. Other policy requirements of RMG FZC and regulators on document retention shall be adhered to as prescribed.

The records covered and to be retained are;

- All account opening/customer KYC records;
- Identification records with supporting documentation
- Transactional records (all data records on transactions) including specific dates, codes, methods used to identify the client
- Reports and respective name of the RMG FZC employee who prepared the record.

44.2. RMG FZC's records will be kept for the following retention periods:

- Records for UK client are kept according to data retention policy for 5 years following cessation of theclient account,
- Records for EU customers are kept according to data retention policy for 8 years following cessation ofthe client account,
- 6 years for account information and

- 7 years for transaction records after the customer relationship ends.

44.3. RMG FZC's record keeping principles are:

- To retain records of all suspicious activities reports made by members of staff to the MLRO, and all disclosures made by the MLRO to the NCA;

- To keep records of dates when AML training was given, the nature of the training, and confirmation of completion and competence.

- To retain records of senior management information as to effectiveness and compliance of the MLRO and other relevant persons
- To ensure that all relevant regulatory records can be retrieved in a timely manner on receipt of areasonable request from a regulatory or law enforcement agency, or a court order.

- All records are kept in electronic format in a central repository.

The Senior Management team will be responsible for ensuring accurate record keeping and safe disposal of data records when it is no longer required.

45. Information Sharing

45.1. RMG FZC will cooperate with local law enforcement authorities, regulatory bodies/agencies and business partners on AML investigations to the extent allowable under applicable privacy and other laws. We will:

- Establish a centralised process for receiving and responding to requests for information sharing and similar;

- Promptly evaluate all information sharing requests received, including those from bank partners, and provide prompt response under applicable privacy laws.

- Ensure employees don't disclose suspicious activity reports to external partners without written permission from the MLRO.

45.2. RMG FZC may outsource specified systems and controls to third-party vendors however, the company remains fully responsible for complying with local AML laws and regulations. The MLRO in conjunction with the legal counsel is responsible for approving contracts and agreements with third-party service providers and will keep a list of outsourcing vendors.The MLRO will oversee the vendor engagement process including:

- Conducting due diligence on capabilities and AML related risks before engaging a prospective vendor
- Establishing an SLA with the vendor in terms of meeting local regulatory requirements
- Performing periodic review on vendor's service against Service Level Agreement.
- Requesting vendors provide training to applicable employees
- Presenting vendor's risk assessment findings to the AML Risk committee.

46. Glossary of Abbreviations

AML	Anti-Money Laundering
CEO	Chief Executive Officer
CO	Compliance Officer
CTF	Counter-Terrorism Financing
CDD	Customer Due Diligence
EFT	Electronic Funds Transfer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
ICT	Information and Communication Technology
KYC	Know Your Customer
KYCC	Know Your Customer's Customer
KYE	Know Your Employee

MLR	Money Laundering Regulations 2017
POCA	Proceeds of Crime Act, 2002
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report