ANTI-MONEY LAUNDERING AND SANCTIONS RULEBOOK (“AML) 2026

(Version 1.1)

Table of Contents

1. INTRODUCTION **3**
1.1 Jurisdiction 3
1.2 Application 3
Application table 5
1.3 Responsibility for compliance with the AML Rulebook 5
2. OVERVIEW AND PURPOSE OF THE AML RULEBOOK **6**
Financial Action Task Force Standards 8
Basel Committee Standards 8
Wolfsberg Group 8
Sanctions 9
3. INTERPRETATION AND TERMINOLOGY **10**
3.1 Interpretation 10
3.2 Glossary for AML 10
4. GENERAL COMPLIANCE REQUIREMENTS **19**
4.1 General requirements 19
4.2 Groups, branches and subsidiaries 20
4.3 Group policies 21
4.4 Notifications 21
4.5 Record keeping 22
4.6 Annual AML Return 25
4.7 Co-operation with the Regulator 25
4.8 Employee disclosures 25
5. APPLYING A RISK-BASED APPROACH TO AML/TFS **26**
5.1 The risk-based approach 26
6. BUSINESS RISK ASSESSMENT **28**
6.1 Assessing the money laundering risks of a business 28
6.2 AML/TFS systems and controls 30
7. CUSTOMER RISK ASSESSMENT **32**
7.1 Assessing the money laundering risks of a customer 32
Guidance on the customer risk assessment 37
Guidance on high-risk customers 37
Guidance on low-risk customers 38
7.2 Prohibition on establishing business relationships with certain customers 38
Guidance on anonymous accounts 39
8. CUSTOMER DUE DILIGENCE **40**
8.1 Requirement to undertake Customer Due Diligence 40
8.2 Timing of Customer Due Diligence 43
8.3 Customer Due Diligence requirements 45
Guidance on verification of the identity of Beneficial Owners 51
Guidance on Politically Exposed Persons (PEPs) and corruption 52
Guidance on FATF Jurisdictions Under Increased Monitoring / Subject to a Call for Action 53
8.4 Enhanced Customer Due Diligence 53
8.5 Simplified Customer Due Diligence 56

8.6 Ongoing Customer Due Diligence 57
8.7 Failure to conduct or complete Customer Due Diligence 59
8.8 Portability of Customer Due Diligence information 60
9. AML/TFS COMPLIANCE AND THIRD PARTIES 61
9.1 Reliance on a third party 61
9.2 Business partner identification 64
9.3 Outsourcing and agents 67
10. CORRESPONDENT BANKING, WIRE TRANSFERS, ANONYMOUS ACCOUNTS AND AUDIT 70
10.1 Application 70
10.2 Correspondent banking 70
10.3 Wire transfers and the Travel Rule 71
10.4 Audit 74
10.5 Anonymous and nominee accounts 74
11. TARGETED FINANCIAL SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS 76
11.1 Resolutions and Sanctions 76
11.2 Government, regulatory and international findings 77
12. MONEY LAUNDERING REPORTING OFFICER 81
12.1 Appointment of an MLRO 81
12.2 Qualities of an MLRO 82
12.3 Responsibilities of an MLRO 83
12.4 Reporting 84
13. AML/TFS TRAINING AND AWARENESS 86
13.1 Training and awareness 86
13.2 Frequency 87
13.3 Record-keeping 87
14. SUSPICIOUS ACTIVITY/TRANSACTION REPORTS 89
14.1 [Not in use] 89
14.2 Internal reporting requirements 89
14.3 Suspicious Activity/Transaction Reports 91
14.4 Suspension of Transactions and “no tipping-off” requirement 93
14.5 Record-keeping 93
14.6 Freezing of assets 93
15. DNFBP REGISTRATION AND SUPERVISION 94
15.1 DNFBP prohibition 95
15.2 Criteria for registration as a DNFBP 95
15.3 Application for registration as a DNFBP 96
15.4 Grant of an application 96
15.5 Refusal of an application 97
15.6 DNFBP notifications 97
15.7 Suspension and withdrawal of DNFBP registration 97
15.8 Disclosure of regulatory status 98
15.9 Co-ordination between the Regulator and the Registrar of Companies 98
(a) The GMC Registrar of Companies shall not grant a Person who is a DNFBP a commercial licence to operate in GMC until the Regulator has confirmed to the Registrar of Companies that it intends to register the Person as a DNFBP. 98

(b) The Regulator shall as soon as is practicable notify the Registrar of Companies where it suspends or withdraws the registration of a DNFBP. 98

(c) The GMC Registrar of Companies shall as soon as is practicable suspend or withdraw (as the case may be) the commercial licence of the DNFBP where it receives a notification under (2). 98

16. NON-PROFIT ORGANISATIONS 100

16.1 Responsibility for NPO compliance 100

16.2 Record Keeping 100

16.3 Co-operation 100

17. FINANCIAL INTELLIGENCE UNIT 102

1. INTRODUCTION

1.1 Jurisdiction

1.1.1 (1) The AML Rulebook is issued by the Gelephu Financial Services Office ("**GFSO**") and applies in Gelephu Mindfulness City ("**GMC**").

(2) [*Not in use*]

1.2 Application

1.2.1 (1) Subject to (2), the AML Rulebook applies to:

(a) every Relevant Person in respect of all its activities carried out in or from GMC; and

(b) the Persons specified in Rule 1.3.3 as being responsible for a Relevant Person's compliance with the AML Rulebook.

(2) In respect of a Relevant Person that is:

(a) A Licensed Firm, other than a Credit Rating Agency, and a Licensed Body, only the requirements of Chapters 1 to 14 of the AML Rulebook apply;

(b) a Representative Office, only the requirements of Chapters 1 to 6 and 11 to 14 of the AML Rulebook apply;

(c) a DNFBP, only the requirements of Chapters 1 to 9 and 11 to 15 of the AML Rulebook apply; and

(d) an NPO, only the requirements of Chapter 16 of the AML Rulebook apply.

Guidance

1. Chapters 7 to 9 of the AML Rulebook deal with customers. Asthe Representative Office does not have customers, these chapters do not apply.

2. Chapter 10 of the AML Rulebook deals with correspondent banking, electronic transfer of funds and audits.

3. Relevant Persons should consider these Chapters and determine which provisions apply. To assist Relevant Persons the following table sets out the application of the AML Rulebook to each of the different types of Relevant Persons specified in Rule 1.2.1(1). This table is for guidance purposes only.

Application table

Relevant Person	Applicable Chapter(s)	
Licensed Firm, other than a Credit Rating Agency, or Licensed Body	1 - 14	
Representative Office	1 - 6	11 - 14
DNFBP	1 - 9	11 - 15
NPO	16	

1.3 Responsibility for compliance with the AML Rulebook

1.3.1 A Relevant Person's Governing Body is responsible for establishing, maintaining and monitoring the Relevant Person's AML/TFS policies, procedures, systems and controls and compliance with the AML Rulebook and the GMC Financial Services Act ("**FSA**") 2025.

1.3.2 A Relevant Person's Governing Body must ensure the policies, procedures, systems and controls referred to in Rule 1.3.1 are effective to meet the obligations of the Relevant Person.

1.3.3 (1) Responsibility for a Relevant Person's compliance with the AML Rulebook lies with every member of the Governing Body, and its Senior Management.

(2) In carrying out their responsibilities under the AML Rulebook, every member of a Relevant Person's Governing Body, its Senior Management and Money Laundering Reporting Officer ("**MLRO**"), as the case may be, must exercise due skill, care and diligence.

(3) Nothing in this Rule precludes the Regulator from taking enforcement action against any Person, including any one or more of the following Persons, in respect of a breach of any Rule in the AML Rulebook:

(a) a Relevant Person;

(b) members of a Relevant Person's Senior Management; or

(c) an Employee of a Relevant Person.

2. OVERVIEW AND PURPOSE OF THE AML RULEBOOK

Guidance

1. Under Section 15A of the FSA, the GFSO ("**the Regulator**") has jurisdiction for the regulation of AML/TFS in GMC. The AML Rulebook sets out the requirements imposed by the Regulator.

2. [*Not in use*]

3. The AML Rulebook has been designed to provide a primary reference point for Relevant Persons that are supervised by the Regulator for AML/TFS compliance in accordance with the scope of application outlined in Rule 1.2.1. Accordingly it applies to all Relevant Persons, but to different degrees as provided in Rule 1.2.1(2). The AML Rulebook takes into consideration the fact that Relevant Persons have differing money laundering risk profiles. A Relevant Person should familiarise itself with the AML Rulebook and assess the extent to which the Chapters and sections apply to it. Relevant Persons should also ensure they are aware of, and take into account, all notices issued by the Regulator.

4. The AML Rulebook is not intended to be read in isolation from developments in international policy and best practice. To the extent applicable, Relevant Persons need to be aware of, and take into account, how these may impact the Relevant Person's day-to-day operations. This is particularly relevant when considering the United Nations Security Council ("**UNSC**") Resolutions, and Sanctions imposed by other jurisdictions which may apply to a Relevant Person depending on the Relevant Person's jurisdiction of origin, its business and/or customer base.

5. Chapter 1 specifies who is ultimately responsible for a Relevant Person's compliance with the AML Rulebook. The Regulator expects the Governing Body and Senior Management of a Relevant Person to establish a robust and effective AML/TFS compliance culture for the business.

6. Chapter 2 provides an overview of the AML Rulebook and Chapter 3 sets out the key definitions in the AML Rulebook.

7. Chapter 4 outlines the general compliance requirements including Group policies, notifications, record-keeping requirements and the annual AML Return.

8. Chapter 5 explains the meaning of the risk-based approach ("**RBA**"), which should be applied when complying with the AML Rulebook. The RBA requires a risk-based assessment of a Relevant Person's business in Chapter 6, and its customers in Chapter 7. A risk-based assessment should be a dynamic process involving regular review, and the use of these reviews to establish the appropriate

processes to match the levels of risk. No two Relevant Persons will have the same approach and implementation of the RBA and the AML Rulebook permits a Relevant Person to design and implement systems and controls that are appropriate to its business and customers, with the obvious caveat that such systems should be reasonable and proportionate in light of the money laundering risks. The Regulator expects the RBA to determine the breadth and depth of the Customer Due Diligence ("**CDD**") which is undertaken for a particular customer under Chapter 8, though the Regulator understands that there is an inevitable overlap between the risk-based assessment of the customer in Chapter 7 and CDD in Chapter 8. This overlap may occur at the initial stages of onboarding of customers but may also occur when undertaking ongoing CDD.

9. Chapter 9 sets out where a Relevant Person may rely on a third party to undertake all or some of its CDD obligations. Reliance on third-party CDD reduces the need to duplicate CDD already performed for a customer. Alternatively, a Relevant Person may outsource some or all of its CDD obligations to a service provider.

10. Chapter 10 sets out certain obligations in relation to correspondent banking, wire transfers and other matters which are limited to Licensed Firm, other than a Credit Rating Agency, and Recognised Bodies and, in particular, to banks.

11. Chapter 11 sets out a Relevant Person's obligations in relation to both Sanctions issued by the UNSC and other Sanctions, and government, regulatory and international findings in relation to money laundering, terrorist financing and the financing of weapons of mass destruction ("**WMD**").

12. Chapter 12 sets out the obligation for a Relevant Person to appoint an MLRO and the responsibilities of such a Person.

13. Chapter 13 sets out the requirements for AML/TFS training and awareness. A Relevant Person should adopt the RBA when complying with Chapter 13, so as to make its training and awareness proportionate to the money laundering risks of the business and the role of the relevant Employee(s).

14. Chapter 14 contains the obligations applying to all Relevant Persons concerning Suspicious Activity/Transaction Reports to be submitted to the GFSO.

15. Chapter 15 sets out additional obligations applying to DNFBPs, including registration and notification requirements.

16. Chapter 16 sets out the obligations applying to Relevant Persons that are NPOs.

17. [*Not in use*]

18. [*Not in use*]

Financial Action Task Force Standards

19. The Financial Action Task Force ("**FATF**") is an inter-governmental body whose purpose is to develop and promote international standards aimed at preventing money laundering and terrorist financing.

20. The Regulator has had regard to the FATF Recommendations in making these Rules and has determined to closely align these Rules with the FATF Recommendations, where that is deemed to be necessary and appropriate. A Relevant Person may wish to refer to the FATF Recommendations and Interpretive Notes to assist it in complying with these Rules. However, in the event that a FATF Recommendation or Interpretive Note conflicts with a Rule in the AML Rulebook, the relevant Rule takes precedence.

21. A Relevant Person may also wish to refer to the FATF typology reports, which may assist in identifying new money laundering threats and provide information on money laundering and terrorist and proliferation financing methods. The FATF typology reports cover many pertinent topics for Relevant Persons, including corruption, new payment methods, money laundering using trusts and Company Service Providers, and vulnerabilities of free trade zones.

Basel Committee Standards

22. The Basel Committee on Banking Supervision has published a set of guidelines for banks (Sound Management of Risks related to Money Laundering and Financing of Terrorism) which are intended to supplement FATF Recommendations. Banks operating in GMC should read the Basel Committee guidelines in conjunction with FATF Recommendations and in complying with these Rules.

23. In the event that any of the Basel Committee guidelines conflict with a Rule in the AML Rulebook, the relevant Rule takes precedence.

Wolfsberg Group

24. The Wolfsberg Group is an association of thirteen global banks that has published guidance aimed at assisting financial institutions in managing money laundering risks (Wolfsberg Statement Guidance on a Risk Based Approach for Managing Money Laundering Risks) and in preventing terrorist financing (Wolfsberg Statement on the Suppression of the Financing of Terrorism). Banks operating in GMC should be familiar with relevant Wolfsberg Group published guidance in conjunction with the FATF Recommendations and in complying with these Rules.

25. In the event that any part of the Wolfsberg Group published guidance conflicts with a Rule in the AML Rulebook, the relevant Rule takes precedence.

Sanctions

26. GMC is required to comply with all Sanctions issued by the UNSC. Targeted Financial Sanctions ("**TFS**") are Sanctions issued by the UNSC involving asset freezing and other financial prohibitions targeted at individuals, entities or groups with the aim of combatting terrorism and terrorist financing, and countering the proliferation of WMD.

27. UNSC Sanctions and Sanctions apply in GMC. Relevant Persons must comply with Targeted Financial Sanctions. Sanctions compliance is emphasised by specific obligations contained in the AML Rulebook requiring Relevant Persons to establish and maintain effective systems and controls to comply with applicable Sanctions, including in particular Targeted Financial Sanctions, as set out in Chapter 11.

28. The FATF has issued guidance on Targeted Financial Sanctions. Such guidance has been issued to assist in implementing the Targeted Financial Sanctions and activity-based financial prohibitions.

29. Sanctions and the import and export controls imposed or administered by other national and supranational bodies may apply or be relevant to a Relevant Person or its operations and the conduct of its business. In particular, Sanctions administered by the European Union, the U.K. ("**HM Treasury**") and the U.S. (Office of Foreign Assets Control ("**OFAC**")) may need to be carefully considered. The Regulator expects a Relevant Person to consider and take positive steps to ensure compliance where required or appropriate.

3. INTERPRETATION AND TERMINOLOGY

3.1 Interpretation

3.1.1 A reference in the AML Rulebook to "money laundering" in lower case includes terrorist financing, proliferation financing, the financing of unlawful organisations and sanctions e including non-compliance with Targeted Financial Sanctions, unless the context provides or implies otherwise.

3.2 Glossary for AML

Guidance on the term "customer"

1. The point at which a Person becomes a customer will vary from business to business. However, the Regulator considers that it would usually occur at or prior to the business relationship being formalised, for example, by signing of a client agreement or the acceptance by the customer of terms of business.

2. The Regulator does not consider that a Person would be a customer of a Relevant Person merely because such Person receives marketing information from a Relevant Person or where a Relevant Person refers a Person who is not a customer to a third party, including a Group member.

3. The Regulator considers that a Counterparty would generally be a customer for the purposes of the AML Rulebook and would therefore require a Relevant Person to undertake CDD on such a Person. However, this would not include a counterparty in a Transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ancillary business services for consumption by the Relevant Person such as cleaning, catering, stationery, IT or other similar services.

4. A Representative Office should not have any customer in relation to its GMC operations.

3.2.1 The following terms and abbreviations bear the following meanings for the purposes of these Rules.

Term	Definition
GMC	Means Gelephu Mindfulness City
GMC Board	Means the Board of Directors of GMC
GMC Entity	Means a Legal Person which is incorporated or registered in GMC, excluding a registered Branch.

Term	Definition
AML Rulebook	Means the Anti-Money Laundering and Sanctions Rules and Guidance Rulebook.
AML Return	Means the return which is required to be completed by Relevant Persons in accordance with AML 4.6.
AML/TFS	Means anti-money laundering, including measures undertaken against terrorist financing, proliferation financing, financing of unlawful organisations and sanctions non-compliance, and the observance of and compliance with applicable Sanctions including Targeted Financial Sanctions.
Authorised Person	Means a Person, other than a Licensed Body, who is authorised under the FSA.
Beneficial Owners	Means, in relation to a customer, a Natural Person who ultimately owns or controls the customer or a Natural Person on whose behalf a transaction is conducted or a business relationship is established and includes: 1. in relation to a body corporate, a Person referred to in Rule 8.3.3(2); 2. in relation to a Partnership, a Person referred to in Rule 8.3.4(2); 3. in relation to a trust or other similar Legal Arrangement, a Person referred to in Rule 8.3.5(2); and 4. in relation to a foundation, a Person referred to in Rule 8.3.6(2).
Body Corporate	Means any body corporate, including limited liability partnership and a body corporate constituted under the law of a country or territory outside of GMC.
Client	Means a Retail Client, Professional Client or Market Counterparty as defined in COBS 2.
Client Agreement	Means an agreement between an Authorised Person and a Client which is made or entered into in accordance with COBS 3.3.
Client Money	Means money of any currency which an Authorised Person holds on behalf of a Client, including any receivables of the Authorised Person in respect of bank accounts or clearing or brokerage accounts, or which an Authorised Person treats as Client Money, subject to the exclusions in COBS 14.2.6.
COBS	Means the Conduct of Business Rulebook.
Company	Includes: 1. any Body Corporate wherever incorporated; and 2. any unincorporated body constituted under the law of a country, territory or jurisdiction outside GMC.

Term	Definition
Company Service Provider	Means a Person that, carries out the following services on behalf of a customer: 1. acting as a formation agent of Legal Persons; 2. acting as, or arranging for another Person to act as, a director or secretary of a company, a partner of a partnership or a similar position in relation to other Legal Persons or Legal Arrangements; 3. providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other Legal Person or Legal Arrangement; 4. acting as, or arranging for another Person to act as, a trustee of an express trust or performing the equivalent function for another form of Legal Arrangement; or 5. acting as, or arranging for another Person to act as, a nominee shareholder for another Person.
Contract of Insurance	Has the meaning given in Part 4 of Schedule 1 of FSA.
Contravention	Means a contravention of any Regulations or Rules made by the GMC Board and the Regulator, as the case may be.
Correspondent Account	Means an account opened on behalf of a Correspondent Banking Client to receive deposits from, to make payments on behalf of or to otherwise handle financial transactions for or on behalf of the Correspondent Banking Client.
Correspondent Bank	Means a bank in a jurisdiction other than GMC where a Licensed Firm opens a Correspondent Account.
Correspondent Banking Client	Means a Client of a Licensed Firm which uses the firm's correspondent banking services account to clear transactions for its own customer base.
Counterparty	Means any Person with or for whom a Licensed Firm carries on, or intends to carry on, any regulated business or associated business. In this context, a Counterparty includes an individual, unincorporated association, Company, government, local authority or other public body.
Credit Rating Agency	Means a Person carrying on, in or from GMC, the Regulated Activity of Operating a Credit Rating Agency for which it has an authorisation under its Financial Services Licence.
Customer Due Diligence (CDD)	Has the meaning given in AML 8.3.

Term	Definition
Designated Non-Financial Business or Profession (DNFBP)	Means the following class of Persons who carry out the following businesses in GMC: 1. a real estate agency which carries out transactions with other Persons that involve the acquiring or disposing of real property; 2. a dealer in precious metals or precious stones; 3. a dealer in any saleable item of a price equal to or greater than USD15,000; 4. an accounting firm, audit firm, insolvency firm or taxation consulting firm; 5. a law firm, notary firm or other independent legal business; or 6. a Company Service Provider.
Director	Means: 1. In relation to an Undertaking established in GMC, a Person who appears on the Register of Directors maintained by the GMC Registrar of Companies; 2. In relation to all other Undertakings, a Person who has been admitted to a register which has a corresponding meaning to the Register of Directors or performs the function of acting in the capacity of a Director, by whatever name called; 3. who is employed or appointed by a Person in connection with that Person's business, whether under a contract of service or for services or otherwise; or 4. whose services, under an arrangement between that Person and a third party, are placed at the disposal and under the control of that Person.
eKYC	Means verification of customer identity by way of electronic, non-face-to-face means only.
eKYC System	Means the technology and associated processes used to undertake eKYC.
Employee	Means an individual: 1. who is employed or appointed by a Person in connection with that Person's business, whether under a contract of service or for services or otherwise; or 2. whose services, under an arrangement between that Person and a third party, are placed at the disposal and under the control of that Person.
Enhanced Customer Due Diligence or Enhanced CDD	Means undertaking Customer Due Diligence and the enhanced measures under AML 8.4.

Term	Definition
FATF	Means the Financial Action Task Force.
FATF Recommendations	Means the publication entitled the "International Standards on Combatting Money Laundering and the Financing of Terrorism andProliferation", as published and amended by the FATF from time to time by FATF.
FIU	Means the Financial Intelligence Unit of GMC.
Financial Crime	Includes: 1. fraud or dishonesty; 2. misconduct or misuse of information relating to a financial market; 3. handling the proceeds of crime; or 4. the financing of terrorism.
Financial Institution	Means: 1. a Licensed Firm; or 2. any Person that carries out as its principal business an activity which would be a Regulated Activity if carried out in GMC; and 3. that is not one of the following: a. a governmental organisation, including the Central Bank of Bhutan or its equivalent in any state; or b. a multilateral development bank.
Financial Services Licence	Means a permission given, or having effect as if so given, by the Regulator in accordance with Part 4 of FSA.
Financial Services Regulator	Means a regulator of financial services activities established in a jurisdiction other than GMC.
FSA	Means the GMC Financial Services Act 2025.
Governing Body	Means the board of directors, partners, committee of management or other governing body of an Undertaking.
Group	Has the meaning as defined in FSA.
Guidance	Has the meaning given in section 15(2) of FSA.
HM Treasury	Means the UK government’s economic and finance ministry.
IMF	Means the International Monetary Fund.
International Organisation	Means an organisation established by formal political agreement between member countries, where the agreement has the status of an international treaty, and the organisation is recognised in the law of countries which are members.

Term	Definition
Jurisdictions Subject to a Call for Action	Means jurisdictions identified by FATF as 'high-risk jurisdictions subject to a call for action' or any equivalent list of jurisdictions issued by FATF.
Jurisdictions Under Increased Monitoring	Means jurisdictions identified by FATF as 'jurisdictions under increased monitoring' or any equivalent list of jurisdictions issued by FATF.
Legal Arrangement	Means express trusts or other similar legal arrangements.
Legal Person	Means any entity other than a Natural Person that can establish a customer relationship with a Relevant Person or otherwise own property. This can include companies, Bodies Corporate or unincorporate, trusts, foundations, partnerships, associations, states and governments and other relevantly similar entities.
Listed Body Corporate	Means, for the purposes of Rule 8.3.3(4), a Body Corporate listed on a stock exchange recognised by the Regulator.
Local Terrorist List	Means any sanctions list issued by GMC or the Royal Government of Bhutan.
Money Laundering Reporting Officer (MLRO)	Means the Controlled Function described in the General Rulebook ("GEN") Rule 5.3.8 and for a Recognised Body, the Key Individual described in the Markets Infrastructure Rulebook ("MIR") Rule 2.3.2.
Natural Person	Means an individual.
Non-Face-to-Face (NFTF)	Where a customer is not physically present for a business operation or transaction with a Relevant Person.
Non-Profit Organisation (NPO)	Means a Legal Person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes or for other charitable purposes.
OECD	Means the Organisation for Economic Co-operation and Development.
OFAC	Means the Office of Foreign Assets Control of the U.S. Department of the Treasury.
Parent	Means a Holding Company.
Partner	Means, in relation to an Undertaking which is a Partnership, a Person occupying the position of a partner, by whatever name called.

Term	Definition
Partnership	Means any partnership, including a partnership constituted under the law of a country, jurisdiction or territory outside GMC, but not including a Limited Liability Partnership.
Payment Transaction	Has the meaning given in section 258 of FSA.
Person	A person includes any Natural Person, Body Corporate or body unincorporated, including a Legal Person, company, Partnership, unincorporated association, government or state.
Politically Exposed Person (PEP)	Means a Natural Person, and includes where relevant a family member or close associate, who is or has been entrusted with a prominent public function, including but not limited to, a head of state or of government, senior officials and functionaries of an international or supranational organisation, senior politician, senior government, judicial or military official, ambassador, senior executive of a state owned corporation, or an important political party official, but not middle ranking or more junior individuals in these categories.
Licensed Body	Means a Licensed Investment Exchange or a Licensed Clearing House.
Recognition Order	Has the meaning given in section 258 of FSA.
Regulated Activity	Has the meaning given in section 19 of FSA.
Regulated Financial Institution	A Person who does not hold a Financial Services Licence from the GFSO but who is licensed in a jurisdiction other than GMC to carry on any financial service by another Financial Services Regulator.
Regulation	Means any regulation made in GMC.
Regulator	Means the Gelephu Financial Services Office (“GFSO”).
Relevant Person	Has the meaning as defined in section 258 of FSA.
Representative Office	Means the business operations of Person authorised to carry on the Regulated Activity of Operating a Representative Office in GMC and which actually carries on the Regulated Activity of Operating a Representative Office.
RBA	Means a risk-based approach, as further detailed in Chapter 5.
Rule	Means any rule made by the Regulator in accordance with Part 2 of FSA.

Term	Definition
Sanctions	Means any law executing foreign policy, security, sanction, trade embargo, or anti-terrorism objectives or similar restrictions imposed, administered or enforced from time to time by: 1. GMC, GFSO or the Royal Government of Bhutan; 2. the United Nations Security Council; 3. the European Union; 4. HM Treasury of the United Kingdom; 5. the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury; 6. any other relevant governmental authority; 7. any relevant inter-governmental or supra-national authority; or 8. any of their successors.
Sanctions List	Means any official list of Persons, entities or groups targeted by Sanctions.
Senior Management	Means, in relation to a Relevant Person, every member of the Relevant Person's executive management and includes: 1. for a GMC Entity, every member of the Relevant Person's Governing Body; 2. for a Branch, the Person or Persons who control the day-to-day operations of the Relevant Person in GMC; 3. for an auditor, every member of the Relevant Person's executive management in GMC.
Shareholder	Means a Natural Person or legal entity governed by private or public law, who holds, directly or indirectly: 1. Shares of the Issuer in its own name and on its own account; 2. Shares of the Issuer in its own name, but on behalf of another Natural Person or legal entity; or 3. depository receipts, in which case the holder of the depository receipt shall be considered as the shareholder of the underlying Shares represented by the depository receipts.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated or licensed and which is not affiliated with a regulated financial Group that is subject to effective consolidated supervision.
Simplified Customer Due Diligence	Means Customer Due Diligence that has been modified pursuant to the operation of AML 8.5.
Source of Funds	Means the origin of customer's funds which relate to a Transaction or service and includes how such funds are connected to a customer's Source of Wealth.

Term	Definition
Source of Wealth	Means how the customer's global wealth or net worth is or was acquired or accumulated.
Spot Commodity	Has the meaning given in section 258 of FSA.
Suspicious Activity/Transaction Report (SAR/STR)	Means a report regarding suspicious activity, including a suspicious Transaction, made to the FIU.
Targeted Financial Sanctions (TFS)	Means financial sanctions issued by the UNSC against specific individuals, entities or groups in order to combat terrorism, terrorist financing and the proliferation of WMD, including those listed on the Local Terrorist List or the UNSC Consolidated List on this basis. Financial Sanctions include asset freezing and prohibitions on making funds or other assets or services directly or indirectly available for the benefit of the target of the relevant Sanctions.
Transaction	Means any transaction undertaken by a Relevant Person for or on behalf of a customer in the course of carrying on a business in or from GMC.
Undertaking	Means: 1. a Body Corporate or Partnership; or 2. an unincorporated association carrying on a trade or business, with or without a view to profit.
UN Consolidated List	Means the consolidated list of all individuals and entities subject to measures imposed by the UNSC.
UNSC	Means the United Nations Security Council.
Unlawful Organisation	Means an organisation, the establishment or activities of which have been declared to be criminal by GMC or the Royal Government of Bhutan.
Virtual Asset	Has the meaning given in section 258 of FSA.
Waiver	Means in relation to GEN 8.2 written notice provided under FSA.

4. GENERAL COMPLIANCE REQUIREMENTS

4.1 General requirements

4.1.1 (1) A Relevant Person must establish and maintain effective AML/TFS policies, procedures, systems and controls to prevent opportunities for money laundering, in relation to the Relevant Person and its activities.

(2) A Relevant Person's AML/TFS policies, procedures, systems and controls must:

(a) ensure compliance with GFSO laws and guidance;

(b) enable suspicious Persons and Transactions to be detected and reported;

(c) ensure the Relevant Person is able to provide an appropriate audit trail of a Transaction; and

(d) ensure compliance with any other obligation in these Rules.

(3) A Relevant Person must take reasonable steps to ensure that its Employees comply with the relevant requirements of its AML/TFS policies, procedures, systems and controls.

(4) A Relevant Person must review the effectiveness of its AML/TFS policies, procedures, systems and controls at least annually.

(5) The review process may be undertaken:

(a) internally by its internal audit or compliance function; or

(b) by a competent firm of independent auditors or compliance professionals.

(6) The review process required under Rule 4.1.1(4) must cover at least the following:

(a) a sample testing of customer documentation relevant to an assessment of the adequacy of the customer risk assessment or CDD performed by the Relevant Person;

(b) an analysis of all Suspicious Activity/Transaction Reports to highlight any area where procedures or training may need to be enhanced; and

(c) a review of the adequacy of the level of responsibility and oversight of the Relevant Person’s Governing Body and Senior Management in ensuring the Relevant Person has implemented and maintained adequate controls.

Guidance

Where appropriate, a Relevant Person should incorporate all material risks identified in the business risk assessment, including those that might arise with the introduction of a new business practice or introduction of new technology, within scope of the annual review under Rule 4.1.1(4).

4.1.2 If another jurisdiction's laws or regulations prevent or inhibit a Relevant Person from complying with these Rules, the Relevant Person must immediately inform the Regulator in writing.

4.2 Groups, branches and subsidiaries

4.2.1 (1) A Relevant Person which is a GMC Entity must ensure that its policies, procedures, systems and controls required by Rule 4.1.1 apply to:

(a) all of its branches or subsidiaries; and

(b) all of its Group entities in GMC.

(2) The requirement in 4.2.1 (1) does not apply if the Relevant Person can satisfy the Regulator that the relevant branch, subsidiary or Group entity is subject to regulation, including AML/TFS regulation, by a Financial Services Regulator or other competent authority in a country or jurisdiction with AML/TFS regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance with such regulations.

(3) Where the regulator in another jurisdiction does not permit the implementation of policies, procedures, systems and controls consistent with these Rules, the Relevant Person must:

(a) inform the Regulator in writing immediately; and

(b) apply appropriate additional measures to manage the money laundering risks posed by the relevant branch or subsidiary.

Guidance

A Relevant Person that is a GMC Entity should conduct a periodic review to verify that any branch or subsidiary operating in another jurisdiction is in compliance with the obligations imposed under these Rules.

4.2.2 A Relevant Person must:

(a) communicate the policies and procedures that it establishes and maintains in accordance with these Rules to its Group entities, branches and subsidiaries; and document the basis for its satisfaction that the requirement in Rule 4.2.1(1) is met.

Guidance

In relation to an Authorised Person, if the Regulator is not satisfied with respect to the AML/TFS compliance of its branches and subsidiaries in another jurisdiction, it may take action, including making it a condition of the Licensed Firm's Financial Services Licence that it must not operate a branch or subsidiary in that jurisdiction.

4.3 Group policies

4.3.1 A Relevant Person which is part of a Group must ensure that it:

(a) has developed and implemented policies and procedures for the sharing of information between Group entities, including the sharing of information relating to CDD and money laundering risks;

(b) has in place adequate safeguards on the confidentiality and use of information exchanged between Group entities, including consideration of relevant data protection legislation;

(c) remains aware of the money laundering risks of the Group as a whole and of its exposure to the Group and takes active steps to mitigate such risks;

(d) contributes to a Group-wide risk assessment to identify and assess money laundering risks for the Group; and

(e) provides its Group-wide compliance, audit and AML/TFS functions with customer account and Transaction information from its Branches and Subsidiaries when necessary for AML/TFS purposes.

4.4 Notifications

4.4.1 A Relevant Person must inform the Regulator in writing immediately if, in the course of its activities carried on in or from GMC or in relation to any of its Branches or Subsidiaries, it:

(a) receives a request for information from a regulator or agency in another jurisdiction responsible for AML/TFS or Sanctions regarding enquiries into potential money laundering;

(b) becomes aware, or has reasonable grounds to believe, that the following has or may have occurred in or through its business:

(i) money laundering;

(ii) a breach of Sanctions; or

(iii) acts amounting to bribery under the Organisation for Economic Co-operation and Development ("**OECD**") Convention on Combating Bribery of Foreign Public Officials in International Business Transactions;

(c) becomes aware of any money laundering or Sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or

(d) becomes aware of a significant breach of a Rule in the AML Rulebook.

4.4.2 A Relevant Person must inform the Regulator in writing as soon as possible if, in the course of its activities carried on in or from GMC, it suspects or becomes aware that another Person outside of its business is engaged in:

(a) money laundering;

(b) a breach of Sanctions; or

(c) acts amounting to bribery under the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

This requirement does not apply to information or documents that are legally privileged or available in the public domain.

4.5 Record keeping

4.5.1 A Relevant Person must, where relevant, maintain the following records for at least six years from the date on which the notification or report was made, the business relationship ends or the Transaction is completed, whichever occurs last:

(a) a copy of all documents and information obtained in undertaking during initial and ongoing CDD or due diligence on business partners;

(b) records, consisting of the original documents or certified copies, in respect of the customer business relationship, including:

(i) business correspondence and other information relating to a customer's account;

(ii) sufficient records of transactions to enable individual transactions to be reconstructed; and

(iii) internal findings and analysis relating to a transaction or any business, if the transaction or business appears unusual or suspicious, whether or not it results in a Suspicious Activity/Transaction Report;

(c) internal notifications of suspicious activity made to its MLRO under Rule 14.2.2;

(d) Suspicious Activity/Transaction Reports and any relevant supporting documents and information, including internal findings and analysis; any relevant communications with the FIU;

(e) the documents in Rule 4.6.1; and

(f) any other matter that the Relevant Person is expressly required to record under these Rules.

Guidance

A Relevant Person must comply with all applicable Rules on record keeping, regardless of whether or not it is outsourcing an element of its CDD process (see Rule 9.3). This includes the obligation for the Relevant Person to maintain a copy of all documents obtained during initial and ongoing CDD. When using eKYC for CDD, the Relevant Person should retain all the necessary data gathered during biometric authentication to ensure compliance with applicable Rules.

4.5.2 A Relevant Person must immediately provide to the Regulator, upon request, or a law enforcement agency, pursuant to a valid and enforceable request or requirement, a copy of the record referred to in Rule 4.5.1.

Guidance

The Regulator expects that a Relevant Person will be able to ordinarily provide the records within one Business Day of a request from the Regulator.

4.5.3 A Relevant Person must document, and provide to the Regulator immediately, any of the following:

(a) the risk assessment of its business as required by Rule 6.1.1;

(b) how the assessment in (a) was used for the purposes of complying with Rule 6.1.2;

(c) the risk assessment of the customer undertaken under Rule 7.1.1(1)(a); and

(d) the determination made under Rule 7.1.1(1)(b).

4.5.4 The records maintained by a Relevant Person must be kept in such a manner that:

(a) the Regulator or another competent third party is able to assess the Relevant Person's compliance with legislation applicable in GMC;

(b) any Transaction which was processed by or through the Relevant Person on behalf of a customer or other third party can be reconstructed;

(c) any customer or third party can be identified;

(d) all internal notifications of suspicious activity made to its MLRO under Rule 14.2.2, and all Suspicious Activity/Transaction Reports, can be identified; and

(e) the Relevant Person can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

Guidance

1. The records required to be kept under Rule 4.5.1 may be kept in electronic format, provided that such records are readily accessible and available to respond promptly to any requests from the Regulator for information.

2. If the date on which the business relationship with a customer ended is unclear, it may be taken to have ended on the date of the completion of the last Transaction.

4.5.5 Where the records referred to in Rule 4.5.1 are kept by a Relevant Person outside GMC, a Relevant Person must:

(a) take reasonable steps to ensure that the records are held in a manner consistent with these Rules;

(b) ensure that the records are easily accessible to the Relevant Person; and

(c) upon request by the Regulator, ensure that the records are immediately available for inspection.

4.5.6 A Relevant Person must:

(a) identify where there is secrecy or data protection legislation that might restrict access without delay to the records referred to in Rule 4.6.1; and

(b) where such legislation exists, obtain without delay certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons in (a).

4.5.7 A Relevant Person must be able to demonstrate that it has complied with the training and awareness requirements in Chapter 13 through appropriate measures, including the maintenance of relevant training records.

Guidance

The Regulator considers that "appropriate measures" in Rule 4.5.7 may include the maintenance of a training log setting out details of:

(a) the dates when the training was given;

(b) the nature of the training; and

(c) the names of Employees who received the training.

4.6 Annual AML Return

4.6.1 A Relevant Person must complete the prescribed AML Return form and submit it to the Regulator by the end of April each year. The AML Return must cover the period from 1 January to 31 December of the preceding year.

Guidance

1. The Regulator may grant a Waiver where a Relevant Person was licensed or authorised, as applicable, on or after 1 November of the relevant reporting year.

4.7 Co-operation with the Regulator

4.7.1 A Relevant Person must:

(a) be open and co-operative in all its dealings with the Regulator; and

(b) ensure that any communication with the Regulator is conducted in the English language.

4.8 Employee disclosures

4.8.1 A Relevant Person must ensure that it does not prejudice an Employee who discloses any information regarding money laundering to the Regulator or to any other relevant body involved in the prevention of money laundering.

Guidance

The Regulator considers that a "relevant body" in Rule 4.8.1 would include the FIU, any other law enforcement agencies, or the police.

5. APPLYING A RISK-BASED APPROACH TO AML/TFS

5.1 The risk-based approach

5.1.1 A Relevant Person must:

(a) assess and address its money laundering risks under the AML Rulebook by reviewing the risks to which the Relevant Person is exposed as a result of the nature of its business, customers, products, services and any other matters which are relevant in the context of money laundering; and

(b) ensure that any risk-based assessment undertaken for the purposes of complying with a requirement in the AML Rulebook is:

(i) objective and proportionate to the risks;

(ii) based on reasonable grounds;

(iii) properly documented; and

(iv) updated at appropriate intervals.

Guidance

1. Rule 5.1.1 requires a Relevant Person to adopt an approach to AML/TFS which is proportionate to the risks. This is called the "risk-based approach" ("**RBA**"). The Regulator expects the RBA to be a key part of the Relevant Person's AML/TFS compliance culture and to cascade down from the Senior Management to the rest of the organisation. Embedding the RBA within its business allows a Relevant Person to make decisions and allocate AML/TFS resources in the most efficient and effective way.

2. In implementing the RBA, a Relevant Person is expected to have in place processes to identify, assess, monitor, manage and mitigate money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks. Correspondingly, when the risks are lower, simplified measures are permitted. Simplified measures are not permitted where there is a suspicion of money laundering.

3. The RBA should not be seen as a "tick-box" approach to AML/TFS. Instead a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks, however, even where a customer is assessed through the RBA as being low-risk, a minimum of simplified CDD must be

undertaken in relation to that customer.

4. In adopting an RBA, a Relevant Person should continue to meet the requirements that are mandated under the AML Rulebook including:

   (a)

   (b) assessing the relevant money laundering risks in accordance with Chapter 6 or Chapter 7 of AML (as applicable);undertaking CDD in accordance with Rule 8.3.1;

   (c) undertaking Enhanced CDD pursuant to Rule 8.1.1(3) in accordance with Rule 8.4.1; and

   (d) undertaking Simplified CDD in accordance with Rule 8.5.1 where permissible pursuant to Rule 8.1.1(4).

5. Section 4.5 sets out the requirements regarding record-keeping for the purposes of the AML Rulebook. These Rules apply in relation to Rule 5.1.1(b)(iii).

6. BUSINESS RISK ASSESSMENT

6.1 Assessing the money laundering risks of a business

6.1.1 A Relevant Person must:

(a) take appropriate steps to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities. Relevant Persons must take into account that money laundering risks include the risk of terrorist financing, proliferation financing, the financing of unlawful organisations including non-compliance with Targeted Financial Sanctions.

(b) when identifying and assessing the risks in (a), take into account, to the extent relevant, any vulnerabilities relating to:

(i) its type of customers and their activities;

(ii) the countries or geographic areas in which it does business;

(iii) its products, services and activity profiles;

(iv) its distribution channels and business partners;

(v) the complexity and volume of its Transactions;

(vi) the development of new products and business practices including new delivery mechanisms, channels and partners;

(vii) the use of new or developing technologies for both new and pre-existing products and services; and

(c) take appropriate measures to ensure that any risk identified as part of the assessment in (a) is taken into account in its day-to-day operations and is mitigated, including in relation to:

(i) the development of new products;

(ii) the taking on of new customers; and

(iii) changes to its business profile.

6.1.2 A Relevant Person must use the information obtained in undertaking its business risk assessment to:

(a) develop and maintain its AML/TFS policies, procedures, systems and controls as required by Rule 6.2.1;

(b) ensure that its AML/TFS policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 6.1.1;

(c) assess the effectiveness of its AML/TFS policies, procedures, systems and controls as required by Rule 6.2.1(c);

(d) assist in the allocation and prioritisation of AML/TFS resources; and

(e) assist in the carrying out of the customer risk assessment under Chapter 7.

6.1.3 Without limiting compliance with Rules 6.1.1 and 6.1.2, prior to launching any new product, service, or business practice, or using a new or developing technology, a Relevant Person must take reasonable steps to ensure that it has:

(a) assessed and identified the money laundering risks relating to the product, service, business practice or technology; and

(b) taken appropriate steps to mitigate or eliminate the risks identified under (a).

Guidance

1. Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business from being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, the nature of the products and services sold, and the geographical operations in which it operates.

2. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers under Chapter 7.

3. In addition to assessing risk arising from money laundering, a business risk assessment should assess the potential exposure of a Relevant Person to other Financial Crime, such as fraud and the theft of personal data. The business risk assessment should also address the Relevant Person’s potential exposure to cyber security risk, as this risk may have a material impact on the Relevant Person’s ability to prevent Financial Crime.

4. A Relevant Person should, as a separate and distinct element of its business risk assessment, undertake a Targeted Financial Sanctions risk assessment in order to identify, understand, assess and mitigate those risks. This should include

conducting a proliferation financing and terrorist financing risk assessment.

5. A Relevant Person should, prior to launching any new product, service or business practice, pay specific attention to assessing the potential for risks associated with all applicable aspects of Financial Crime. This is especially important given the innovative nature of any such new offering as the Relevant Person may be less familiar with the functioning of the offering, compared to existing offerings.

6. Similarly, in using a new or developing technology, a Relevant Person should pay specific attention to assessing the potential for risks associated with Financial Crime that might arise as a result of implementing that innovative technology. For example, while the use of eKYC Systems may reduce the risk of impersonation fraud at customer onboarding, NFTF interaction with the customer may increase the risk of Financial Crime after a business relationship has been established, through transaction fraud, money laundering or theft of digitally stored CDD documentation.

7. A business risk assessment under Rule 6.1.1(b) should include an assessment of the risks associated with the carrying on of NFTF business, particularly the use of eKYC Systems.

6.2 AML/TFS systems and controls

6.2.1 A Relevant Person must:

(a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Relevant Person and its activities;

(b) ensure that its systems and controls in (a):

(i) include the provision to the Relevant Person's Senior Management of regular management information on the operation and effectiveness of its AML/TFS systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering risks;

(ii) enable it to determine whether a customer or a Beneficial Owner is a PEP;

(iii) enable the Relevant Person to comply with these Rules.

(c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML/TFS systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk

adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

Guidance

1. In Rule 6.2.1(c) the frequency of risk assessments will depend on the nature, size and complexity of the Relevant Person's business and also on when any material changes are made to its business. The risk assessments should also take into account a range of financial crime, including fraud, bribery and corruption.

2. The risk assessment under Rule 6.2.1(c) should identify actions to mitigate risks associated with undertaking NFTF business generally, and the use of eKYC specifically. This is because distinct risks are often likely to arise where business is conducted entirely in an NFTF manner, compared to when the business relationship includes a mix of face-to-face and NFTF interactions. The assessment should make reference to risk mitigation measures recommended by the Regulator and other relevant bodies.

7. CUSTOMER RISK ASSESSMENT

Guidance

1. This Chapter prescribes the risk-based assessment that must be undertaken by a Relevant Person on a customer and the proposed business relationship, Transaction or product. The outcome of this process is to produce a risk rating for a customer, which determines the level of CDD that must be undertaken in relation to that customer under Chapter 8. Chapter 8 prescribes the requirements of CDD, Enhanced CDD for high-risk customers and, where appropriate, Simplified CDD for low-risk customers.

2. CDD in the context of AML/TFS refers to the process of identifying a customer, verifying such identification and monitoring the customer's business and the potential for any money laundering risk on an ongoing basis. CDD is required to be completed following a risk-based assessment of the customer and the proposed business relationship, transaction or product.

3. Relevant Persons should note that the ongoing CDD requirements in Rule 8.6.1 require a Relevant Person to review a customer's risk rating to ensure that it remains appropriate in light of the potential money laundering risks.

4. The risk-based assessment of the customer and the proposed business relationship, Transaction or product required under this Chapter is required to be undertaken prior to the establishment of a business relationship with a customer. Because the risk rating assigned to a customer resulting from this assessment determines the level of CDD that must be undertaken for that customer, this process must be completed before the CDD is completed for the customer. The Regulator is aware that in practice there will often be some degree of overlap between the customer risk assessment and CDD. For example, a Relevant Person may undertake some aspects of CDD, such as identifying Beneficial Owners, when it performs a risk assessment of the customer. Conversely, a Relevant Person may also obtain relevant information as part of CDD which has an impact on its customer risk assessment. Where information obtained as part of CDD of a customer affects the risk rating of a customer, the change in risk rating should be reflected in the degree of CDD undertaken.

7.1 Assessing the money laundering risks of a customer

7.1.1 (1) A Relevant Person must:

(a) undertake a risk-based assessment of every customer; and

(b) assign the customer a risk rating proportionate to the assessed money laundering risks associated with the customer.

(2) The customer risk assessment in (1) must be completed:

(a) prior to establishing a business relationship with a customer;

(b) on a periodic basis, in accordance with Rule 8.6.1(e); and

(c) whenever it is otherwise appropriate for existing customers, including where the Relevant Person becomes aware of any change to the risk factors associated with the customer that might contribute to the potential for money laundering risk to increase materially.

(3) When undertaking a risk-based assessment of a customer under 7.1.1(1)(a), a Relevant Person must identify, assess and consider:

(a) the customer and any Beneficial Owners;

(b) the purpose and intended nature of the business relationship, and the nature of the customer's business;

(c) the nature, ownership and control structure of the customer, its beneficial ownership (if any) and its business;

(d) the customer's country of origin, residence, nationality, place of incorporation or place of business;

(e) the relevant product, service or Transaction;

(f) in relation to life insurance or other similar insurance policies, the beneficiary of the policy and Beneficial Owners of the beneficiary; and

(g) the outcomes of the business risk assessment undertaken under Chapter 6.

7.1.2 (1) When undertaking a risk-based assessment of a customer and considering whether or not to assign a high-risk rating under 7.1.1(1)(b), a Relevant Person must take into account all relevant risk factors that would reasonably apply to the customer, including but not limited to:

(a) customer risk factors, including whether the:

(i) business relationship is conducted in unusual circumstances;

(ii) customer is resident, established, registered or conducts business in a geographical area or jurisdiction of high risk (as set out in paragraph (c));

(iii) customer is a Legal Person or a Legal Arrangement that is a vehicle for holding personal assets;

(iv) customer is a company that has nominee shareholders or shares in bearer form;

(v) customer is a business that is cash intensive, such as a business that receives a majority of its revenue in cash;

(vi) corporate structure of the customer or any group to which it belongs is unusual or excessively complex given the nature of the business;

(b) product, service, transaction or delivery channel risk factors, including whether:

(i) the service involves private banking;

(ii) the product, service or transaction is one that might allow for anonymity or obfuscation of the true identity of any of the parties involved in the transaction;

(iii) the situation involves NFTF business relationships or transactions, or lacks appropriate safeguards, such as electronic signatures or eKYC;

(iv) payments will be received from unknown or unassociated third parties;

(v) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in another country;

(vi) new products and new business practices are involved, including new delivery mechanisms or the use of new or developing technologies for both new and pre-existing products; and

(c) geographical or jurisdictional risk factors, including whether the relevant country or countries:

(i) are identified by credible sources, as:

(A) not having effective systems to counter money laundering; or

(B) not implementing requirements to counter money laundering that are consistent with FATF Recommendations;

(ii) are identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering or the production and supply of illicit drugs;

(iii) are subject to Sanctions, embargos or similar measures issued by, for example, the United Nations or the State;

(iv) are identified by credible sources as providing funding or support for terrorism;

(v) have organisations operating within their territory that have been designated by the State, other countries or International Organisations as terrorist organisations.

(2) For the purposes of 7.1.2(1)(c), a credible source includes, but is not limited to, mutual evaluations reports, detailed assessment reports or follow-up reports issued by FATF, the International Monetary Fund ("**IMF**"), the World Bank, the OECD and other International Organisations.

7.1.3 (1) When undertaking a risk-based assessment of a customer and considering whether or not to assign a low-risk rating under 7.1.1(1), a Relevant Person must take into account all relevant risk factors that would reasonably apply to the customer, including but not limited to:

(a) customer risk factors, including whether the customer is:

(i) a public body or a publicly owned enterprise;

(ii) resident, established, registered or conducts business in a geographical area or jurisdiction of lower risk (as set out in paragraph (c));

(iii) A Licensed Firm;

(iv) a Regulated Financial Institution that is subject to regulation and supervision, including AML/TFS regulation and supervision, in a jurisdiction with AML/TFS regulations that are equivalent to the standards set out in the FATF Recommendations;

(v) a Subsidiary of a Regulated Financial Institution referred to in (iv), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML/TFS standards as its Parent;

(vi) a company whose Securities are listed by the Regulator, another Financial Services Regulator or a Regulated Exchange, which is subject to disclosure obligations broadly equivalent to those set out in the Market Rules;

(vii) a law firm, notary firm or other legal business that carries on its business in GMC;

(viii) an accounting firm, insolvency firm, auditor or other audit firm that carries on its business in GMC;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(i) a Contract of Insurance which is non-life insurance;

(ii) a Contract of Insurance which is a life insurance product with no investment return or redemption or surrender value;

(iii) an insurance policy for a pension scheme that does not provide for an early surrender option, and cannot be used as collateral;

(iv) a pension, superannuation or similar scheme that satisfies the following conditions:

(A) the scheme provides retirement benefits to employees;

(B) contributions to the scheme are made by way of deductions from wages; and

(C) the scheme rules do not permit the assignment of a member's interest under the scheme.

(v) a product where the risks of money laundering are adequately managed by other factors such as transaction limits or transparency of ownership; and

(c) geographical and jurisdictional risk factors, including whether a country or countries:

(i) are identified by credible sources as having effective systems to counter money laundering;

(ii) are identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, or the production and supply of illicit drugs;

(iii) have been assessed by credible sources, as having:

(A) requirements to counter money laundering that are consistent with the FATF Recommendations; and

(B) effectively implement FATF Recommendations.

(2) For the purposes of 7.1.3(1)(c), a credible source includes, but is not limited to, mutual evaluations, detailed assessment reports or follow-up reports issued by FATF, the IMF, the World Bank, the OECD and other International Organisations.

Guidance on the customer risk assessment

1. The risk assessment of a customer requires a Relevant Person to allocate an appropriate risk rating to the customer. Risk ratings should be either descriptive, such as "low", "medium" or "high", or a sliding, ordinal numeric scale such as 1 for the lowest risk to 10 for the highest, with at least three differentiated risk ratings. All the factors set out in both 7.1.2 and 7.1.3 should be considered in order to assess and allocate the appropriate risk rating to the customer.

2. Depending on the outcome of a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide to what degree CDD will need to be performed. For a customer exhibiting significant potential risk for money laundering the Relevant Person is required to carry out Enhanced CDD under Rule 8.4, in addition to the normal CDD required under Rule 8.3. For a customer rated low risk, the Relevant Person may be able to carry out Simplified CDD under Rule 8.5. For any other customer, the Relevant Person must undertake CDD under Rule 8.3.

3. Using the RBA, a Relevant Person could, when assessing two customers with near identical risk profiles, consider that one is high-risk and the other low-risk. This may occur, for example, where both customers may be undertaking the same high-risk activity, but one customer may be a customer in relation to a low-risk product, or may be a long-standing customer of a Group company which has been introduced to the Relevant Person.

Guidance on high-risk customers

1. When assessing the risk factors referred to in 7.1.2(1), the presence of one or more risk factors may not always indicate a high risk of money laundering in a particular situation.

2. An example of a business relationship conducted in unusual circumstances, for

the purposes of Rule 7.1.2(1)(a)(i), would include, but is not limited to a business relationship or proposed business relationship that involves, or would involve, significant unexplained geographic distance between the location of the Relevant Person and the customer or proposed customer.

3. The highest risk products or services in respect of money laundering are those where unlimited third-party funds can be freely received from or paid to third parties, without evidence of the identity of the third parties being obtained and the identity being verified.

4. Money laundering risks are likely to be increased if a Person is able to hide behind corporate structures such as limited companies, trusts, special purpose vehicles and nominee arrangements. When devising its internal procedures, a Relevant Person should consider how its customers and operational systems impact the capacity of its staff to identify suspicious activities and Transactions. Generally, the lowest risk products in respect of money laundering are those where funds can only be received from a named customer by way of payment from an account held in the customer's name, and similarly where the funds can only be remitted to a named customer.

Guidance on low-risk customers

When assessing the risk factors referred to in 7.1.3(1), a Relevant Person must bear in mind that the presence or absence of one or more risk factors may not always indicate a high or low risk of money laundering respectively in a particular situation.

7.2 Prohibition on establishing business relationships with certain customers

7.2.1 A Relevant Person must not establish a business relationship with a prospective customer that is a Legal Person or Legal Arrangement if the ownership or control arrangements of the customer prevents the Relevant Person from identifying one or more of the customer's Beneficial Owners.

7.2.2 A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

7.2.3 A Relevant Person must not knowingly establish or maintain an anonymous account, an account in a fictitious name, or a nominee account which is held in the name of one Person but which is controlled by or held for the benefit of another Person whose true identity has not been disclosed to the Relevant Person.

Guidance

1. In Rule 7.2.1, ownership arrangements which may prevent the Relevant Person from identifying one or more Beneficial Owners include bearer shares and other negotiable instruments in which ownership is determined by possession.

2. A Shell Bank is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial Group that is subject to effective consolidated supervision. The Regulator does not consider that the existence of a local agent or low-level staff constitutes physical presence.

7.2.4 If a Relevant Person uses a numbered account with an abbreviated name, it must ensure that:

(a) such an account is used only for internal purposes;

(b) it has undertaken the same CDD procedures in relation to the account holder as are required for other account holders;

(c) it maintains the same information in relation to the account and account holder as is required for other accounts and account holders; and

(d) staff performing AML/TFS functions, including staff responsible for identifying and monitoring transactions for suspicious activity, and staff performing compliance and audit functions, have full access to information about the account and the account holder.

Guidance on anonymous accounts

A Relevant Person should note that, in addition to the prohibition in Rule 7.2.3 against knowingly establishing anonymous accounts, accounts in a fictitious name or nominee accounts, Relevant Persons are prohibited from opening of accounts held under borrowed, mock or fake names or accounts designated solely with numbers and without the names of account holders.

8. CUSTOMER DUE DILIGENCE

8.1 Requirement to undertake Customer Due Diligence

8.1.1 (1) A Relevant Person that is a Licensed Firm or a Recognised Body must undertake CDD under Rule 8.3.1 where the Relevant Person:

(a) establishes a business relationship with a customer;

(b) carries out an occasional Transaction for a customer that is of an amount equal to or more than USD15,000;

(c) suspects a customer of, or a Transaction to be for the purposes of, money laundering; or

(d) doubts the veracity or adequacy of any document or information previously provided by, or obtained for, a customer in relation to (a), (b) or (c) above.

(2) A Relevant Person that is a DNFBP must undertake CDD under Rule 8.3.1 where it:

(a) is a real estate agency and it prepares for or is involved in a Transaction, or the provision of real estate agency services to a Person, that involves the buying and selling of real property;

(b) is a dealer in precious metals or precious stones and it is involved in a Transaction in cash that amounts to USD15,000 or more, whether or not the Transaction is executed in a single operation or in several operations that are or appear to be linked;

(c) is a dealer in any saleable item of a price equal to or greater than USD15,000 and it is involved in a Transaction in cash that amounts to USD15,000 or more, whether or not the Transaction is executed in a single operation or in several operations that are or appear to be linked;

(d) is an accounting firm, audit firm, insolvency firm or taxation consulting firm and it prepares for or is involved in the provision of accounting, auditing, insolvency or taxation consulting services to a Person;

(e) is a law firm, notary firm or other independent legal business and it prepares for or is involved in the provision of legal or notarial services to another Person participating in financial or real property Transactions concerning the following activities:

(i) the buying and selling of real property;

(ii) the managing of client money, securities or other assets;

(iii) the management of bank, savings or securities accounts;

(iv) the organisation of contributions for the creation, operation or management of companies; or

(v) the creation, operation or management of legal persons or arrangements, and buying and selling of business entities;

(f) is a Company Service Provider and it prepares for or is involved in the provision of any of the following services to another Person:

(i) acting as a formation agent of Legal Persons or Legal Arrangements;

(ii) acting as, or arranging for another Person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other Legal Persons or Legal Arrangements;

(iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other Legal Person or Legal Arrangement;

(iv) acting as, or arranging for another Person to act as, a trustee of an express trust or performing the equivalent function for another form of Legal Arrangement; or

(v) acting as, or arranging for another Person to act as, a nominee shareholder for another Person.

(3) In addition to undertaking CDD in accordance with Rule 8.3.1, a Relevant Person must undertake Enhanced CDD in accordance with Rule 8.4.1 for each of its customers assigned a high-risk rating;

(4) A Relevant Person may undertake Simplified CDD in accordance with Rule 8.5.1 by modifying the CDD undertaken in accordance with Rule 8.3.1 for any customer assigned a low-risk rating.

Guidance

1. Relevant Persons are reminded that they are required to comply with any notices and guidance issued by the FIU relating to CDD and Suspicious Activity/Transaction Reports.

2. The FIU requires:

(a) a DNFBP that is a dealer in precious metals or precious stones to obtain relevant identification documents, such as passport and trade licence, as applicable, and report to the FIU for all cash transactions equal to or exceeding USD15,000 with individuals and all cash or wire transfer transactions equal to or exceeding USD15,000 with entities. The Regulator expects a dealer in any saleable item or a price equal to or greater than USD15,000 to also comply with this requirement;

(b) a DNFBP that is a real estate agent to obtain relevant identification documents, such as passport and trade licence, as applicable, and report to the FIU for all sales or purchases of Real Property where:

(i) the payment for the sale/purchase includes a total cash payment of USD15,000 or more whether in a single cash payment or multiple cash payments;

(ii) the payment for any part or all of the sale/purchase amount includes payment(s) using Virtual Assets;

(iii) the payment for any part or all of the sale/purchase amount includes funds that were converted from or to a Virtual Asset.

8.1.2 (1) A Relevant Person must also apply CDD measures to each existing customer under Rules 8.3.1, 8.4.1 or 8.5.1 as applicable:

(a) with a frequency appropriate to the outcome of the risk-based approach taken in relation to each customer; and

(b) when the Relevant Person becomes aware that any circumstances relevant to its risk assessment for a customer have changed.

(2) For the purposes of 8.1.2(1), in determining when it is appropriate to apply CDD measures in relation to existing customers, a Relevant Person must take into account, amongst other things:

(a) any indication that the identity of the customer, or the customer's Beneficial Owners, has changed;

(b) any Transactions that are not reasonably consistent with the Relevant Person's knowledge of the customer;

(c) any change in the purpose or intended nature of the Relevant Person's relationship with the customer; or

(d) any other matter that might affect the Relevant Person's risk assessment of the customer.

Guidance

1. A Relevant Person should undertake appropriate CDD in a manner proportionate to the customer's money laundering risks. This means that all customers are subject to CDD under Rule 8.3.1. However, for high-risk customers, additional Enhanced Customer Due Diligence measures should also be undertaken under Rule 8.4.1. For customers having a low-risk rating, the requirements under Rule 8.3.1 may be modified according to the assessed risk, in accordance with Rule 8.5.1.

2. The frequency for undertaking CDD for existing customers will be determined by the risk rating assigned to a particular customer. The Regulator expects that customers rated high risk for money laundering should be reviewed more frequently than customers rated lower risk for money laundering.

3. A Relevant Person should undertake CDD to guard against a range of money laundering risks as well as a range of financial crime risks, including fraud.

8.2 Timing of Customer Due Diligence

8.2.1 (1) For a Relevant Person that is a Licensed Firm or Licensed Body:

(a) the appropriate CDD obligations, subject to (1)(b), must be fulfilled before the Relevant Person undertakes any transaction on behalf of the customer or when undertaking an occasional transaction under 8.1.1(1)(b).

(b) the Relevant Person does not have to fulfil the verification of the identity of a customer and Beneficial Owners obligations under the AML Rules before undertaking a Transaction for a customer or occasional transaction where it has, on reasonable grounds, established that:

(i) there is little risk of money laundering and that risk is effectively managed; and

(ii) doing so would interrupt or delay the normal course of business in respect of effecting the Transaction.

(2) (a) A Relevant Person that is a DNFBP must fulfil the appropriate CDD and reporting obligations where applicable before the Relevant Person prepares for or carries out a Transaction or provision of a service in Rule 8.1.1(2)(a), (d), (e) or (f).

(b) A Relevant Person that is a DNFBP as a result of carrying on one or more of the business activities referred to in Rule 8.1.1(2)(b) or (c) must fulfil the appropriate CDD and reporting obligations where applicable before the Relevant Person prepares for or carries out a transaction that includes a total cash payment of USD15,000 or more, whether in a single cash payment or multiple cash payments.

(3) The Relevant Person does not have to fulfil the verification of the identity of a customer and Beneficial Owners obligations under the AML Rules preparing for or carrying out a Transaction for its customer concerning those business activities referred to in Rule 8.1.1(2) where it has, on reasonable grounds, established that:

(i) there is little risk of money laundering and that risk is effectively managed; and

(ii) doing so would interrupt or delay the normal course of business in respect of effecting the Transaction.

(4) A Relevant Person that has relied on Rule 8.2.1(1)(b) or 8.2.1(3) must fulfil its CDD obligations as soon as practicable after effecting the Transaction.

(5) Where the Relevant Person, having relied on Rule 8.2.1(1)(b) or 8.2.1(3) is unable to complete the verification of the identity of a customer and any Beneficial Owners within twenty Business Days of effecting a Transaction or occasional transaction it must:

(a) consider the circumstances and determine whether to make an internal notification of suspicious activity to the MLRO under Rule 14.2.2;

(b) where it has determined that it is unnecessary to make such a report, return to the customer any monies associated with the Transaction or occasional transaction, excluding any reasonable costs incurred by the Relevant Person;

(c) where it has determined that it is necessary to make such a report, not return any monies or provide any investments to the customer, unless instructed to do so by the MLRO and otherwise act in accordance with instructions issued by the MLRO; and

(d) not establish any further business relationship with that customer until the verification process has been completed for that customer in accordance with these Rules.

8.2.2 (1) A Relevant Person must ensure that its AML/TFS systems and controls referred to in Rule 6.2.1 include risk management policies and procedures

concerning the conditions under which business relationships may be established with a customer before completing verification of the identity of a customer and Beneficial Owners.

Guidance

1. Examples of situations that might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained might be where: there is a suspicion of money laundering in relation to that customer; there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile; or it appears to the Relevant Person that a Person other than the nominal customer is the real customer.

2. Situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period or executing a time critical Transaction which, if not executed immediately, would or may cause a customer to incur a financial loss due to price movement or loss of opportunity or when a customer seeks immediate insurance cover.

3. When complying with Rule 8.2.1, a Relevant Person should also, where relevant, consider Rule 8.7.1 regarding failure to conduct or complete CDD and Chapter 14 regarding Suspicious Activity/Transaction Reports and tipping off.

8.3 Customer Due Diligence requirements

8.3.1 (1) In undertaking CDD, a Relevant Person must:

(a) identify the customer and verify the customer's identity including identification and verification of the identity of any Person purporting to act on behalf of the customer;

(b) identify all the Beneficial Owners and take reasonable measures to verify the identity of the Beneficial Owners, such that the Relevant Person is satisfied that it knows who the Beneficial Owners are;

(c) assess and understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship; and

(d) conduct ongoing due diligence of the business relationship as required under Rule 8.6.1.

(2) In addition to complying with 8.3.1 (1)(a), for life insurance or other similar policies, a Relevant Person must:

(a) record the names of beneficiary(ies) in the policy;

(b) verify the identity of all Persons in all classes of beneficiaries when a payout of the policy is due;

(c) undertake the measures referred to in (a) and (b) as soon as the beneficiary of the policy is identified or designated; and

(d) verify the identity of beneficiaries and any Beneficial Owners of a beneficiary before it makes a payout under the policy.

(3) A Relevant Person must have systems and controls in place and take reasonable measures to determine whether:

(a) a customer,

(b) any Beneficial Owners of the customer; or

(c) for a life insurance or other similar policy, any beneficiary of the policy, or any Beneficial Owners of a beneficiary;

(4) If a PEP is identified under 8.3.1(3), then the Relevant Person must, in addition to CDD under 8.3.1, undertake Enhanced CDD under 8.4.1.

8.3.2 (1) For the purposes of Rule 8.3.1(1)(a), a Relevant Person must identify a customer and verify the customer's identity in accordance with this Rule.

(2) If a customer is a Natural Person, a Relevant Person must obtain and verify information about the person's:

(a) full name (including any alias);

(b) date of birth;

(c) nationality;

(d) legal domicile; and

(e) current residential address, other than a post office box.

(3) If a customer is a Body Corporate, the Relevant Person must obtain and verify:

(a) the full name of the Body Corporate and any trading name;

(b) the address of its registered office and, if different, its principal place of business;

(c) the date and place of incorporation or registration;

(d) relevant corporate documents of the customer; and

(e) the full names of the members of its Governing Body and persons exercising a senior management position.

(4) If a customer is a foundation, the Relevant Person must obtain and verify:

(a) a certified copy of the charter and by-laws of the foundation or any other documents constituting the foundation; and

(b) documentary evidence of the appointment of the guardian or any other person who may exercise powers in respect of the foundation.

(5) If a customer is a trust or other similar Legal Arrangement, the Relevant Person must obtain and verify:

(a) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement; and

(b) documentary evidence of the appointment of the trustee or any other person exercising powers under the trust or arrangement.

Guidance on CDD

1. The information required under 8.3.2(2)(a) and (b) should be obtained through a review of an original, current, valid passport or, where a customer does not own a passport, an official identification document which includes a photograph. For the purposes of Rule 8.3.2(2)(a) and (b), an official government identification document in digital form and issued by a governmental competent authority is considered valid.

2. A Relevant Person should ensure that any documents used for the purpose of identification are original documents, whichever format they are in, including digital.

3. The verification of a customer's identity, including their address, should be based on official documents. Where that is not possible, a Relevant Person should consider using additional documents or information obtained from different independent sources to verify identity. Any lack of official documents and alternative means of verification should lead the Relevant Person to re-assess the customer's risk classification and the associated level of due diligence to be undertaken.

4. [*Not in use*]

5. The Relevant Person must always verify the address of a customer subject to Enhanced Customer Due Diligence under Rule 8.4.1.

6. Where personal identity documents, such as a passport, identity card or other identification documentation cannot be reviewed in original form, the identification documentation provided should be certified as a true copy of the original document by any one of the following:

   (a) a registered lawyer;

   (b) a registered notary;

   (c) a chartered accountant;

   (d) a government ministry;

   (e) a post office;

   (f) a police officer; or

   (g) an embassy or consulate.

   The individual or authority undertaking the certification should be contactable if necessary. Where a copy of an original identification document is made by a Relevant Person, the copy should be dated, signed and marked with 'original sighted'.

7. In complying with Rule 8.3.2(2), a Relevant Person should take reasonable steps to identify whether a customer has more than one nationality or residency rights in jurisdictions other than their jurisdiction of birth. The existence of such residency rights or dual nationality may be a potential risk factor and should be considered as such in the customer risk assessment required by Rule 7.1.1(3) and Rule 7.1.2.

8. Where a Relevant Person uses eKYC for CDD purposes, appropriate measures must be adopted to mitigate the risks that may arise from eKYC processes and the use of an eKYC System. A Relevant Person must ensure that eKYC is secure and effective, includes an appropriate combination of authentication factors when verifying the identity of the customer and ensure it is at least as stringent as face-to-face CDD. Measures should be in place to verify the authenticity of any official government identification document and the actual customer.

9. When employing an eKYC System to assist with CDD, a Relevant Person should:

   a. ensure that it has a thorough understanding of the eKYC System itself and the risks of eKYC, including those outlined by relevant guidance from FATF and other international standard setting bodies;

b. comply with all the Rules of the Regulator relevant to eKYC including, but not limited to, applicable requirements regarding the business risk assessment, as per Rule 6.1, and outsourcing, as per Rule 9.3;

c. combine eKYC with transaction monitoring, anti-fraud and cyber-security measures to support a wider framework preventing applicable Financial Crime; and

d. take appropriate steps to identify, assess and mitigate the risk of the eKYC system being misused for the purposes of Financial Crime.

10. In undertaking CDD, a Relevant Person that is a Licensed Body should have regard to the provisions of the Market Infrastructure Rulebook ("**MIR**") requiring appropriate measures be taken to prevent money laundering, Market Abuse and Financial Crime, including those set out at MIR 2.8.5(c) and MIR 2.9.

8.3.3 (1) For the purposes of Rule 8.3.1(1)(b), and subject to (4), a Relevant Person must identify the Beneficial Owners of a Body Corporate in accordance with this Rule.

(2) The Relevant Person must identify any Natural Person who:

(a) owns or controls (in each case whether directly or indirectly) 25% or more of the shares or voting rights in the Body Corporate;

(b) controls the Body Corporate; or

(c) exercises ultimate control over the management of the Body Corporate.

(3) For the purposes of (2)(b), a Natural Person controls a Body Corporate if such person:

(a) holds, directly or indirectly:

(i) 25% or more of the Body Corporate's shares;

(ii) 25% or more of the voting rights in the Body Corporate; or

(iii) the right to appoint or remove a majority of the board of directors of the Body Corporate; or

(b) has the right to exercise, or actually exercises, significant influence or control over the Body Corporate.

(4) A Relevant Person is not required to comply with Rule 8.3.1(1)(b) if the customer is:

(a) a Listed Body Corporate; or

(b) a Body Corporate that is wholly-owned by any of the government bodies of GMC or Bhutan.

8.3.4 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a Partnership in accordance with this Rule.

(2) The Relevant Person must identify any Natural Person who:

(a) ultimately is entitled to or controls (in each case whether directly or indirectly) 25% or more share of the capital or profits of the Partnership or 25% or more of the voting rights in the Partnership; or

(b) otherwise exercises ultimate control over the management of the Partnership.

8.3.5 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a customer that is a trustee of a trust or an equivalent position in respect of a similar Legal Arrangement in accordance with this Rule.

(2) The Relevant Person must identify:

(a) the settlor of the trust;

(b) any other trustee(s) aside from the customer;

(c) each beneficiary of the trust;

(d) where the persons or some of the persons benefiting from the trust have not been determined, the class of persons in whose main interest, in the opinion of the Registrar, the trust has been established or operates; and

(e) any Natural Person who has control over the trust.

(3) For the purposes of (2)(e) "control" means a power, whether exercisable alone, jointly with another person or with the consent of another person, under the trust instrument or by law to:

(a) dispose of, advance, lend, invest, pay or apply trust property;

(b) vary or terminate the trust;

(c) add or remove a person as a beneficiary to or from a class of beneficiaries;

(d) appoint or remove trustees or give another person control over the trust; and

(e) direct, withhold consent to or veto the exercise of a power mentioned in sub-paragraphs (a) to (d).

(4) Where any of the persons identified under (2)(a) to (e) are fulfilled by a Body Corporate or Partnership, the Relevant Person must identify the Beneficial Owners of Body Corporate or Partnership in accordance with Rule 8.3.3 and Rule 8.3.4.

8.3.6 (1) For the purposes of Rule 8.3.1(1)(b), a Relevant Person must identify the Beneficial Owners of a customer that is a foundation or other Legal Arrangement similar to a foundation in accordance with this Rule.

(2) The Relevant Person must identify:

(a) the founder;

(b) the foundation council members, or otherwise members of the governing body of the foundation;

(c) the guardian, if any;

(d) the beneficiaries, if named, or designee if no beneficiaries are named, in whose main interest, in the opinion of the Relevant Person, the foundation or arrangement has been established or operates; and

(e) any Natural Person who has control over the foundation or other Legal Arrangement.

(3) For the purposes of (2)(e), a Natural Person shall have "control" over a foundation or a Legal Arrangement if such person:

(a) holds, directly or indirectly, 25% or more of the voting rights in the conduct and management of the foundation or the Legal Arrangement; or

(b) holds the right, directly or indirectly, to appoint or remove a majority of the officials of the foundation or the Legal Arrangement.

(4) Where any of the persons identified under (2)(a) to (d) are a Body Corporate or Partnership, the Relevant Person must identify the Beneficial Owners of Body Corporate or Partnership in accordance with Rule 8.3.3 and Rule 8.3.4.

Guidance on verification of the identity of Beneficial Owners

1. In determining whether an individual meets the definition of Beneficial Owners, regard should be given to all the circumstances of the case, in particular the size of an individual's legal engagement or beneficial ownership in a Transaction.

2. For a retail investment fund that is widely-held and where the investors invest via pension contributions, the Regulator would not expect the manager of the fund to look through to any underlying investors where there are none with any material control or ownership of the fund. However, for a closely-held fund with a small number of investors, each having a large shareholding or other interest, the Regulator would expect a Relevant Person to identify and verify each of the Beneficial Owners, depending on the risks identified as part of its risk-based assessment of the customer. For a corporate health policy with defined benefits, however, the Regulator would not expect a Relevant Person to identify the Beneficial Owners.

3. An eKYC System may be used as part of the identification and verification of Beneficial Owners. When determining whether to use the eKYC System to assist in the CDD of a Beneficial Owner, a Relevant Person should establish if the eKYC System used allows it to comply fully with the relevant Rules in relation to CDD.

Guidance on Politically Exposed Persons (PEPs) and corruption

1. Individuals who have, or have had, a high political profile, or hold, or have held, public office, may pose a higher money laundering risk to a Relevant Person as their position may make them prone to corruption. This risk also extends to members of their families and to known close associates. Being a PEP does not, in itself, of course, incriminate individuals or entities.

2. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such a Person, if he were undertaking money laundering, would attempt to place his money offshore, away from his home jurisdiction, where he is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his home jurisdiction to confiscate or freeze his criminal proceeds.

3. A Relevant Person should be aware that customer relationships with family members or close associates of PEPs involve similar risks to those with PEPs themselves.

4. The risk of corruption-related money laundering increases where a Relevant Person deals with a PEP. Corruption may involve serious crimes and has become the subject of increasing global concern. Corruption offences are predicate AML crimes.

5. The Regulator considers that after leaving office, a PEP remains a higher risk for money laundering if such an individual continues to exert political influence or otherwise poses a risk of being involved in corruption.

6. The fact that an individual is a PEP does not automatically mean that the individual must be assessed to be a high-risk customer: however, Enhanced CDD still needs to be undertaken on PEPs. A Relevant Person will need to assess the particular circumstances relating to each PEP to determine what risk category is appropriate.

Guidance on FATF Jurisdictions Under Increased Monitoring / Subject to a Call for Action

1. A Relevant Person should maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action and screen them for potential exposure as part of CDD. Customer exposure to jurisdictions appearing on these lists should be taken into account when developing and applying risk-based measures relating to CDD. Customers exposed to such jurisdictions may present higher money laundering risks and specific counter-measures including Enhanced CDD may be required.

8.4 Enhanced Customer Due Diligence

8.4.1 Where a Relevant Person is required to undertake Enhanced CDD, having assigned a customer a high-risk rating or it or its Beneficial Owners is a PEP, then, in addition to CDD under Rule 8.3.1, it must:

(a) obtain:

(i) additional identification information on the customer and all Beneficial Owners;

(ii) additional information on the intended nature of the business relationship;

(iii) information on the reasons for a Transaction;

(b) update the CDD information which it holds on the customer and any Beneficial Owners more regularly;

(c) identify and verify:

(i) the Source of Funds; and

(ii) the Source of Wealth;

of the customer and, if applicable, all Beneficial Owners;

(d) conduct enhanced monitoring of the business relationship, by increasing the

frequency and intensity of controls applied, and determining which groups of transactions need further examination;

(e) obtain the approval of Senior Management to commence a business relationship with the customer;

(f) require the first payment to be carried out through an account in the customer's name with a financial institution that is subject to AML/TFS regulation and supervision in a jurisdiction that has standards equivalent to those set out in the FATF Recommendations; and

(g) for a customer who is a Natural Person, verify the current residential address (other than a post office box).

Guidance

1. In Rule 8.4.1, Enhanced CDD measures are mandatory to the extent that they are applicable to the relevant customer or the circumstances of the business relationship and to the extent that the risks would reasonably require it. Therefore, the extent of additional measures to be conducted is a matter for the Relevant Person to determine on a case-by-case basis.

2. In Rule 8.4.1(e), Senior Management approval may be given by an individual member of the Relevant Person's Senior Management or by a committee of senior managers appointed to consider high-risk customers. Such approval may also be outsourced within the Group, but only to a suitably qualified individual or committee.

3. For high-risk customers, a Relevant Person should, in order to mitigate the perceived potential and actual risks, exercise a greater degree of diligence throughout the course of the customer relationship and should endeavour to understand the nature of the customer's business and consider whether it is consistent and reasonable.

4. A Relevant Person should be satisfied that a customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

5. For Enhanced CDD, where there are one or more Beneficial Owners, verification of the customer's Source of Funds and Wealth may require enquiring into the Beneficial Owners' Source of Funds and Wealth because the Source of the Funds would normally be associated with the Beneficial Owners and not the customer.

6. The Regulator considers that verification of Source of Funds includes obtaining independent corroborating evidence such as the proof of dividend payments

connected to a shareholding, bank statements, salary/bonus certificates, loan documentation and proof of all Transactions which gave rise to payments into the account. A customer should be able to demonstrate and have documented how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a Transaction.

7. The Regulator considers that verification of Source of Wealth includes obtaining independent corroborating evidence such as share certificates, publicly available registers of ownership, bank or brokerage account statements, probate documents, audited accounts and financial statements, news items from a reputable source and other similar evidence.

8. A Relevant Person may commission a report from a third-party vendor to obtain further information on a customer or Transaction or to investigate a customer or Beneficial Owners in very high-risk cases. Such a report may be particularly useful where there is little or no publicly available information on a Person or on a Legal Arrangement or where the Relevant Person has difficulty in obtaining and verifying information.

9. For Rule 8.4.1, circumstances where it may be applicable to require the first payment made by a customer in order to open an account with a Relevant Person to be carried out through a bank account in the customer's name include:

   (a) where, following the use of other Enhanced Customer Due Diligence measures, the Relevant Person is not satisfied with the results of that due diligence; or

   (b) as an alternative measure, where one of the measures in Rule 8.4.1(a) to (e) cannot be carried out.

10. A Relevant Person should maintain up-to-date lists of Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action and take these lists into account in developing and applying risk-based measures relating to CDD including the development of compliance procedures.

11. CDD should include screening for customer exposure to Jurisdictions Under Increased Monitoring and Jurisdictions Subject to a Call for Action. Customer exposure to such jurisdictions may present higher money laundering risks and specific risk-based countermeasures may be required. In the case of customer exposure to Jurisdictions Under Increased Monitoring, this may include undertaking Enhanced CDD. In the case of customer exposure to Jurisdictions Subject to a Call for Action, Enhanced CDD should always be undertaken.

12. Pursuant to directives of the NAMLCFTC, Relevant Persons must exercise appropriate levels of due diligence on Transactions originating from, routed

through or destined for Jurisdictions Subject to a Call for Action and any other financial or non-financial engagement involving an individual or entity from such jurisdictions.

13. Relevant Persons should assess if they should notify the FIU if customers or potential customers are from a High Risk Country or are engaged in transactions that may involve a High Risk Country. Currently, these must be notified to the FIU prior to conducting Transactions where the remitter or the beneficiary is an individual or entity associated with a Jurisdiction Subject to a Call for Action. Such Transactions may only be executed in line with guidance issued by the FIU.

8.5 Simplified Customer Due Diligence

8.5.1 (1) Where a Relevant Person is permitted to undertake Simplified CDD under Rule 8.1.1(4), modification of Rule 8.3.1 may include:

(a) verifying the identity of the customer and any Beneficial Owners after the establishment of the business relationship;

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identification document other than by requesting a copy;

(d) reducing the degree of ongoing monitoring of Transactions, based on a reasonable monetary threshold or on the nature of the Transaction; and

(e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of Transactions or business relationship established.

(2) The modification undertaken under 8.5.1(1) must be proportionate to the customer's money laundering risks.

Guidance

1. A Relevant Person should not use a "one size fits all" approach for all of its low-risk customers. Notwithstanding that the risks may be low for all such customers

in that category, the extent of CDD undertaken needs to be proportionate to the specific risks identified on a case-by-case basis.

2. A Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.

3. An example of where a Relevant Person might reasonably reduce the degree of ongoing monitoring and scrutinising of Transactions, based on a reasonable monetary threshold or on the nature of the Transaction, would be where the Transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the Transaction is not material for money laundering purposes given the nature of the customer and the Transaction type.

8.6 Ongoing Customer Due Diligence

8.6.1 When undertaking ongoing CDD under Rule 8.3.1(1)(d), a Relevant Person must:

(a) monitor Transactions undertaken during the course of its customer relationship to ensure that the Transactions are consistent with the Relevant Person's knowledge of the customer, his business and risk rating;

(b) pay particular attention to any complex or unusually large Transactions or unusual patterns of Transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the Transactions in (b);

(d) periodically review the adequacy of the CDD information it holds on customers and Beneficial Owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating; and

(e) periodically review each customer to ensure that the risk rating assigned to a customer under Rule 7.1.1(1)(b) remains appropriate for the customer in light of the money laundering risks.

8.6.2 A Relevant Person must apply an intensified and ongoing monitoring programme with respect to higher risk Transactions and customers.

Guidance

1. The customer identification process does not end at the time of establishing a

business relationship with a customer or, where relevant, undertaking a specific transaction or business activity on behalf of a customer. Following the start of the customer relationship, a Relevant Person should ensure that all relevant evidence and information is kept up to date including, for example, the list of authorised signatories who can act on behalf of a corporate customer.

2. In complying with Rule 8.6.1(d), a Relevant Person should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up to date. A Relevant Person is expected to ensure that the information and the evidence obtained from a customer is valid and has not expired, for example when obtaining copies of identification documentation such as a passport or identification card. Examples of non-static identity documentation include passport number and residential/business address and, for a Legal Person, its share register or list of partners.

3. A Relevant Person should undertake a review under Rule 8.6.1(d) and (e) particularly when:

   (a) the Relevant Person changes its CDD documentation requirements;

   (b) an unusual Transaction with the customer is expected to take place;

   (c) there is a material change in the business relationship with the customer; or

   (d) there is a material change in the nature or ownership of the customer.

4. The degree of the ongoing due diligence to be undertaken will depend on the customer risk assessment carried out under Rule 7.1.1.

5. A Relevant Person's Transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination thereof, are one of the most important aspects of effective CDD. Whether a Relevant Person should undertake the monitoring by means of a manual or computerised system, or both, will depend on a number of factors, including:

   (a) the size and nature of the Relevant Person's business and customer base; and

   (b) the complexity and volume of customer Transactions.

8.6.3 A Relevant Person must review its customers, their businesses and Transactions, against Sanctions Lists when complying with Rule 8.6.1(d).

8.7 Failure to conduct or complete Customer Due Diligence

8.7.1 (1) Where, in relation to a customer, a Relevant Person is unable to conduct or complete the requisite CDD in accordance with Rule 8.1.1 it must, where appropriate:

(a) not carry out a Transaction with or for the customer through a bank account or in cash;

(b) not open an account or otherwise provide a service;

(c) not otherwise establish a business relationship or carry out a Transaction;

(d) terminate or suspend any existing business relationship with the customer;

(e) return any monies or assets received from the customer; and

(f) consider whether the inability to conduct or complete CDD necessitates the making of a Suspicious Activity/Transaction Report under Rule 14.3.1(c).

(2) A Relevant Person is not obliged to comply with (1)(a) to (e) if:

(a) to do so would amount to "tipping off" the customer; or

(b) the FIU directs the Relevant Person to act otherwise.

Guidance

1. In complying with Rule 8.7.1(1) a Relevant Person should apply one or more of the measures in (a) to (f) as appropriate in the circumstances. Where CDD cannot be completed to a significant degree, it may be appropriate not to carry out a Transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD such as identifying and verifying Beneficial Owners cannot be undertaken, a Relevant Person should not establish a business relationship with the customer.

2. A Relevant Person should note that Rule 8.7.1 applies to both existing and prospective customers. For prospective customers, it may be appropriate for a Relevant Person to terminate the business relationship before a product or service is provided. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances whilst further investigations are carried out. Whichever course of action is taken, the Relevant Person should be careful not to tip off the customer.

3. A Relevant Person should adopt the RBA in order to inform the appropriate level of CDD to be undertaken for existing customers. For example, if a Relevant Person considers that any of its existing customers (which may include customers who migrates into GMC) have not been subject to CDD of a standard equivalent to that required by the AML Rulebook, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with Rule 8.7.

8.8 Portability of Customer Due Diligence information

8.8.1 (1) A Relevant Person "A" that is a Licensed Firm or a Licensed Body must provide another Relevant Person, "B", that is a Licensed Firm or a Licensed Body, at the request of B, with the Customer Due Diligence information for customers that has been collected by A under Rules 8.3 and 8.4, subject to:

(a) those customers being customers of both A and B at the time that the request is made;

(b) B obtaining the written consent of the customers to whom the request relates and providing A with that consent for the release of such information by A;

(c) the request being made solely for the purposes of conducting Customer Due Diligence on the customers to whom the request relates; and

(d) in the preceding twelve months B not having requested Customer Due Diligence information from A for the same customers to whom the request relates.

(2) Relevant Person A must also provide Relevant Person B with any other information relevant to CDD that has been provided to it by those customers.

8.8.2 Following a request made under Rule 8.8.1, A must transfer to B without undue delay all Customer Due Diligence information in its possession for those customers.

8.8.3 Relevant Person A must not charge B a fee for the provision of Customer Due Diligence information provided under Rule 8.8.1.

9. AML/TFS COMPLIANCE AND THIRD PARTIES

9.1 Reliance on a third party

9.1.1 (1) A Relevant Person may rely on the following third parties to conduct one or more of the elements of CDD on its behalf:

(a) a Licensed Firm or Licensed Body;

(b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent Person in another jurisdiction;

(c) a Financial Institution;

(d) a member of the Relevant Person's Group; or

(e) other specialised utilities for the provision of outsourced AML/TFS services.

(2) In (1), a Relevant Person may rely on the information previously obtained by a third party which covers one or more elements of CDD.

(3) Where a Relevant Person seeks to rely on a Person in (1) it may only do so if and to the extent that:

(a) it immediately obtains the necessary CDD information from the third party in (1);

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of CDD will be available from the third party on request without delay;

(c) the Person in (1)(b) to (d) is subject to regulation, including AML/TFS compliance requirements, by a Non-GMC Financial Services Regulator or other competent authority in a country with AML/TFS regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;

(d) the Person in (1) has not relied on any exception from the requirement to conduct any relevant elements of CDD which the Relevant Person seeks to rely on; and

(e) in relation to (2), the information is up to date.

(4) Where a Relevant Person relies on a member of its Group to conduct one or more

of the elements of CDD on its behalf, such Group member need not meet the condition in (3)(c) if:

(a) the Group is subject to policies and requirements equivalent to FATF standards, either:

(i) where the Group applies and implements a Group-wide policy on CDD and record-keeping which is equivalent to the standards set by FATF; or

(ii) where the effective implementation of those CDD and record-keeping requirements and AML/TFS programmes are supervised at Group level by a Non-GMC Financial Services Regulator or other competent authority in a jurisdiction with AML/TFS regulations that are equivalent to the standards set out in the FATF Recommendations;

(b) no exception from identification obligations has been applied in the original identification process; and

(c) a written statement is received from the introducing member of the Relevant Person's Group confirming that:

(i) the customer has been identified in accordance with the relevant standards under (4)(a) and (b);

(ii) any identification evidence can be accessed by the Relevant Person without delay; and

(iii) the identification evidence will be kept for at least six years.

(5) If a Relevant Person is not reasonably satisfied that a customer or Beneficial Owners has been identified and verified by a third party in a manner consistent with these Rules, the Relevant Person must immediately perform the CDD itself with respect to any deficiencies identified.

(6) Notwithstanding the Relevant Person's reliance on a Person in 9.1.1(1), the Relevant Person remains responsible for compliance, and liable for any failure to meet the CDD requirements in the AML Rulebook.

9.1.2 (1) When assessing under Rule 9.1.1(3) or 9.1.1(4) if AML/TFS regulations in another jurisdiction are equivalent to FATF standards, a Relevant Person must take into account factors including, but not limited to:

(a) mutual evaluation reports, assessment reports or follow-up reports published by FATF, the IMF, the World Bank, the OECD or other

International Organisations;

(b) membership of FATF or other international or regional groups such as the Asia/Pacific Group on Money Laundering ("**APG**");

(c) contextual factors such as political stability or the level of corruption in the jurisdiction;

(d) evidence of recent criticism of the jurisdiction, including in:

(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML/TFS regimes by organisations referred to in (a); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations;

(e) whether adequate arrangements exist for co-operation between the AML/TFS regulator in that jurisdiction and the Regulator.

(2) A Relevant Person making an assessment under (1) must rely only on sources of information that are reliable and up to date.

(3) A Relevant Person must keep adequate records of how its assessment is made, including the sources and materials considered.

Guidance

1. In complying with Rule 9.1.1(3)(a), "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, and not just basic information such as name and address. However, compliance can be achieved by having necessary information sent to an email or other appropriate means. For the avoidance of doubt, it does not necessarily require a Relevant Person to immediately obtain the underlying certified documents used by the third party to undertake its CDD because under Rule 9.1.1(3)(b), these need only be available on request without delay.

2. The Regulator would expect a Relevant Person, in complying with Rule 9.1.1(5), to fill any gaps in the CDD process as soon as it becomes aware that a customer or Beneficial Owners has not been identified and verified by the third party in a manner consistent with these Rules.

3. If a Relevant Person acquires another business, either in whole or in substantial part, the Regulator would permit the Relevant Person to rely on the CDD conducted by the business it is acquiring, but would expect the Relevant Person to

have done the following:

(a) as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD undertaken; and

(b) to have undertaken CDD on all the customers to cover any deficiencies identified in (a) as soon as possible following the acquisition, prioritising high-risk customers.

4. Where the legislative framework of a jurisdiction (such as secrecy or data protection legislation) prevents a Relevant Person from having access to CDD information upon request without delay as referred to in Rule 9.1.1(3)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

5. If a Relevant Person relies on a third party located in a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the Relevant Person must ensure that the foreign jurisdiction has AML/TFS regulations which are equivalent to the standards set out in the FATF Recommendations (see Rule 9.1.1(3)(c)).

6. Relevant Persons are prohibited from using third parties located in Jurisdictions Subject to a Call for Action to perform CDD.

9.2 Business partner identification

9.2.1 (1) Prior to establishing the business relationship, a Relevant Person must establish and verify the identity of its business partners by obtaining sufficient and satisfactory evidence of the identity of any business partner it relies upon in carrying on its Regulated Activities.

(2) A Relevant Person must maintain accurate and up-to-date information and conduct ongoing due diligence on its business partners, throughout the course of the business relationship.

(3) If at any time a Relevant Person becomes aware that it lacks sufficient information or documentation concerning a business partner's identification, or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify such business partner's identity.

(4) In the context of this Rule, a 'business partner' includes:

(a) a third party as specified in Rule 9.1.1(1);

(b) a member of the Relevant Person's Group;

(c) a Correspondent Bank; or

(d) any other service provider.

(5) A Relevant Person that establishes, operates or maintains a Correspondent Account for a Correspondent Banking Client must ensure that it has arrangements to:

(e) conduct due diligence in respect of the opening of a Correspondent Account for a Correspondent Banking Client, including measures to identify:

(i) its ownership and management structure;

(ii) its major business activities and customer base;

(iii) its location; and

(iv) the intended purpose of the Correspondent Account;

(f) identify all third parties that will use the Correspondent Account; and

(g) monitor Transactions processed through a Correspondent Account that has been opened by a Correspondent Banking Client, in order to detect and report any suspicion of money laundering.

Guidance

Under (4)(d), service providers include agents that directly facilitate the activities of Authorised Persons in servicing their clients, as distinct from other service providers that provide purely ancillary services, such as IT, facilities management etc. to an Authorised Person.

9.2.2 A Relevant Person must not:

(1) establish a correspondent banking relationship with a Shell Bank;

(2) establish or keep anonymous accounts or accounts in false names; or

(3) maintain a nominee account which is held in the name of one Person, but controlled by or held for the benefit of another Person whose identity has not been disclosed to the Relevant Person.

Guidance

1. "Know your business partner" is as important as "Know Your Customer".

A Relevant Person is therefore required to verify the identity of a prospective business partner and to obtain evidence of it. The same documentation that is used to identify customers should be obtained from the business partner prior to conducting any business.

2. A Relevant Person should verify whether any secrecy or data protection law exists in the country of incorporation of the business partner that would prevent access to relevant data.

3. The requirement to identify the business partner is meant to cover only those business partners who may pose any relevant money laundering risks to the Relevant Person. Hence, a Relevant Person would not be required to establish and verify the identity of, for example, its maintenance or cleaning service.

4. The Regulator may take into account the identity of a Relevant Person's business partner and the nature of their relationship in considering the fitness and propriety of a Relevant Person.

5. Before entering into a business relationship, a Relevant Person should conduct a due diligence investigation, which includes ensuring that the business partner is an existing Person authorised to conduct the kind of business in question and, if applicable, verifying that this Person is duly regulated by a Financial Services Regulator or other relevant regulatory authority or regulator. In accordance with "The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking", the Relevant Person should take into account, and verify the nature of:

(a) the business to be conducted and the major business activities of the business partner;

(b) the jurisdiction where the business partner is located as well as that of its parent; and

(c) the transparency and the nature of the ownership and the management structure.

6. A Relevant Person may also gather information about the reputation of the business partner, including whether it has been subject to investigation or regulatory action in relation to money laundering.

7. A Relevant Person should adopt a risk-based approach when verifying its business partners' identities. Depending on the money laundering risks assessment of the Relevant Person's business partner, the Relevant Person should decide the level of detail of the business partner identification and verification process.

8. A Relevant Person should have in place specific arrangements to ensure

that adequate due diligence and identification measures with regard to the business relationship are taken.

9. The Relevant Person should conduct regular reviews of the relationship with its business partners.

10. The Senior Management or Governing Body of a Relevant Person should give its approval before it establishes any new correspondent banking relationships.

11. A Relevant Person should also have arrangements to guard against establishing a business relationship with business partners who permit their accounts to be used by Shell BanksFurther details on the definition of Shell Banks are set out in Guidance 2 to Rule 10.2.2.

9.3 Outsourcing and agents

9.3.1 A Relevant Person which outsources any one or more elements of its CDD to a service provider (including those within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations:

(a) Prior to appointing a service provider to undertake CDD, a Relevant Person must undertake an initial assurance assessment to evaluate the suitability of the service provider and must ensure that the service provider's obligations are clearly documented in a binding agreement.

(b) After engaging a service provider the Relevant Person must undertake periodic assurance assessments to ensure that the services provided meet the obligations recorded in the binding agreement and allow it to meet all the requirements that it is subject to.

Guidance

1. The use by a Relevant Person of a service provider’s eKYC System that enables a Relevant Person to undertake eKYC constitutes outsourcing for the purposes of Rule 9.3.1.

2. When undertaking an assurance assessment of an eKYC System for the purpose of Rule 9.3.1(a), a Relevant Person should seek to establish that the eKYC System is reliable and independent, and allows the Relevant Person to comply with all applicable legislation including applicable Rules and Regulations. In addition, a Relevant Person should consider applying guidance on assurance standards issued by the Regulator, competent -authorities, FATF, and other relevant standard setting bodies.

3. In limited circumstances, a Relevant Person may place reliance on the assurance

assessment of the eKYC System conducted entirely by another entity. Such circumstances comprise the following.

(a) Where an assurance assessment of the eKYC System has been undertaken by a Related entity and specifically addresses the legislation applicable to the Relevant Person. In such circumstances, the Relevant Person remains responsible for the eKYC System's compliance with applicable legislation including applicable Rules and Regulations and it should maintain a copy of the assessment.

(b) Where the eKYC System has been authorised by a competent authority of the GMCor a competent authority in a jurisdiction with AML/TFS laws equivalent to the GMC. In such circumstances, the eKYC system should be authorised for use in CDD. Further, the Relevant Person should undertake its own review to ensure that any use of the relevant eKYC System is appropriate and enables compliance with all legislation applicable to the Relevant Person including applicable Rules and Regulations.

(c) Where a Relevant Person chooses to employ a third party to assist in its own assurance assessment of the eKYC System, it should ensure that a competent and independent firm with relevant expertise and resources be employed. The Relevant Person remains wholly responsible for the eKYC System's compliance with, and any failure to meet, the legislation applicable to the Relevant Person including applicable Rules and Regulations. In complying with Rule 9.3.1, a Relevant Person should ensure that the service provider can be replaced with minimal disruption in the event the outsourcing arrangement is terminated.

4. An Authorised Person is also required to comply with the outsourcing obligations in GEN 3.3.31 and 3.3.32 and PRU 6.8. A Recognised Body is also required to comply with the outsourcing obligations in MIR 2.14.

9.3.2 **Authorised Persons Providing Money Services**

(1) An Authorised Person that is engaged in Providing Money Services must:

(a) maintain a complete, current and accurate register of all agents and members of its Group it uses to conduct its operations and make that register available to the Regulator upon request;

(b) include all agents and members of its Group identified in (a) as part of its AML/TFS compliance programme and monitor the compliance of such agents and members of its Group with the requirements of its AML/TFS programme;

(c) comply with all AML/TFS requirements imposed in all jurisdictions within which it operates and ensure the compliance of its agents and members of its Group operating on its behalf with all AML/TFS requirements in the jurisdictions in which they are operating;

(d) when executing a Payment Transaction, assess and consider all relevant information, including information about the Payer and the Payee, including any beneficiary as may be applicable, and require its agents and members of its Group, as appropriate, to determine whether a Suspicious Activity/Transaction Report should be filed by it or its agents or a member of its Group; and

(e) where appropriate, ensure that the relevant equivalent of a Suspicious Activity/Transaction Report is filed in all other jurisdictions related to a suspicious Payment Transaction and make available to all authorities responsible for AML/TFS compliance all transaction information related to the suspicious transaction.

(2) An Authorised Person making an assessment under (1) must rely upon current sources of information when making such assessment and must keep adequate records concerning such assessments, including all sources and materials considered, for a period of at least six years.

Guidance

Agents directly facilitate the activities of Authorised Persons in servicing their clients, as distinct from other service providers that provide purely ancillary services, such as IT, facilities management etc. to an Authorised Person.

10. CORRESPONDENT BANKING, WIRE TRANSFERS, ANONYMOUS ACCOUNTS AND AUDIT

10.1 Application

10.1.1 This Chapter applies to Licensed Bodies and all Licensed Firms, other than Credit Rating Agencies and Representative Offices.

10.2 Correspondent banking

10.2.1 A Licensed Firm proposing to have a correspondent banking relationship with a respondent bank must:

(a) undertake CDD on the respondent bank;

(b) as part of (a), gather sufficient information about the respondent bank to understand fully the nature of the business, including making appropriate enquiries as to its management, its major business activities and the countries or jurisdictions in which it operates;

(c) determine from publicly available information the reputation of the respondent bank and the quality of supervision that is subject to, including whether it has been the subject of a money laundering investigation or relevant regulatory action;

(d) assess the respondent bank's AML/TFS controls and ascertain if they are adequate and effective in light of the FATF Recommendations;

(e) ensure that prior approval of the Licensed Firm's Senior Management is obtained before entering into a new correspondent banking relationship;

(f) ensure that the respective responsibilities of the parties to the correspondent banking relationship are properly documented;

(g) be satisfied that, in respect of any customers of the respondent bank who have direct access to accounts of the Licensed Firm, the respondent bank:

(i) has undertaken CDD (including ongoing CDD) at least equivalent to that in Rule 8.3.1 in respect of each customer; and

(ii) is able to provide the relevant CDD information in (i) to the Licensed Firm upon request; and

(h) document the basis for its satisfaction that the requirements in (a) to (g) are met.

10.2.2 A Licensed Firm must:

(a) not enter into a correspondent banking relationship with a Shell Bank; and

(b) take appropriate measures to ensure that it does not enter into, or continue a corresponding banking relationship with, a bank which is known to permit its accounts to be used by Shell Banks.

Guidance

1. The rules and guidance set out in Rule 9.2 above also apply to correspondent banking business partners. This Rule provides further details on specific requirements applicable to a correspondent banking business relationship.

2. With regard to Correspondent Banking Clients and, if applicable, other qualified professionals, specific care should be taken to assess their AML/TFS arrangements regarding customer identification, Transaction monitoring, terrorist financing and other relevant elements, and to verify that these business partners comply with the same or equivalent AML/TFS requirements as the Relevant Person. Information on applicable laws and regulations regarding the prevention of money laundering should be obtained.

3. A Relevant Person should ensure that a Correspondent Banking Client does not use the Relevant Person's products and services to engage in business with Shell Banks. A Shell Bank would be a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial Group that is subject to effective consolidated supervision. The Regulator does not consider that the existence of a local agent or low-level staff constitutes physical presence.

4. If applicable, information on distribution networks and delegation of duties should be obtained.

10.3 Wire transfers and the Travel Rule

10.3.1 In this section:

(a) "**account**" includes a digital wallet when the wire transfer is a transfer of Virtual Assets;

(b) "**account holder**" includes a wallet holder when the wire transfer is a transfer of Virtual Assets;

(c) "**account number**" includes a wallet address when the wire transfer is a transfer of Virtual Assets;

(d) "**batch transfer**" means a transfer comprised of a number of individual wire transfers that are bundled for transmission, whether or not the individual wire transfers are intended ultimately for one or more beneficiaries;

(e) "**beneficiary**" means the Natural or Legal Person or the Legal Arrangement that is identified by the originator as the receiver of the requested wire transfer;

(f) "**originator**" means the account holder who instructs the wire transfer from the relevant account, or where there is no account, the Natural or Legal Person that places the order with the ordering Financial Institution to perform the wire transfer; and

(g) "**wire transfer**" includes any value transfer arrangement.

10.3.2 (1) A Licensed Firm and Licensed Body must:

(a) when it sends or receives a wire transfer on behalf of a customer, ensure that the wire transfer and any related messages contain accurate originator and beneficiary information;

(b) ensure that, while the wire transfer is under its control, the information in (a) remains with the wire transfer and any related message throughout the payment chain;

(c) monitor wire transfers for the purpose of detecting those wire transfers that do not contain both originator and beneficiary information and take appropriate measures to identify any money laundering risks; and

(d) not effect wire transfers without the information required under (3) and (4).

(2) The requirement in (1) does not apply to a Licensed Firm or Licensed Body which:

(a) provides Financial Institutions with messages or other support systems for wire transfers; or

(b) undertakes a wire transfer to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

(3) A Licensed Firm and Licensed Body must ensure that information accompanying all wire transfers contains at a minimum:

(a) the name of the originator;

(b) the originator account number where such an account is used to process the Transaction or a unique Transaction reference number if no originator account number exists;

(c) the originator's address, or national identity number, or travel document number, or customer identification number, or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the Transaction or a unique Transaction reference number if no beneficiary account number exists.

(4) A Licensed Firm and Licensed Body must ensure that for batch transfers:

(a) it has verified the originator information required under (3)(a) to (c); and

(b) the batch file contains the beneficiary information required under (3)(d) and (e) for each beneficiary and that the information is fully traceable in the beneficiaries jurisdiction.

Guidance

1. 'FATF Recommendation Number 16' seeks to ensure that national or international electronic payment and message systems, including fund or wire transfer systems such as SWIFT, are not misused as a means to break the money laundering audit trail. Therefore, the information about a customer as the originator of the wire transfer should remain with the payment instruction throughout the payment chain.

2. Relevant Persons should monitor for, and conduct enhanced scrutiny of, suspicious activities, including incoming wire transfers that do not contain complete originator information, including name, address and account number or unique reference number.

3. The Regulator considers that concealing or removing in a wire transfer any of the information required by Rule 10.3.2(3) would be a breach of the requirement to ensure that the wire transfer contains accurate originator and beneficiary information.

4. The Regulator expects compliance by Licensed Firms and Licensed Bodies and with ‘FATF Recommendation Number 15’, FATF’s Interpretative Note (R.15/INR.15) and ‘FATF Recommendation Number 16’ that include requirements to obtain, hold, and transmit originator and beneficiary information

and to not allow transfers where such information is lacking including where the value transfer involves Virtual Assets. Licensed Firms and Licensed Bodies should note that, pursuant to section 10.3, the Regulator does not differentiate between the responsibilities of the originator or the beneficiary when it comes to ensuring that all relevant information accompanies a wire transfer, and that no de minimis threshold is applied to the size of a relevant wire transfer.

10.4 Audit

10.4.1 A Licensed Firm or Licensed Body must ensure that its internal audit function undertakes regular reviews and assessments of the effectiveness of the Licensed Firm or Licensed Body's money laundering policies, procedures, systems and controls, and its compliance with its obligations in the AML Rulebook.

Guidance

1. The review and assessment undertaken for the purposes of Rule 10.4.1 may be undertaken:

   (a) internally by the Licensed Firm or Licensed Body's internal audit function; or

   (b) by a competent firm of independent, external auditors or compliance professionals.

2. The review and assessment undertaken for the purposes of Rule 10.4.1 should cover at least the following:

   (a) sample testing of compliance with the Licensed Firm or Licensed Body's CDD arrangements;

   (b) an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and

   (c) a review of the nature and frequency of the dialogue between Senior Management and the MLRO.

10.5 Anonymous and nominee accounts

10.5.1 A Licensed Firm or Licensed Body must not establish or maintain:

(a) an anonymous account or an account in a fictitious name; or

(b) a nominee account which is held in the name of one Person, but which is controlled by or held for the benefit of another Person whose identity has not been disclosed to the Licensed Firm or Licensed Body.

11. TARGETED FINANCIAL SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

11.1 Resolutions and Sanctions

11.1.1 (1) A Relevant Person must establish and maintain effective systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or Sanctions which it is required to comply with, under legislation applicable in GMC or any other jurisdiction.

(2) A Relevant Person must immediately notify the Regulator when it becomes aware that it is, for or on behalf of a Person:

(a) carrying on or about to carry on an activity;

(b) holding or about to hold money or other assets; or

(c) undertaking or about to undertake any other business whether or not arising from or in connection with (a) or (b);

where such carrying on, holding or undertaking constitutes or may constitute a contravention of any Sanctions with which the Relevant Person is required to comply, under legislation applicable in GMC or any other jurisdiction.

(3) A Relevant Person must ensure that the notification stipulated in (2) above includes the following information:

(a) a description of the relevant activity in (2)(a), (b) or (c); and

(b) the action proposed to be taken or that has been taken by the Relevant Person with regard to the matters specified in the notification.

Guidance

1. In Rule 11.1.1(1), taking reasonable measures to comply with resolutions or Sanctions may include, for example, a Relevant Person not undertaking a transaction for or on behalf of a Person without undertaking further due diligence in respect of that Person.

2. Relevant resolutions or Sanctions mentioned in Rule 11.1.1 may, among other things, relate to money laundering, terrorist financing or the financing of WMD, or otherwise be relevant to the activities carried on by the Relevant Person. For example:

(a) a Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a Person engaged in money laundering, terrorist financing or the financing of WMD; and

(b) a Licensed Exchange or Licensed Clearing House, as a Recognised Body, should additionally exercise due care to ensure that it does not facilitate fund raising activities or listings by Persons engaged in money laundering or terrorist financing or financing of WMD.

3. A Relevant Person should be proactive in checking for, and taking measures to comply with, relevant resolutions or Sanctions which the Relevant Person is required to comply with, under legislation applicable in GMC or any other jurisdiction. The Regulator expects Relevant Persons to perform checks on an ongoing basis against their customer databases and records for any names appearing in resolutions or Sanctions which the Relevant Person is required to comply with as well as to monitor transactions accordingly.

4. A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and Sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with this Rulebook.

5. [*Not in use*]

6. [*Not in use*]

11.2 Government, regulatory and international findings

11.2.1 (1) A Relevant Person must establish and maintain systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions issued by:

(a) the government of GMC;

(b) the FIU;

(c) the UNSC;

(d) FATF;

(e) the Basel Committee on Banking Supervision;

(f) the Regulator; and

(g) any other jurisdiction which promulgates Sanctions to which it is subject,

concerning the matters in (2).

(2) For the purposes of (1), the relevant matters are:

(a) arrangements for preventing money laundering, terrorist financing or the financing of weapons of mass destruction in a particular country or jurisdiction, including any assessment of material deficiency in adopting international standards against a relevant country or jurisdiction; and

(b) the names of Persons, groups, organisations or entities or any other body where suspicion of money laundering exists.

(3) For the purposes of (1), measures that a Relevant Person must undertake when taking reasonable measures to comply with findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions, include, but are not limited to, countermeasures:

(a) requiring specific elements of enhanced CDD;

(b) requiring enhanced reporting mechanisms or systematic reporting of financial transactions;

(c) limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;

(d) prohibiting Relevant Persons from relying on third parties located in a specified jurisdiction to conduct CDD;

(e) requiring the review and amendment, or if necessary termination, of correspondent relationships with banks in a specified jurisdiction;

(f) prohibiting the execution of specified electronic fund transfers; or

(g) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in a specified jurisdiction.

(4) [*Not in use*]

(5) A Relevant Person must immediately notify the Regulator in writing if it becomes aware of non-compliance by a Person with a finding, recommendation, guidance, directive, resolution, Sanction, notice or other conclusion and provide the

Regulator with sufficient details of the Person concerned and the nature of the non-compliance.

Guidance

1. The purpose of this Rule is to ensure that a Relevant Person takes into consideration the broad range of tools used by competent authorities and international organisations to communicate AML/TFS risks to stakeholders.

2. The Regulator may require enhanced CDD or other specific countermeasures to address risks identified in a specific country or jurisdiction. The Regulator may impose such countermeasures either when called upon to do so by FATF or independently of any FATF request.

3. Relevant Persons considering Transactions or business relationships with Persons located in countries or jurisdictions that have been identified as deficient should be aware of the background against which the assessments or the specific recommendations have been made. These circumstances should be taken into account in respect of business introduced from such jurisdictions, and when receiving inward payments for existing customers or in respect of inter-bank transactions.

4. The Relevant Person's MLRO is not obliged to report all Transactions from these countries or jurisdictions to the FIU if they do not qualify as suspicious.

5. Transactions with counterparties located in countries or jurisdictions which are no longer identified as deficient or have been relieved from special scrutiny (for example, taken off sources mentioned in this Guidance) may nevertheless require attention which is higher than normal.

6. In order to assist Relevant Persons, the Regulator may publish findings, guidance, directives or Sanctions from the FATF or other relevant bodies. However, the Regulator expects a Relevant Person to take its own steps in acquiring relevant information from various available sources. For example, a Relevant Person may obtain relevant information from consolidated lists of financial Sanctions published by the European Union, HM Treasury, and OFAC.

7. In addition, the systems and controls mentioned in Rule 11.2.1 should be established and maintained by a Relevant Person taking into account its risk assessment under Chapters 6 and 7. In relation to the term "make appropriate use" in Rule 11.2.1, this may mean that a Relevant Person cannot undertake a Transaction for or on behalf of a Person or that it may need to undertake further due diligence in respect of such a Person.

8. A Relevant Person should be proactive in obtaining and appropriately using

available national and international information, for example, suspect lists or databases from credible public or private sources with regard to money laundering, including obtaining relevant information from sources mentioned in Guidance 6 above. The Regulator encourages Relevant Persons to perform checks against their customer databases and records for any names appearing on such lists and databases as well as to monitor Transactions accordingly.

9. The risk of terrorists entering the financial system can be reduced if Relevant Persons apply effective AML/TFS strategies, particularly with respect to CDD. Relevant Persons should assess which countries carry the highest risks and should conduct an analysis of Transactions from countries or jurisdictions known to be a source of terrorist financing.

10. The Regulator may require Relevant Persons to take any special measures it may prescribe with respect to certain types of Transactions or accounts where the Regulator reasonably believes that any of the above may pose a money laundering risks to GMC.

11. Relevant Persons are required to have arrangements in place to ensure the ability to comply with all applicable Sanctions in relation to physical delivery of commodities including Spot Commodities.

12. [*Not in use*]

12. MONEY LAUNDERING REPORTING OFFICER

12.1 Appointment of an MLRO

12.1.1 (1) A Relevant Person must appoint an individual as the MLRO who has an appropriate level of seniority, experience and independence to act in the role, with responsibility for implementation and oversight of its compliance with the Rules in the AML Rulebook. It must do so by completing and filing with the Regulator the appropriate form specified by the Regulator.

(2) The MLRO in (1) and Rule 12.1.7 must possess a GMC work visa.

12.1.2 The individual appointed as the MLRO of a DNFBP that comprises of one officer, partner or principal can, with the prior approval of the Regulator, be the same person as the officer, partner or principal of the DNFBP.

12.1.3 The individual appointed as the MLRO of a Representative Office must be the same individual who holds the position of Principal Representative of that Representative Office.

Guidance

1. Licensed Firms are reminded that under GEN Rule 5.5.1, the MLRO function is a mandatory appointment. For the avoidance of doubt, the individual appointed as the MLRO of a Licensed Firm, other than a Representative Office, is the same individual who holds the Controlled Function of MLRO of that Licensed Firm. Licensed Firms are also reminded that the guidance under GEN Rule 5.5.2 sets out the grounds under which the Regulator will determine whether to grant a waiver from the residence requirements for an MLRO. The same guidance is relevant to other Relevant Persons seeking a waiver from the MLRO residence requirements.

2. The individual appointed as the MLRO of a Licensed Exchange or Licensed Clearing House is the same individual who holds the position of MLRO of that Licensed Exchange or Licensed Clearing House under the relevant MIR Rule.

12.1.4 If the MLRO leaves the employment of the Relevant Person, the Relevant Person must immediately appoint a new MLRO or arrange temporary cover for the MLRO appointment.

12.1.5 A Relevant Person, other than a Representative Office, must appoint an individual to act as a deputy MLRO of the Relevant Person to fulfil the role of the MLRO in his absence.

12.1.6 A Relevant Person's MLRO and deputy MLRO must deal with the Regulator in an open and co-operative manner and must disclose appropriately any information of which the

Regulator would reasonably be expected to be notified.

Guidance

1. The individual appointed as the deputy MLRO need not apply for the Regulator's approval.

2. A Relevant Person should make adequate arrangements to ensure that it remains in compliance with the AML Rulebook in the event that its MLRO is absent. Adequate arrangements would include appointing a temporary MLRO for the period of the MLRO's absence or making sure that the Relevant Person's AML/TFS systems and controls allow it to continue to comply with these Rules when the MLRO is absent.

12.1.7 A Relevant Person may outsource the role of MLRO to an individual outside the Relevant Person provided that the individual under the outsourcing agreement is and remains suitable to perform the MLRO role.

Guidance

Where a Relevant Person outsources specific AML/TFS tasks of its MLRO to another individual or a third-party provider, including the case where they are within its corporate Group, the Relevant Person remains responsible for ensuring that the duties undertaken by the MLRO ensure its compliance with the requirements in the AML Rulebook. The Relevant Person should satisfy itself of the suitability of anyone who acts as MLRO.

12.2 Qualities of an MLRO

12.2.1 A Relevant Person must ensure that its MLRO has:

(a) direct access to the Governing Body and its Senior Management;

(b) sufficient and up-to-date qualifications and experience to fulfil the role;

(c) sufficient resources including, if necessary, an appropriate number of appropriately trained Employees to assist in the performance of his duties in an effective, objective and independent manner;

(d) a level of seniority and independence within the Relevant Person to enable him to act on his own authority;

(e) timely and unrestricted access to information the Relevant Person has about the financial and business circumstances of a customer or any Person on whose behalf the customer is or has been acting sufficient to enable him to carry out his

responsibilities in accordance with Rule 12.3.1; and

(f) unrestricted access to relevant information about the features of the Transaction which the Relevant Person has entered into or may have contemplated entering into with or for the customer or a Person on whose behalf a customer is or has been acting.

Guidance

The Regulator considers that a Relevant Person will need to consider this Rule especially when appointing an outsourced MLRO. Any external MLRO that is appointed will need to have the actual or effective level of seniority that the role requires.

12.3 Responsibilities of an MLRO

12.3.1 A Relevant Person must ensure that its MLRO implements and has oversight of and is responsible for the following matters:

(a) the day-to-day operations for compliance by the Relevant Person with its AML/TFS policies, procedures, systems and controls;

(b) acting as the point of contact to receive internal notifications of suspicious activity from the Relevant Person's Employees under Rule 14.2.2;

(c) taking appropriate action under Rule 14.3.1 following receipt of a notification from an Employee;

(d) making Suspicious Activity/Transaction Reports;

(e) acting as the point of contact within the Relevant Person for competent authorities and the Regulator regarding money laundering issues;

(f) responding promptly to any request for information made by competent authorities or the Regulator;

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11; and

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under Chapter 13.

Guidance

Depending on the size, nature and complexity of its business and operations, Relevant Persons and MLROs should consider whether it is appropriate to screen prospective employees for money laundering risks prior to employment to ensure high standards when hiring.

12.4 Reporting

12.4.1 The MLRO must report semi-annually to the Governing Body or Senior Management of the Relevant Person on the following matters:

(a) the results of the review under Rule 4.1.1(4);

(b) the Relevant Person's compliance with the Regulations and Rules of the Regulator (including this AML Rulebook);

(c) relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions and how the Relevant Person has taken them into account;

(d) internal notification(s) of suspicious activity to the MLRO made under Rule 14.2.2 by the Relevant Person's Employees, or its agents or members of its Group where acting on its behalf, and action taken in respect of those reports, including the grounds for all decisions;

(e) Suspicious Activity/Transaction Reports made by the Relevant Person, or its agents or members of its Group where acting on its behalf, and action taken in respect of those reports including the grounds for all decisions; and

(f) other relevant matters related to AML/TFS as it concerns the Relevant Person's business.

12.4.2 A Relevant Person must ensure that its Governing Body or Senior Management promptly:

(a) assess the report provided under Rule 12.4.1;

(b) take action, as required, subsequent to consideration of the findings of the report, in order to resolve any identified deficiencies; and

(c) make a record of their assessment pursuant to(a) and the action taken pursuant to (b).

12.4.3 The Relevant Person must provide to the Regulator a copy of:

(a) the report provided under Rule 12.4.1; and

(b) the record made under Rule 12.4.2(c).

13. AML/TFS TRAINING AND AWARENESS

13.1 Training and awareness

13.1.1 A Relevant Person must:

(a) provide AML/TFS training to all relevant Employees at appropriate and regular intervals;

(b) ensure that its AML/TFS training enables its Employees to:

(i) know the identity, and understand the responsibilities, of the Relevant Person's MLRO and deputy MLRO;

(ii) understand the relevant legislation relating to money laundering;

(iii) understand its policies, procedures, systems and controls related to money laundering and any changes to these;

(iv) recognise and deal with Transactions, risks, trends, techniques and other activities which may be related to money laundering;

(v) understand the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged and that may warrant an internal notification of suspicious activity to the MLRO under Rule 14.2.2;

(vi) understand its arrangements regarding the making of an internal notification to the MLRO of suspicious activity under Rule 14.2.2;

(vii) be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

(viii) understand the roles and responsibilities of Employees in combatting money laundering; and

(ix) understand the relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11;

(c) ensure that its AML/TFS training:

(i) is appropriately tailored to the Relevant Person's activities, including its products, services, customers, distribution channels, business partners and

the level and complexity of its Transactions; and

(ii) indicates the different levels of money laundering risks and vulnerabilities associated with the matters in (i); and

(d) ensure that its AML/TFS training is up to date with money laundering trends and techniques.

13.2 Frequency

13.2.1 A Relevant Person must provide AML/TFS training to all Employees at least annually, in accordance with Rule 13.1.1.

13.3 Record-keeping

13.3.1 All relevant details of the Relevant Person's AML/TFS training must be recorded, including:

(a) dates when the training was given;

(b) the nature of the training; and

(c) the names of the Employees who received the training.

13.3.2 These records must be kept for at least six years from the date on which the training was given.

Guidance

1. The Regulator considers it appropriate that all new relevant Employees of a Relevant Person be given appropriate AML/TFS training as soon as reasonably practicable after commencing employment with the Relevant Person, and thereafter on a periodic basis.

2. A relevant Employee would include a member of the Senior Management or operational staff, any Employee with customer contact or who handles or may handle customer monies or assets, and any other Employee who might otherwise encounter money laundering in the business.

3. Relevant Persons should take an RBA to AML/TFS training. The Regulator considers that AML/TFS training should be provided by a Relevant Person to each of its relevant Employees at intervals appropriate to the role and responsibilities of the Employee. In the case of a Licensed Firm, the Regulator

expects that training should be provided to each relevant Employee at least annually.

4. The manner in which AML/TFS training is provided by a Relevant Person need not be in a formal classroom setting and may instead be providedvia an online course or any other similarly appropriate manner.

14. SUSPICIOUS ACTIVITY/TRANSACTION REPORTS

14.1 [*Not in use*]

14.2 Internal reporting requirements

14.2.1 A Relevant Person must establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or Transactions in relation to potential money laundering or terrorist financing.

14.2.2 A Relevant Person must have policies, procedures, systems and controls to ensure that whenever any Employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting,

that a Person is engaged in or attempting money laundering or terrorist financing and that Employee promptly notifies the Relevant Person's MLRO and provides the MLRO with all relevant details.

14.2.3 A Relevant Person must have policies and procedures to ensure that disciplinary action can be taken against any Employee who fails to make such a report.

Guidance

1. Circumstances that might give rise to suspicion or reasonable grounds for suspicion of money laundering or terrorist financing include:

(a) Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;

(b) Transactions requested by a Person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a Relevant Person in relation to a particular customer;

(c) where the size or pattern of Transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or may have been deliberately structured to avoid detection;

(d) a customer's refusal to provide the information requested without reasonable explanation;

(e) where a customer who has just entered into a business relationship uses the relationship for a single Transaction or for only a very short period of time;

(f) extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

(g) unnecessary routing of funds through third-party accounts; or

(h) unusual Transactions without an apparently profitable motive.

2. CDD measures form the basis for recognising suspicious activity or Transactions. Sufficient guidance must therefore be given to the Relevant Person's Employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering or terrorist financing is taking place. This should involve training that will enable relevant Employees to seek and assess the information that is required for them to judge whether a Person is involved in suspicious activity or Transactions related to money laundering or terrorist financing.

3. Where appropriate, a Relevant Person should also utilise the methods described in paragraph 1 above to detect a range of Financial Crimes, including fraud. Bearing in mind the evolving nature of Financial Crime and the methods used to further it, a Relevant Person should apply best practice when determining which behaviours would be considered suspicious and what measures are required to detect suspicious activity and Transactions. Such practices may include, but are not limited to, incorporating the analysis of customer behaviour metrics into the monitoring of suspicious activity and Transactions.

4. The requirement for Employees to notify the Relevant Person's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

5. A Relevant Person may allow its Employees to consult with their line managers before sending a report to the MLRO. The Regulator would expect that such consultation does not prevent making a report whenever an Employee has stated that he has knowledge, suspicion or reasonable grounds for knowing or suspecting that a Person may be involved in money laundering. Whether or not an Employee consults with his line manager or other Employees, the responsibility remains with the Employee to decide for himself whether a notification to the MLRO should be made.

6. An Employee, including the MLRO, who considers that a Person has engaged in or is engaging in activity or Transactions that he knows or suspects to be

suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime of money laundering or terrorist financing.

7. Activity or Transactions that appear unusual are not necessarily suspicious. Even customers with a stable and predictable Transaction profile will have periodic Transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of Transactions or account activity. So the unusual is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A Transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report it then arises.

8. Effective CDD measures may provide the basis for recognising unusual and suspicious activity and Transactions. Refusal to provide documentation to support CDD or refusal to disclose a beneficial owner may be considered suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising "suspicious activity" is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

9. A Relevant Person may consider implementing policies and procedures whereby disciplinary action is taken against an Employee who fails to notify the Relevant Person's MLRO.

10. Relevant Persons should comply with guidance issued by the competent authority with regard to identifying and reporting suspicious activity and Transactions relating to money laundering, terrorist financing and proliferation financing.

14.3 Suspicious Activity/Transaction Reports

14.3.1 A Relevant Person must ensure that where the Relevant Person's MLRO receives an internal notification of suspicious activity under Rule 14.2.2, the MLRO, without delay:

(a) investigates and documents the circumstances in relation to which the notification made under Rule 14.2.2 was made;

(b) determines whether in a SAR/STR must be made and document such determination; and

(c) if required, make a SAR/STR as soon as practicable.

14.3.2 The MLRO must, following receipt of an internal notification of suspicious activity under Rule 14.2.2, document:

(a) the steps taken to investigate the circumstances in relation to which the internal notification is made; and

(b) where no external SAR/STR is made, the reasons why no such report was made.

14.3.3 Where, following a notification to the MLRO of suspicious activity under 14.2.2, no SAR/STR is made, a Relevant Person must record the reasons for not making a SAR/STR.

14.3.4 A Relevant Person must ensure that if the MLRO decides to make a SAR/STR, his decision is made independently and is not subject to the consent or approval of any other Person.

14.3.5 Relevant Persons are required to register on goAML upon receipt of their Financial Services Permission, Recognition Order or registration licence in order to submit SAR/STRs.

Guidance

1. Relevant Persons are reminded that the failure to report suspicions of money laundering or terrorist financing may constitute a criminal offence that is punishable.

2. Relevant Persons should comply with guidance issued by the FIU regarding reporting suspicious activity and Transactions relating to money laundering, terrorist financing and proliferation financing.

3. SARs/STRs should be submitted to the FIU. Firms should check with the Regulator or the FIU on how to submit SARs/STRs.

4. In the preparation of a SAR/STR, if a Relevant Person knows or assumes that the funds which form the subject of the report do not belong to a customer but to a third party, this fact and the details of the Relevant Person's proposed course of further action in relation to the case should be included in the report.

5. If a Relevant Person has filed a SAR/STR, the FIU may instruct the Relevant Person on how to continue its business relationship, including effecting any Transaction with a Person. If the customer in question expresses his wish to move the funds before the Relevant Person receives instruction from the FIU on how to proceed, the Relevant Person should immediately contact the FIU for further instructions.

14.4 Suspension of Transactions and "no tipping-off" requirement

14.4.1 A Relevant Person must not carry out Transactions that it knows or suspects or has reasonable grounds for knowing or suspecting to be related to money laundering or terrorist financing until it has informed the FIU pursuant to Rule 14.3.1.

Guidance

1. Relevant Persons must not tip off any Person, that is, inform any Person that he is being scrutinised, or investigated by any other competent authority for possible involvement in suspicious Transactions or activity related to money laundering or terrorist financing.

2. If a Relevant Person reasonably believes that performing CDD measures will tip off a customer or potential customer, it may choose not to pursue that process and should file a Suspicious Activity/Transaction Report. Relevant Persons should ensure that their Employees are aware of and sensitive to these issues when considering the CDD measures.

14.5 Record-keeping

14.5.1 All relevant details of any notification to the MLRO under Rule 14.2 or Suspicious Activity/Transaction Reports filed pursuant to Rule 14.3 must be maintained for at least six years from the date on which the report was made.

14.6 Freezing of assets

Guidance

The Regulator has certain powers under FSA to impose a requirement restricting a Licensed Firm or Licensed Body from disposing of or transferring property including, for example, assets or other funds suspected of money laundering. It may also impose an order restraining a Person from transferring or disposing of any assets suspected of money laundering or terrorist financing. In cases involving suspected money laundering or terrorist financing, the Regulator will usually take such action in coordination with the FIU.

15. DNFBP REGISTRATION AND SUPERVISION

Guidance

1. The FSA gives the Regulator the power to supervise DNFBPs' compliance with applicable AML requirements. The FSA also gives the Regulator a number of other powers in relation to DNFBPs, including powers of enforcement. This includes the power to obtain information and to conduct investigations into possible breaches of FSA. The Regulator may also impose fines for breaches of FSA or the Rules. It may also suspend or withdraw the registration of a DNFBP in various circumstances.

2. The Regulator (GFSO) may appoint another GMC department or government body to supervise DNFBPs' compliance with relevant AML requirements.

3. The Regulator takes a risk-based approach to regulation of persons which it supervises. Generally, the Regulator will work with DNFBPs to identify, assess, mitigate and control relevant risks where appropriate.

4. Rule 15.1.1 requires a DNFBP to be registered by the Regulator to conduct its activities in GMC. Rule 15.2.1 sets out the criteria a DNFBP must meet to be registered. The Regulator may suspend or withdraw the registration of a DNFBP where the DNFBP no longer meets the criteria for registration.

5. A DNFBP is defined in Rule 3.2.1 and includes the following class of persons whose business is carried out in GMC:

   (a) a real estate agency which carries out transactions with other Persons that involve the acquiring or disposing of real property;

   (b) a dealer in precious metals or precious stones;

   (c) a dealer in any saleable item of a price equal to or greater than USD15,000;

   (d) an accounting firm, audit firm, insolvency firm or taxation consulting firm;

   (e) a law firm, notary firm or other independent legal business; or

   (f) a Company Service Provider.

6. In determining if a Person is a DNFPB, the Regulator will adopt a 'substance over form' approach,that is, it will consider what business or profession is in fact being carried on, its main characteristics, and not just what business or profession the Person purports, or is licensed, to carry on in GMC.

7. The Regulator considers that a "law firm, notary firm or other independent legal business, includes any business or profession that involves a legal service, including advice or services related to laws in GMC The Regulator does not consider it necessary for the purposes of the definition that the:

   (a) Person is licensed to provide legal services in GMC; or

   (b) the individuals or employees providing the legal service are qualified or authorised to do so.

8. The Regulator considers that "accounting firm, audit firm, insolvency firm or taxation consulting firm", includes forensic accounting services that use accounting skills, principles and techniques to investigate suspected illegal activity or to analyse financial information for use in legal proceedings.

15.1 DNFBP prohibition

15.1.1 A Person who is a DNFBP must not carry on any activities in or from GMC unless that Person is registered under AML 15.4 by the Regulator as a DNFBP.

15.1.2 The Regulator may delegate its powers for the registration, suspension and cancellation of a DNFBP's registration to the GMC Registrar of Companies.

15.2 Criteria for registration as a DNFBP

15.2.1 (1) To be registered as a DNFBP, an applicant must demonstrate to the Regulator's satisfaction that:

   (a) it is fit and proper to perform AML/TFS functions; and

   (b) it has adequate resources, systems and controls, including policies and procedures, to comply with all applicable AML/TFS requirements under FSA and these Rules;

(2) In assessing if an applicant is fit and proper under (1)(a), the Regulator may, without limiting the matters it may take into account under that paragraph, consider the applicant, its senior management, its Beneficial Owners, other entities in its Group and any other Person with whom it has a relationship.

(3) The Regulator will in assessing if an applicant is fit and proper, consider the cumulative effect of matters that, if considered individually, may be regarded as insufficient to give reasonable cause to doubt the fitness and propriety of the

applicant.

15.3 Application for registration as a DNFBP

15.3.1 A Person may apply to the Regulator to be registered as a DNFBP by completing and submitting the appropriate form.

15.3.2 The Regulator may require an applicant to provide additional information or documents reasonably required by the Regulator for it to be able to consider an application for registration including, but not limited to, information or documents relating to the activities, ownership, group structure, financial and other resources of the applicant.

15.3.3 Where, at any time between filing an application and the grant or refusal of registration as a DNFBP, an applicant becomes aware of a material change in its circumstances that is reasonably likely to be relevant to its application, it shall inform the Regulator in writing of the change without delay.

15.3.4 Any Person who is a DNFBP upon the making of this Chapter and was previously a Relevant Person prior to the making of this Chapter:

(a) is deemed to be registered as a DNFBP at the time of the making of this Chapter; and

(b) must apply for registration under Rule 15.3:

(i) within 12 months of the making of this Chapter; or

(ii) at the date of the renewal of its Commercial Licence under the GMC Registrar of Companies; whichever comes first.

15.4 Grant of an application

15.4.1 The Regulator may grant an application for DNFBP registration as a DNFBP if it is satisfied that the applicant meets the criteria for registration under Rule 15.2.

15.4.2 Where the Regulator decides to register a DNFBP, it shall as soon as is practicable inform the applicant in writing of that decision and of the date on which registration is to take effect.

15.5 Refusal of an application

15.5.1 The Regulator may refuse to grant an application for DNFBP registration where it is not satisfied that the applicant meets the criteria for registration under Rule 15.2.

15.6 DNFBP notifications

15.6.1 A DNFBP must promptly notify the Regulator of any change in its:

(a) name;

(b) legal status;

(c) address;

(d) MLRO;

(e) senior management; or

(f) Beneficial ownership.

15.6.2 (1) A DNFBP must notify the Regulator in writing at least ten Business Days in advance of it ceasing to carry on the business activities.

(2) The notice must include a request to cancel its registration, an explanation of the reason for the DNFBP ceasing business, the planned date of the cessation of its activities, and copies of any relevant documents must be submitted with the notice.

15.7 Suspension and withdrawal of DNFBP registration

15.7.1 (1) The Regulator may suspend the registration of a DNFBP at the request of the DNFBP or on its own initiative.

(2) The Regulator may withdraw the registration of a DNFBP:

(a) at the request of the DNFBP;

(b) if the Registrar of Companies notifies it that the DNFBP no longer holds the relevant commercial licence to operate in GMC; or

(c) on its own initiative.

15.7.2 (1) The Regulator may exercise its power on its own initiative under Rule 15.7.1 (1) or (2)(c) where:

(a) the DNFBP no longer meets the criteria for DNFBP registration;

(b) the DNFBP is in breach of, or has been in breach of, GMC legislation including any Rules or any other legislation applicable in GMC;

(c) the DNFBP is insolvent or entering into administration;

(d) the DNFBP is no longer carrying on business in GMC; or

(e) the Regulator considers that exercising the power is necessary or desirable in the pursuit of its objectives in section 1(3) of FSA.

Guidance

1. A DNFBP may request the withdrawal of its registration because, for example, it no longer meets the definition of a DNFBP, becomes insolvent or enters into administration, or proposes to leave GMC.
2. In addition to being able to withdraw registration at the request of a DNFBP, the Regulator may, on its own initiative, suspend or withdraw the registration of a DNFBP in various circumstances.

15.8 Disclosure of regulatory status

15.8.1 A DNFBP must not:

(a) misrepresent its regulatory status with respect to the Regulator expressly or by implication; or

(b) use or reproduce the logo of the Regulator without express written permission from the Regulator and in accordance with any conditions for use imposed by the Regulator.

15.9 Co-ordination between the Regulator and the Registrar of Companies

(a) The GMC Registrar of Companies shall not grant a Person who is a DNFBP a commercial licence to operate in GMC until the Regulator has confirmed to the Registrar of Companies that it intends to register the Person as a DNFBP.

(b) The Regulator shall as soon as is practicable notify the Registrar of Companies where it suspends or withdraws the registration of a DNFBP.

(c) The GMC Registrar of Companies shall as soon as is practicable suspend or withdraw (as

the case may be) the commercial licence of the DNFBP where it receives a notification under (2).

16. NON-PROFIT ORGANISATIONS

16.1 Responsibility for NPO compliance

16.1.1 An NPO's Governing Body is responsible for establishing, maintaining and monitoring the NPO's obligations under this chapter.

16.1.2 An NPO must maintain information on the following:

(a) the purpose and objectives of its stated activities;

(b) the identity of the persons who own, control or direct its activities, including the Governing Body and senior management;

(c) the relevant controls that have been put in place to ensure that all funds are fully accounted for, and are spent in a manner that is consistent with the purpose and objectives of its stated activities; and

(d) the relevant measures that it has taken to confirm the identity, credentials and good standing of beneficiaries and associated NPOs to ensure that they are not involved with terrorists or terrorist organisations and that its charitable funds are not used to support terrorists or terrorist organisations.

16.2 Record Keeping

16.2.1 An NPO must maintain records of its obligations required under Rule 16.1.2, covering both domestic and international transactions, which are sufficiently detailed to verify that funds have been received and spent in a manner consistent with the purpose and objectives of the NPO for a period of at least six years.

16.3 Co-operation

16.3.1 An NPO must deal with the Regulator in an open and co-operative manner and keep the Regulator informed of significant events, or any other matter relating to the NPO, of which the Regulator would reasonably expect to be notified.

16.3.2 An NPO must, at the request of the Regulator:

(a) give or procure the giving of specified information, documents, files, tapes, computer data or other material in the NPO's possession or control to the

Regulator;

(b) make its Employees readily available for meetings with the Regulator;

(c) give the Regulator access to any information, documents, records, files, tapes, computer data or systems, which are within the NPO's possession or control and provide any facilities to the Regulator;

(d) permit the Regulator to copy documents or other material on the premises of the NPO at the NPO's expense;

(e) provide any copies of those documents or other material as requested by the Regulator; and

(f) answer truthfully, fully and promptly, all questions which are put to it by the Regulator.

Guidance

1. An NPO should have systems and controls in place to identify donors, including their place of residence and, where the donor is not a Natural Person, the activities it undertakes.

2. An NPO should take into consideration money laundering risks posed by a donor, including as a result of the jurisdiction in which the donor is resident or the activities the donor undertakes.

3. Where a donor is resident in a high-risk jurisdiction, an NPO should conduct a risk-based assessment to identify money laundering risks posed by that donor.

4. An NPO should encourage donors to make donations through financial channels offered by Financial Institutions regulated by the Regulator or another Financial Services Regulator.

17. FINANCIAL INTELLIGENCE UNIT

Guidance

1. There shall be an independent and autonomous unit to be known as the Financial Intelligence Unit ("**FIU**") established within GFSO as the central authority for receiving, analyzing, and disseminating financial intelligence related to money laundering and sanctions violations within GMC.

17. 1 Functions of the FIU

17.1.1 The Financial Intelligence Unit shall:

(a) receive suspicious transaction reports (STRs), suspicious activity reports (SARs), and other relevant information as prescribed by this Rulebook;
(b) analyze such reports and information for both operational and strategic purposes;
(c) if required, disseminate the results of its analysis to other relevant competent authorities for investigation where there is a suspicion that money laundering or other offences have taken place or is about to take place;
(d) have timely access, directly or indirectly, to financial, administrative, and law enforcement information necessary to perform its functions;
(e) enter into arrangements with foreign or domestic counterparts to facilitate the exchange of financial information in line with the Egmont Group Principles for Information Exchange Between Financial Intelligence Units;
(f) provide feedback to relevant persons on the quality and usefulness of STRs/SARs, including periodic outreach sessions; and
(g) issue advisories, red flags, and typology updates to strengthen AML/TFS compliance

17.2 Powers of the FIU

17.2.1 For the purpose of carrying out its functions, the FIU shall have the following powers:

(a) To enter into agreements and exchange information with foreign FIUs or domestic agencies, subject to applicable laws and safeguards;
(b) To require relevant persons in GMC to provide additional information or clarification on STRs/SARs submitted;
(c) To request, obtain, and access financial, administrative, and law enforcement information from public and private entities in GMC; and
(d) To issue directives, guidelines, and advisories to relevant persons in GMC regarding compliance with money laundering and sanctions obligations.

17.3 Governance and Independence

17.3.1 The head of the FIU shall report to the Managing Director of the GFSO, and also has direct access to the Board of Directors of GMC if required .

17.3.2 The FIU shall not be subject to the direction or control of any external authority in exercising its operational functions in relation to the receipt, analysis, and dissemination of financial intelligence.

17.3.3 The head of the FIU shall:

(a) be responsible for the day-to-day operations and management of the FIU; and
(b) ensure that the FIU carries out its relevant functions and duties as per this AML Rulebook.

17.5 Temporary Freezing Powers

17.5.1 The FIU may issue a temporary freeze notice over property held by a Relevant Person in GMC for a period not exceeding twenty-one days if :

(a) the FIU has a reasonable grounds to suspect that the property may be proceeds of or be connected with criminal activity whether committed in GMC or elsewhere; and
(b) a freeze notice is required to enable further analysis by the FIU or for investigative work to be undertaken by an enforcement authority.

17.5.2 The FIU shall immediately notify the competent court or enforcement authority upon issuing a freeze notice, to ensure oversight and due process.

17.6 Confidentiality and Tipping off

17.6.1 The FIU shall ensure strict confidentiality of all reports and information received from any Relevant Person or from any competent authority.

17.6.2 The FIU shall establish procedures to ensure the security and confidentiality of information held by the FIU.

17.6.3 No staff, consultant, or contractor of the FIU shall disclose information acquired in the course of their duties, except as required by law or for the performance of official functions.

17.6.5 Relevant Persons and their agents shall not disclose to customers, staff or third parties that:

(a) a report or any other information concerning suspected money laundering has been submitted to the FIU; or
(b) an investigation into money laundering has begun or is being carried out.

17.7 Record-Keeping

17.7.1 The FIU shall maintain secure records of all STRs/SARs, analysis, and dissemination activities for a minimum of six years in electronic format, provided that such records are readily accessible and available.