ALDERNEY
GAMBLING CONTROL COMMISSION

Guidance for eGambling businesses on Countering Financial Crime, Terrorist Financing and Proliferation Financing

17th May 2024

Contents

The following acronyms are used within this guidance.

AML	Anti-Money Laundering
App	Application
BACS	Bankers' Automated Clearing System
CDD	Customer Due Diligence
CECIS	Closed-Ended Collective Investment Scheme
CFT	Countering the Financing of Terrorism
CIS	Collective Investment Scheme
DT	Drug Trafficking
EC	European Council
ECDD	Enhanced Customer Due Diligence
ESAs	European Supervisory Authorities
EU	European Union
FATF	Financial Action Task Force
FIS	Financial Intelligence Service
FIU	Financial Investigation Unit
FSB	Financial Services Business
FT	Financing of Terrorism
GP	General Partner
IBAN	International Bank Account Number
IC	Incorporated Cell
ICC	Incorporated Cell Company
IFSWF	International Forum of Sovereign Wealth Funds
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
IT	Information Technology
LLP	Limited Liability Partnership
LP	Limited Partnership
LPP	Legal Professional Privilege
MI	Management Information
ML	Money Laundering
MLCO	Money Laundering Compliance Officer
MLRO	Money Laundering Reporting Officer

MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism
MSP	Money Service Provider
MVTS	Money or Value Transfer Service
NATO	North Atlantic Treaty Organization
NGCIS	Non-Guernsey Collective Investment Scheme
NPO	Non-Profit Organisation
NRA	National Risk Assessment
NRFSB	Non-Regulated Financial Services Business
OECD	Organisation for Economic Co-operation and Development
ECIS	Open-Ended Collective Investment Scheme
OFAC	Office of Foreign Assets Control
PB	Prescribed Business
PC	Protected Cell
PCC	Protected Cell Company
PEP	Politically Exposed Person
PF	Proliferation Financing
PQ	Personal Questionnaire
PSP	Payment Service Provider
RFID	Radio-Frequency Identification
SCDD	Simplified Customer Due Diligence
SDN	Specially Designated National
SIO	Senior Investigating Officer
SWF	Sovereign Wealth Fund
SWIFT	Society for Worldwide Interbank Financial Telecommunication
THEMIS	The FIS Online Reporting Facility for a Disclosure of Suspicion
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UK	United Kingdom
UN	United Nations
UNSCR	United Nations Security Council Resolutions
US	United States of America

Chapter 1

Introduction

1.1 The laundering of criminal proceeds, the financing of terrorism and the financing of the proliferation of weapons of mass destruction (henceforth referred to collectively as "ML, and FT") through the financial and business systems of the world is vital to the success of criminal and terrorist operations as well as the proliferation of weapons of mass destruction. To this end, criminals, terrorists and rogue states seek to exploit the facilities of the world's businesses in order to benefit from such proceeds or financing. Increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal proceeds can be laundered or terrorist funds transferred and have added to the complexity of audit trails. The future of the Bailiwick of Guernsey ("the Bailiwick") as a well-respected international financial centre depends on its ability to prevent the abuse of its designated non-financial prescribed businesses.

Background and scope

1.2 Money laundering is the term given to the process or processes by which criminals conceal or attempt to conceal the origin of the proceeds of their or others' criminal activities. After the money has been laundered it can then appear to be legitimate. Where criminal activity has generated a substantial profit, those involved will seek to find ways of disguising the origins of these profits, changing the form or nature of the funds as well as moving them around so as to legitimise the money and its source(s). Money laundering is a term that is frequently misunderstood. In the Bailiwick of Guernsey it is a defined term; however, in simple terms it means trying to turn funds obtained from or through criminal activity into "clean" money. It also covers handling the benefits of crimes of acquisition such as theft, fraud and tax evasion. In addition it is an offence to be involved in the funding of terrorism or dealing with property that is being used or laundered for that purpose. Operators are reminded that money laundering encompasses the application of funds from any form of criminal activity. The application of funds means spending or otherwise disposing of funds. There is no "*de minimis*" level. It should

be noted that money launderers are willing to spend money in order to launder their funds. This can be through the striking of a "bad bargain" or, potentially utilising the eGambling sector where there is a risk of loss. In addition eGambling operators may find that the activity of gambling is taking place with the proceeds of crime.

1.3 The Bailiwick authorities are committed to ensuring that criminals, including money launderers, terrorists and those financing terrorism or the proliferation of weapons of mass destruction, cannot launder the proceeds of crime through the Bailiwick or otherwise use the Bailiwick's finance and business sectors. This Guidance sets out the standards expected by the AGCC of all eGambling operators in the Bailiwick to ensure the Bailiwick's compliance with the FATF Recommendations. Should an eGambling operator assist in laundering the proceeds of crime or in the financing of a terrorist act or organisation, it could face regulatory investigation, the loss of its reputation, and law enforcement investigation. The involvement of an eGambling operator with criminal proceeds or terrorist funds would also damage the reputation and integrity of the Bailiwick as an international finance centre.

1.4 Under Section 1(1)of the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999 as amended ("the Law") all offences that are indictable under the laws of the Bailiwick are considered to be predicate offences and therefore funds or any type of property, regardless of value, acquired either directly or indirectly as the result of committing a predicate offence, are considered to be the proceeds of crime. Under Bailiwick law all offences are indictable, with the exception of some minor offences which mainly concern public order and road traffic. The range of predicate offences is therefore extremely wide and includes, but is not limited to, the following:

(a) participation in an organised criminal group and racketeering;
(b) terrorism, including FT;
(c) financing of proliferation of weapons of mass destruction;
(d) human trafficking and migrant smuggling;
(e) sexual exploitation, including sexual exploitation of children;
(f) illicit trafficking in narcotic drugs and psychotropic substances;
(g) illicit arms trafficking;
(h) illicit trafficking in stolen and other goods;
(i) corruption and bribery;

(j) fraud and tax evasion;
(k) counterfeiting and piracy of products;
(l) environmental crime;
(m) murder, manslaughter and grievous bodily injury;
(n) kidnapping, illegal restraint and hostage taking;
(o) robbery and theft;
(p) smuggling;
(q) extortion;
(r) forgery;
(s) piracy; and
(t) insider trading and market manipulation.

1.5 The Bailiwick's anti-money laundering ("AML") and countering the financing of terrorism ("CFT") legislation (and by extension this Guidance) applies to all eGambling operators conducting business in and outside the Bailiwick. This includes Bailiwick-based branches and offices of companies incorporated outside of the Bailiwick conducting aspects of eGambling within the Bailiwick.

1.6 The AGCC was established to regulate online gambling (known as eGambling in Alderney). The legislation sets out a number of key licensing objectives which govern the activities of the AGCC and are enshrined in the Alderney eGambling Ordinance, 2009 ("the Ordinance"). These are;

- Protecting and enhancing the reputation of Alderney as a well-regulated eGambling centre;
- Ensuring that eGambling is conducted honestly and fairly and in compliance with good governance;
- Preventing eGambling from being a source of crime, being associated with crime or being used to support crime, including preventing the funding, management and operation of eGambling from being under criminal influence; and
- Protecting the interests of young persons and other vulnerable persons from being harmed or exploited by eGambling.

1.7 In addition the functions of the Commission in relation to eGambling include taking such steps as the Commission considers necessary or expedient,

- For the effective regulation, supervision, and control of eGambling in Alderney and pursuant to the Alderney eGambling (Operations in Guernsey) Ordinance, 2006 in Guernsey,
- In order to pursue the licensing objectives,
- For maintaining confidence in, and the safety, soundness and integrity of Alderney's eGambling sector.

1.8 Within this guidance the term operator encompasses Category 1 eGambling licensees, Category 2 eGambling licensees, Category 1 Associate Certificate holders and Category 2 Associate Certificate holders. Entities undertaking Category 1 activity will have customer relationships and those undertaking Category 2 activity will have business relationships. A business relationship can be considered a customer relationship and customer relationships are business relationships.

1.9 The Alderney eGambling Ordinance 2009 and the Alderney eGambling Regulations, 2009 ("the Regulations") both came into force on 1st January, 2010. These replaced the previous legislative framework and strengthened the AML/CFT regime in force for eGambling operations. On 15th September, 2020 the Alderney eGambling (Amendment) Ordinance, 2020 came into force. This moved AML/CFT obligations from being set out in a Schedule to the Regulations (Schedule 16) and they are now set out in Schedule 4 to the Ordinance (referred to henceforth as "Schedule 4") and whilst the main change was to make this move a number of other revisions were also made to reflect best practice. On 8th February, 2024 the Alderney eGambling (Proliferation Financing etc.) Regulations, 2024 ("the 2024 Regulations") were made by the Commission and took immediate effect. Pursuant to the 2024 Regulations operators are required to consider the risks of a breach of a TFS as if it also included PF in business risk assessments and customer risk assessments. For the purposes of the 2024 Regulations a breach of a TFS includes the non-implementation, circumvention or evasion of the targeted financial sanction. In addition the 2024 Regulations require references in the Ordinance to the NRA are deemed to include a reference to any national risk assessment in

respect of the proliferation of weapons of mass destruction and its financing published by the States of Guernsey Policy & Resources Committee, as amended from time to time

Chapter 2

The Bailiwick's AML and CFT framework

2.1 The Bailiwick's AML and CFT framework includes legislation (henceforth referred to as "the Relevant Enactments"):

A comprehensive list of the Relevant Enactments that are in force from time to time can be found on the website of the GFSC.

https://www.gfsc.gg/commission/financial-crime/handbook-on-countering-financial-crime-AML/CFT/CPF

And such other enactments relating to ML and FT as may be enacted from time to time in the Bailiwick.

2.2 Sanctions legislation is published by the States of Guernsey's Policy & Resources Committee and can be accessed via the below website (and a link is available from the AML/CFT resource area of the AGCC's website):

https://www.gov.gg/sanctionsmeasures

Guidance purpose

2.3 This guidance is issued by the AGCC and, together with the relevant enactments, eGambling legislation, Instructions and Notices forms the basis of the obligation set out in Section 1 of Schedule 4. It is designed to assist those involved in eGambling in complying with the requirements of relevant legislation concerning ML, TF, PF, financial crime and relevant offences to prevent the Bailiwick's financial system from being abused for ML, TF and PF. Instructions, Notices and guidance issued by the AGCC will be used in determining whether or not an eGambling operator has complied with Schedule 4 of the Ordinance.

2.4 This guidance has the following additional purposes:

(a) to outline the legal and regulatory framework for AML and CFT requirements and systems;

(b) to interpret the requirements of the Relevant Enactments and provide guidance on how they may be implemented in practice;

(c) to indicate good industry practice in AML and CFT procedures through a proportionate, risk-based approach;

(d) to assist in the design and implementation of systems and controls necessary to mitigate the risks of eGambling being used in connection with ML and FT and other financial crime and to ensure that customers are not on TFS or PF sanctions lists; and

(e) to assist those involved in aspects of eGambling that may not necessarily have a financial aspect in understanding the need for processes or procedures that must be followed that may not necessarily impact on their area but are required to ensure that eGambling is not used for ML or TF.

2.5 The AGCC acknowledges the differing approaches adopted by eGambling operators to achieve compliance with the requirements of the Relevant Enactments and the ICS Guidelines. This guidance therefore seeks to adopt a technology neutral stance, allowing the operator to embrace whichever technological solution(s) it deems appropriate to meet its obligations.

Requirements of Schedule 4

2.6 Schedule 4 includes requirements relating to:

(a) risk assessment and mitigation;

(b) applying CDD measures;

(c) monitoring customer activity and ongoing CDD;

(d) reporting suspected ML and FT activity;

(e) employee screening and training;

(f) record keeping; and

(g) ensuring compliance, corporate responsibility and related requirements.

2.7 Any paraphrasing of Schedule 4 within parts of this guidance represents the AGCC's own explanation of that schedule and is for the purposes of information and assistance only. Schedule 4 of the Ordinance remains the definitive text for the operator's AML and CFT obligations. The AGCC's paraphrasing does not detract from the legal effect of Schedule 4 or from its enforceability by the courts. In case of doubt, you are advised to consult a Bailiwick Advocate.

Significant failure to meet the required standards

2.8 Existing eGambling operators will be familiar with the requirements of the AGCC with regards to the work that is required in order to commence operations. The grant of the licence or certificate is merely the first stage of commencing operations as activity cannot commence until such time as the AGCC has approved the operators Internal Control System ("ICS") which sets out in detail all parameters of how operations will be conducted and which has a dedicated section relating to AML/CFT matters. The Guidelines issued by the AGCC for the preparation of an Internal Control System can be found on the AGCC's website at

https://www.gamblingcontrol.org/applications-guidance/ics-guidelines

The ICS is a regulatory requirement and must follow the specific headings set out in the Regulations.

2.9 For any operator regulated by the AGCC, the primary consequences of any significant failure to meet the standards required by Schedule 4 , the ICS guidelines and the Relevant Enactments will be legal ones. In this respect the AGCC will have regard to the operator's compliance with the provisions of Schedule 4, the ICS guidelines and the Relevant Enactments when considering whether to take enforcement action against it in respect of a breach of any requirements imposed on the operator. In such cases, the AGCC has powers to impose a range of disciplinary and financial sanctions, including the power to suspend, revoke or withdraw the licence or certificate of the operator where applicable. In addition the AGCC is entitled to take such failure into consideration in the exercise of its judgement as to whether the operator and its key individuals, directors and managers have satisfied the minimum criteria for licensing or certification. In particular, in determining whether the operator is carrying out its business with integrity and skill and whether a natural person is fit and proper, the AGCC must have regard

to compliance with the Ordinance and in particular, Schedule 4, the Regulations, the ICS Guidelines and the Relevant Enactments.

Data Protection

2.10 The Bailiwick's AML and CFT legislation requires the operator to collate and retain records and documentation. Where such records and documentation contain personal data, the operator will need to comply with the Data Protection (Bailiwick of Guernsey) Law, 2017 ("the Data Protection Law") which brings the Bailiwick into line with the European Union's ("EU") regulation on data protection and privacy for all individuals within the EU.

https://www.odpa.gg/

Financial Action Task Force

2.11 The FATF is an inter-governmental body that was established in 1989 by the ministers of its member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating ML, FT, the financing of the proliferation of weapons of mass destruction and other related threats to the integrity of the international financial system. The FATF Recommendations are recognised as the global AML and CFT standard. The FATF Recommendations therefore set an international standard which countries should implement through measures adapted to their particular circumstances. The FATF Recommendations set out the essential measures that countries should have in place to:

(a) identify risks and develop policies and domestic co-ordination;
(b) pursue ML, FT and the financing of proliferation of weapons of mass destruction;
(c) apply preventive measures for the financial sector and other designated sectors;
(d) establish powers and responsibilities for the competent authorities (for example, investigative, law enforcement and supervisory authorities) and other institutional measures;
(e) enhance the transparency and availability of beneficial ownership information of legal persons and legal arrangements; and
(f) facilitate international co-operation

The National Risk Assessment

2.12 In accordance with the FATF Recommendations, the Bailiwick, led by the States of Guernsey's Policy & Resources Committee, conducted a National Risk Assessment ("NRA") which was intially published in January 2020. An updated NRA was published in December 2023 colloquially known as NRA2. The NRA is based on the methodology developed by the International Monetary Fund ("IMF") supplemented by additional information provided by the relevant agencies within the Bailiwick and industry to ensure a thorough assessment of the ML, FT and PF risks presented by the individual sectors within the finance industry and products and services from within the Bailiwick. The key finding of the NRA with regard to ML risk is that as an international finance centre with a low domestic crime rate, the Bailiwick's greatest ML risks comes from the laundering of the proceeds of foreign criminality. The underlying offences most likely to be involved are bribery and corruption and fraud (including tax evasion). The key finding of the NRA with regard to FT risks is that the greatest risks come from its cross-border business being used to support foreign terrorism, by funds being passed through or administered from the Bailiwick. However, this risk is much lower than the ML risks from cross-border business. FT from cross-border business is most likely to arise in the context of secondary terrorist financing, i.e. where criminal proceeds are used to fund terrorism. NRA2 has increased the stated risk of ML in eGambling from medium lower to medium and for terrorist financing from much lower to lower. NRA2 has identified that the risks of PF in the Bailiwick are very low and accordingly the risks of PF in the eGambling sector are negligible. The assessment of risks and vulnerabilities detailed within the NRA will naturally cascade through to specified businesses within the Bailiwick. In this respect, references are made throughout Schedule 4 and this guidance requires the operator to have regard to the content of the NRA when undertaking certain activities, for example, the formulation of its business risk assessments and risk appetite. The Bailiwick will continue to review the NRA on an on-going and trigger-event basis, making changes as necessary taking into account market changes, the advancement of technology and data collected from industry, for example, through various surveys and regulatory returns.

2.13 A copy of the Bailiwick's NRA2 can be found on the website of the States of Guernsey's Policy & Resources Committee:

https://www.gov.gg/finance-risk-assessment

MONEYVAL

2.14 The Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism ("MONEYVAL") is a monitoring body of the Council of Europe. The aim of MONEYVAL is to ensure that its member states have in place effective systems to counter ML and FT and comply with the relevant international standards in these fields. On 10th October, 2012 the Committee of Ministers of the Council of Europe, following a request by the United Kingdom ("UK"), adopted a resolution to allow the Bailiwick, the Bailiwick of Jersey and the Isle of Man (the "Crown Dependencies") to participate fully in the evaluation process of MONEYVAL and to become subject to its procedures. MONEYVAL's most recent evaluation of the Bailiwick was conducted during October 2014 and assessed the Bailiwick's compliance with the FATF 2003 Recommendations. In its report, published on 15 January 2016, MONEYVAL concluded that the Bailiwick has 'a mature legal and regulatory system' and surpassed the equivalent review by the IMF in 2010. MONEYVAL will perform a 4th round assessment of the Bailiwick in April 2024.

https://www.coe.int/en/web/moneyval/jurisdictions/guernesey

Corporate governance

2.15 Good corporate governance should provide proper incentives for the board or senior management to pursue objectives that are in the interests of the operator and its shareholders and should facilitate effective monitoring of the operator for compliance with its AML and CFT obligations.

2.16 The Organisation for Economic Co-operation and Development ("OECD") describes the corporate governance structure of a firm (operator for the purposes of this guidance) as the distribution of rights and responsibilities among different participants, such as the board, managers and other stakeholders, and the defining of the rules and procedures for making decisions on corporate affairs.

2.17 The presence of an effective corporate governance system, within an individual company and across an economy as a whole, is key to building an environment of trust, transparency and accountability necessary for fostering long-term investment, financial

stability and business integrity and helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.

2.18 This chapter, together with Schedule 4, provides a framework for the oversight of the policies, procedures and controls of the operator to counter ML and FT.

2.19 In accordance with Paragraph 15(7) of Schedule 4, references in this chapter and in the wider guidance to the "board" shall mean the board of directors of the operator where it is a body corporate, or the senior management of where it is not a body corporate.

Board responsibility for compliance

2.20 The board of the operator has effective responsibility for compliance with Schedule 4 and the AGCC ICS guidelines . References to compliance in this guidance generally are to be taken as references to compliance with Schedule 4 and the AGCC ICS guidelines.

2.21 The board of the operator is responsible for managing the operator effectively and is in the best position to understand and evaluate all potential risks to the operator, including those of ML and FT as well as the risks of breaching TFS and PF sanctions. The board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant. (Schedule 4 Section 2)

2.22 More information on the process and requirements for conducting business risk assessments can be found in Chapter 4 of this guidance.

2.23 The board must organise and control the operator effectively, including establishing and maintaining appropriate and effective policies, procedures and controls as detailed below, and having adequate resources to manage and mitigate the identified risks of ML and FT taking into account the size, nature and complexity of its business. (Schedule 4 Section 2(4))

2.24 Taking into account the conclusions of the business risk assessments, in accordance with Paragraph 2(7) of Schedule 4, the operator shall have in place effective policies, procedures and controls to identify, assess, mitigate, manage, review and monitor those risks

in a way that is consistent with the requirements of Schedule 4, the Relevant Enactments, the current NRA and the AGCC ICS guidelines and this guidance.

2.25 In addition to the general duty to understand, assess and mitigate risks as set out in Paragraph 2 of Schedule 4 and the requirement to maintain effective policies, procedures and controls contained therein, the operator should be aware that other paragraphs of Schedule 4 and this guidance also contain more specific requirements in respect of the policies, procedures and controls required to mitigate particular risks, threats and vulnerabilities.

2.26 These policies, procedures and controls should enable the operator to comply with the requirements of Schedule 4 and the AGCC ICS guidelines, including amongst other things, to:

(a) conduct, document and maintain business risk assessments to identify the inherent ML and FT risks to the operator and to define the operator's AML and CFT risk appetite and identify the risks of a breach of TFS and PF sanctions (see Chapter 4);

(b) conduct risk assessments of all business relationships to identify those to which Enhanced Customer Due Diligence ("ECDD") measures and monitoring must be applied;

(c) apply sufficient Customer Due Diligence ("CDD") measures to identify, and verify the identity of, customers, beneficial owners and other key principals, whether natural persons, legal persons and legal arrangements, and to establish the purpose and intended nature of the business relationship (see Chapters 5-8);

(d) apply ECDD measures to those business relationships deemed to pose a high risk of ML or FT;

(e) conduct transaction and activity monitoring (see Chapter 9);

(f) monitor business relationships on a frequency appropriate to the assessed risk to ensure that any unusual, adverse or suspicious activity is highlighted and given additional attention (see Chapter 9);

(g) screen customers, payees, beneficial owners and other key principals to enable the prompt identification of any natural persons, legal persons or legal arrangements subject to United Nation ("UN"), EU TFS, PF or other sanction (see Chapter 10);

(h) report promptly to the FIS where an employee knows or suspects, or has reasonable grounds for knowing or suspecting, that another person is involved

in ML and/or FT (including in connection with an attempted transaction) (see Chapter 11) or is subject to sanction as set out in (g) above;

(i) screen potential employees to ensure the probity and competence of board and staff members (see Chapter 12);

(j) provide suitable and sufficient AML and CFT training and training on the risks of breaching TFS and PF sanctions to all relevant employees, identify those employees to whom additional training must be provided and provides such additional training (see Chapter 12);

(k) maintain records for the appropriate amount of time and in a manner which enables the operator to access relevant data in a timely manner (see Chapter 13); and

(l) ensure that, where the operator is a majority owner or exercises control over a branch office or subsidiary established outside the Bailiwick, the branch office or subsidiary applies controls consistent with the requirements of Schedule 4 or requirements consistent with the FATF Recommendations.

Board Oversight of Compliance

2.27 In accordance with Paragraph 13(e) of Schedule 4, the operator shall establish and maintain an effective policy, for which responsibility shall be taken by the board, for the review of its compliance with the requirements of Schedule 4 and this guidance, and such policy shall include provision as to the extent and frequency of such reviews.

2.28 The board must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance, adopting a risk based approach, or whenever material changes to the business of the operator or the requirements of Schedule 4 or this guidance occur. Where, as a result of its review, changes to the compliance arrangements or review policy are required, the board must ensure that the operator makes those changes in a timely manner.

2.29 As part of its compliance arrangements, the operator is responsible for appointing a MLCO who, together with the MLRO and NO is responsible for the operator's compliance with its policies, procedures and controls to forestall, prevent and detect ML and FT. This

Section should therefore be read in conjunction with Chapter 2 of this guidance which sets out the roles and responsibilities of the MLCO, MLRO and NO.

2.30 In addition to appointing a MLCO, the board of the operator must also maintain an independent audit function to test the ML and FT policies, procedures and controls of the operator in accordance with Section 13(e)(ii) of Schedule 4.

2.31 The board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the operator, including the risks identified in the business risk assessments. The policy must include a requirement for sample testing of the effectiveness and adequacy of the operator's policies, procedures and controls.

2.32 The board should take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to the operator are reviewed more frequently. In this respect the policy should review the appropriateness, effectiveness and adequacy of the policies, procedures and controls established in accordance with the requirements of Schedule 4 and this guidance. This includes, but is not limited to:

(a) the application of CDD measures, including ECDD, SCDD and enhanced measures;
(b) the Management Information ("MI") received by the board, including information on any branch offices and subsidiaries;
(c) the management and testing of third parties upon which reliance is placed for the application of CDD measures, for example, under an outsourcing arrangement;
(d) the ongoing competence and effectiveness of the MLRO;
(e) the handling of internal disclosures to the MLRO and external disclosures and any production orders or requests for information to or from the FIS;
(f) the management of sanctions risks and the handling of sanctions notices;
(g) the provision of AML and CFT training, including an assessment of the methods used and the effectiveness of the training received by employees; and
(h) the policies, procedures and controls surrounding bribery and corruption, including both the employees and customers of the operator, for example, gifts and hospitality policies and registers.

2.33 In accordance with Paragraph 13(f) of Schedule 4, the operator shall ensure that a review of its compliance with Schedule 4 and this guidance is discussed and minuted at a meeting of the board at appropriate intervals, and in considering what is appropriate, the operator shall have regard to the risk taking into account –

(a) the size, nature and complexity of the eGambling it conducts,
(b) its registered customers (in relation to a Category 1 eGambling licensee or Category 1 associate certificate holder only), products and services, and
(c) the ways in which it provides those products and services.

2.34 The board may delegate some or all of its duties but must retain responsibility for the review of overall compliance with the AML and CFT requirements of Schedule 4, this guidance and the Relevant Enactments.

2.35 Where the operator identifies any deficiencies as a result of its compliance review policy, it must take appropriate action to remediate those deficiencies as soon as practicable and give consideration to the requirements of Regulation 191 where the deficiencies identified are considered to be serious or material.

Outsourcing

2.36 Where the operator outsources a function to a third party (either within the Bailiwick or overseas, or within its group or externally) the board remains ultimately responsible for the activities undertaken on its behalf and for compliance with the requirements of Schedule 4, this guidance and the Relevant Enactments. The operator cannot contract out of its statutory and regulatory responsibilities to prevent and detect ML and FT. This Section should be read as referring to the outsourcing of any function relevant to the operator's compliance with its obligations under Schedule 4, this guidance and the Relevant Enactments, for example, the appointment of a third party as the operator's MLCO or MLRO, or the use of a third party to gather the requisite identification data for the operator's customers and other key principals. Where the operator is considering the outsourcing of functions to a third party it should:

(a) consider the AGCC's position on outsourcing;

(b) consider implementing a terms of reference or agreement describing the provisions of the arrangement. This will include the formulation of a policy which satisfies the ICS guidelines;

(c) ensure that the roles, responsibilities and respective duties of the operator and the outsourced service provider are clearly defined and documented;

(d) ensure that the board, the MLRO, the MLCO, other third parties and all employees understand the roles, responsibilities and respective duties of each party; and

(e) ensure that it has appropriate oversight of the work undertaken by the outsourced service provider.

2.37 Prior to a decision being made to establish an outsourcing arrangement, the operator must make an assessment of the risk of any potential exposure to ML and TF and must maintain a record of that assessment as part of its business risk assessments. The operator should monitor the risks identified by its assessment of an outsourcing arrangement and review this assessment on an on-going basis in accordance with its business risk assessment obligations. The operator should ensure, at the commencement of an outsourcing arrangement and on an ongoing basis, that:

(a) the outsourced service provider:

(i) has the appropriate knowledge, skill and experience;

(ii) is cognisant of the applicable AML and CFT requirements;

(iii) is sufficiently resourced to perform the required activities;

(iv) has in place satisfactory policies, procedures and controls which are, and continue to be, applied to an equivalent standard and which are kept up to date to reflect changes in regulatory requirements and emerging ML and TF risks; and

(v) is screened and subject to appropriate due diligence to ensure the probity of the outsourced service provider;

(b) the work undertaken by the outsourced service provider is monitored to ensure it complies with the requirements of Schedule 4, this guidance, the ICS guidelines and the Relevant Enactments;

(c) any reports or progress summaries provided to the operator by the outsourced service provider contain meaningful, accurate and complete information about

the activities undertaken, progress of work and areas of non-compliance identified; and

(d) the reports received from the outsourced service provider explain in sufficient detail the materials reviewed and other sources investigated in arriving at its conclusions so as to allow the operator to understand how findings and conclusions were reached and to test or verify such findings and conclusions.

2.38 The fact that the operator has relied upon an outsourced service provider or the report of an outsourced service provider will not be considered a mitigating factor where the operator has failed to comply with a requirement of Schedule 4, this guidance, the ICS guidelines or the Relevant Enactments. The board should therefore ensure the veracity of any reports provided by an outsourced service provider, for example, by spot-checking aspects of such reports.

2.39 The operator must ensure that the outsourced service provider has in place procedures which include a provision that knowledge, suspicion, or reasonable grounds for knowledge or suspicion, of ML and/or TF activity in connection with the outsourcing operator's business will be reported by the outsourced service provider to the MLRO of the outsourcing operator (subject to any tipping off provisions to which the outsourced service provider is subject) in a timely manner. The exception to this would be where the outsourced service provider forms a suspicion that the outsourcing operator is complicit in ML and/or TF activity. In such cases the outsourced service provider, where it is a specified business, must disclose its suspicion to the FIS in accordance with Chapter 11 of this guidance and advise the AGCC of its actions.

2.40 Where the operator chooses to outsource or subcontract work to an unregulated entity, it should bear in mind that it remains subject to the obligation to maintain appropriate policies, procedures and controls to prevent ML and TF. In this context, the operator should consider whether such subcontracting increases the risk that it will be involved in, or used for, ML and/or TF, in which case appropriate and effective controls to address that risk should be implemented.

Foreign branches and Subsidiaries

2.41 In accordance with Paragraph 14 of Schedule 4, the operator shall ensure that any of its branch offices and, where it is a body corporate, anybody corporate of which it is the majority shareholder or control of which it otherwise exercises, which, in either case, is a specified

business in any country or territory outside the Bailiwick (collectively "its subsidiaries"), complies there with:

(i) the requirements of Schedule 4 and this guidance, and

(ii) any requirements under the law applicable in that country or territory which are consistent with the FATF Recommendations, provided that, where requirements under (i) above differ, the operator shall ensure that the requirement which provides the highest standard of compliance, by reference to the FATF Recommendations, is complied with.

2.42 In determining whether the operator exercises control over another entity, examples could include one or more of the following:

(a) where the operator makes appointments to the board or senior management of that entity;

(b) where the operator determines that entity's business model or risk appetite; and/or

(c) where the operator is involved in the day-to-day management of that entity.

2.43 The AML and CFT programmes should incorporate the measures required under Schedule 4, should be appropriate to the business of its subsidiaries and should be implemented effectively at the level of those entities.

2.44 The policies, procedures and controls referenced above should ensure that adequate safeguards on the confidentiality and use of information exchanged between the operator and its subsidiaries are in place and that such sharing and use is subject to the provisions of the data protection legislation of the jurisdictions within which its subsidiaries are located.

2.45 In accordance with Paragraph 14(4) of Schedule 4, the obligations above apply to the extent that the law of the relevant country or territory allows and if the law of the country or territory does not so allow in relation to any requirement of Schedule 4, the operator shall notify the AGCC accordingly.

2.46 In addition to advising the AGCC, the operator should also ensure that appropriate controls are implemented to mitigate any risks arising related to the specific areas where compliance with appropriate AML and CFT measures cannot be met.

2.47 The operator must be aware that the inability to observe appropriate AML and CFT measures is particularly likely to occur in countries or territories which do not, or insufficiently apply, the FATF Recommendations. In such circumstances the operator must take appropriate steps to effectively deal with the specific ML and FT risks associated with conducting business in such a country or territory.

Liaison with the AGCC

2.48 The board of the operator must ensure that the AGCC is notified of any material failure to comply with the provisions of Schedule 4, this guidance or the Relevant Enactments, or of any serious breaches of the policies, procedures or controls of the operator.

2.49 The following are examples of the types of scenarios in which the AGCC would expect to be notified. This list is not definitive and there may be other scenarios where the AGCC would reasonably expect to be notified:

(a) the operator identifies, either through its compliance monitoring arrangements or by other means (for example a management letter from an auditor) areas of material non-compliance where remediation work is required;
(b) the operator receives a report, whether orally or in writing, from an external party engaged to review its compliance arrangements, identifying areas of material non-compliance where remediation work is recommended;
(c) the operator receives a report from a whistle-blower and an initial or provisional investigation reveals some substance to the concerns raised;
(d) the operator is aware that an aspect of material non-compliance may have occurred across more than one member of its corporate group, including the operator (or the parent of the operator where it is a branch office), which may have a bearing on the operator's compliance with its AML and CFT obligations and/or the effectiveness of the operator's compliance arrangements;

(e) the operator discovers that the party to whom it has outsourced functions critical to compliance with Schedule 4, this guidance or the Relevant Enactments has failed to apply one or more of the requirements of Schedule 4, this guidance or the Relevant Enactments and remediation work is required;

(f) any aspect of material non-compliance identified involving a business relationship with a relevant connection to a country listed in a BSSN issued by the AGCC and those covered by sanctions legislation applicable in the Bailiwick, regardless of the values involved; or

(g) any breach of the requirements placed upon the operator by the Bailiwick's sanctions framework, regardless of the number of business relationships or values involved.

2.50 In addition to the above, the AGCC would expect to be notified where the operator identifies a breakdown of administrative or control procedures (for example, a failure of a computer system) or any other event arising which is likely to result in a failure to comply with the provisions of Schedule 4, this guidance and/or the Relevant Enactments.

2.51 The AGCC recognises that from time to time the operator may identify instances of non-compliance as part of its ongoing monitoring or relationship risk assessment review programmes. Provided that a matter meets the following criteria then notification to the Commission may not be required:

(a) it is isolated in nature;

(b) it is readily resolvable within a short period of time;

(c) it does not pose a significant risk to the operator; and

(d) it does not compromise the accuracy of:

  (i) the CDD information held for the customer, beneficial owner or other key principal;

  (ii) the operator's understanding of the beneficial ownership of the customer; and

  (iii) the operator's understanding of the purpose and intended activity of the business relationship.

2.52 Notwithstanding that notification to the AGCC may not be required in the above circumstances, the operator should document its assessment of a matter and its conclusions as to why it is not considered to be material. The AGCC reserves the right to enquire about such instances of non-compliance during on-site visits, thematic reviews and other engagements with the operator. Where the operator has determined that a matter warrants notification to the AGCC, the AGCC would expect to receive early notice, even where the full extent of the matter is yet to be confirmed or the manner of remediation decided.

Money Laundering Compliance Officer

2.53 In accordance with Paragraph 13(a)of Schedule 4, the operator shall appoint an executive officer as the MLCO, provide the name, title and email address of that person to the FIS and provide a copy of that notification to the AGCC as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

2.54 The MLCO appointed by the operator must:

(a) be a natural person;
(b) be of at least executive officer level;
(c) have the appropriate knowledge, skill and experience to fulfil a compliance role within the operator;
(d) be employed by the operator or an entity within the same group as the operator or in another entity that is shown to the satisfaction of the AGCC to be effective;

2.55 The operator must ensure that the MLCO:

(a) has timely and unrestricted access to the records of the operator;
(b) has sufficient resources to perform their duties;
(c) has the full co-operation of the operator's staff;
(d) is fully aware of their obligations and those of the operator; and
(e) reports directly to, and has regular contact with, the board so as to enable the board to satisfy itself that all statutory obligations and provisions in Schedule 4, this guidance and the Relevant Enactments are being met and that the operator

is taking sufficiently robust measures to protect itself against the potential risk of being used for ML or FT

2.56 As defined in Paragraph 15(1) of Schedule 4, the MLCO appointed by the operator shall monitor compliance with policies, procedures and controls to forestall, prevent and detect ML and FT.

2.57 The board is responsible for the operator's compliance with Schedule 4 and this guidance, including establishing appropriate and effective policies, procedures and controls to forestall, prevent and detect ML and FT. By contrast, the MLCO's role is to monitor the operator's compliance with its policies, procedures and controls and periodically report thereon to the board. In this respect the functions of the MLCO include:

(a) overseeing the monitoring and testing of AML and CFT policies, procedures, controls and systems in place to assess their appropriateness and effectiveness;
(b) investigating any matters of concern or non-compliance arising from the operator's compliance review policy;
(c) establishing appropriate controls to mitigate any risks arising from the operator's compliance review policy and to remediate issues where necessary and appropriate in a timely manner;
(d) reporting periodically to the board on compliance matters, including the results of the testing undertaken and any issues that need to be brought to the board's attention; and
(e) acting as a point of contact with the AGCC and to respond promptly to any requests for information made.

2.58 While it is not anticipated that the MLCO will personally conduct all monitoring and testing, the expectation is that the MLCO will have oversight of any monitoring and testing being conducted by the operator, for example, by a compliance team or an outsourcing oversight team, in accordance with the operator's compliance review policy.

2.59 The circumstances of the operator may be such that, due to the small number of employees, the MLCO holds additional functions or is responsible for other aspects of the operator's operations. Where this is the case, the operator must ensure that any conflicts of

interest between the MLCO role and any other functions held are identified, documented and appropriately managed.

2.60 For the avoidance of doubt, the same individual can be appointed to the positions of MLRO and MLCO, provided the operator considers this appropriate having regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively. However such an appointment would need to be referred to in the operator's approved ICS.

Money Laundering Reporting Officer

2.61 In accordance with Paragraph 10(1)(a) of Schedule 4, the operator shall appoint an executive officer as the MLRO, provide the name, title and email address of that person to the AGCC as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment, and ensure that all employees are aware of the name of that person.

2.62 In addition to notifying the Commission, in accordance with Paragraph 10(1)(a) of Schedule 4, the operator shall provide the name, title and email address of the MLRO to the FIS as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

2.63 The MLRO appointed by the operator must:

(a) be a natural person;
(b) be of at least executive officer level;
(c) have the appropriate knowledge, skill and experience;
(d) be employed by the operator or an entity within the same group as the operator or in another entity that is shown to the satisfaction of the AGCC to be effective;

2.64 The operator must ensure that the MLRO:

(a) is the main point of contact with the FIS in the handling of disclosures;

(b) has unrestricted access to the CDD information of the operator's customers, including the beneficial owners thereof;
(c) has sufficient resources to perform their duties;
(d) is available on a day-to-day basis;
(e) receives full co-operation from all staff;
(f) reports directly to, and has regular contact with, the board or equivalent of the operator; and
(g) is fully aware of both their personal obligations and those of the operator under Schedule 4, this guidance and the Relevant Enactments.

2.65 The operator must provide the MLRO with the authority to act independently in carrying out their responsibilities under Part 1 of the Disclosure Law or Section 12, 15 or 15A of the Terrorism Law. The MLRO must be free to have direct access to the FIS in order that any suspicious activity may be reported as soon as possible. The MLRO must also be free to liaise with the FIS on any question of whether to proceed with a transaction in the circumstances.

Nominated Officer

2.66 In accordance with Paragraph 10(1)(b) of Schedule 4, the operator shall nominate a person to –

(a) receive disclosures, under Part I of the Disclosure Law and Section 12 or Section 15 of the Terrorism Law (a "Nominated Officer"), in the absence of the MLRO, and
(b) otherwise carry out the functions of the MLRO in that officer's absence,
and ensure that all employees are aware of the name of that Nominated Officer.

2.67 In accordance with Paragraph 10(1)(b) of Schedule 4, the operator shall provide the name, title and email address of any person to the AGCC and the FIS as soon as is reasonably practicable and, in any event, within fourteen days starting from the date of that person's appointment.

2.68 The Nominated Officer must:

(a) be a natural person; and

(b) have the appropriate knowledge, skill and experience.

2.69 The operator must communicate the name of the Nominated Officer to all employees of the operator and ensure that all employees of the operator are aware of the natural person(s) to whom internal disclosures are to be made in the absence of the MLRO.

Chapter 3

Risk based approach

Introduction

3.1 This chapter is designed to assist the operator in taking a risk-based approach to the prevention of its products and services being used for the purposes of ML and FT and is broken down into three main sections:

(a) Risk-Based Approach - which provides a high-level overview of the risk-based approach;
(b) Business Risk Assessments - which details the relevant requirements of Schedule 4, together with the ICS guidelines and guidance, in respect of the operator undertaking ML and FT business risk assessments and determining its risk appetite; and
(c) Relationship Risk Assessments - which sets out the relevant obligations of Schedule 4, together with the AGCC guidance, for the conducting of risk assessments of new and existing business relationships.

Risk-Based Approach

Definition, Purpose and Benefits

3.2 A risk-based approach towards the prevention and detection of ML and FT aims to support the development of preventative and mitigating measures that are commensurate with the ML and FT risks identified by the operator and to deal with those risks in the most cost-effective and proportionate way.

3.3 Paragraph 1 of Schedule 4 provides a general duty for the operator to understand, assess and mitigate risks. In this respect the operator shall:

(a) understand its ML and FT risks and the risks of breaching TFS or PF sanctions; and

(b) have in place effective policies, procedures and controls to:

(i) identify,

(ii) assess,

(iii) mitigate,

(iv) manage, and

(v) review and monitor,

those risks in a way that is consistent with the requirements of Schedule 4, the Relevant Enactments, the requirements of this guidance and the NRA.

3.4 A risk-based approach prescribes the following procedural steps to manage the ML and FT risks faced by the operator:

(a) identifying the specific threats posed to the operator by ML and FT and those areas of the operator's business with the greatest vulnerability;

(b) assessing the likelihood of those threats occurring and the potential impact of them on the operator;

(c) mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;

(d) managing the residual risks arising from the threats and vulnerabilities that the operator has been unable to mitigate; and

(e) reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the operator which necessitate changes to its policies, procedures and controls.

3.5 In applying a risk-based approach and taking the steps detailed above, it is crucial that, regardless of the specific considerations and actions of the operator, clear documentation is prepared and retained to ensure that the board and senior management can demonstrate their compliance with the requirements of Schedule 4 and the ICS Guidelines and this guidance.

3.6 A risk-based approach starts with the identification and assessment of the risk that has to be managed. In the context of Schedule 4 and this guidance, a risk-based approach requires the operator to assess the risks of how it might be involved in ML and FT, taking into account its customers (and the beneficial owners of customers), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

3.7 In determining how the risk-based approach should be implemented, the operator should analyse and seek to understand how the identified ML and FT risks affect its business. This determination should take into account a range of information, including (amongst others) the type and extent of the risks that the operator is willing to accept in order to achieve its strategic objectives, its AML and CFT experience and the Bailiwick's NRA.

3.8 Through the business risk assessments, the operator can establish the basis for a risk-sensitive approach to managing and mitigating ML and FT risks. It should be noted, however, that a risk-based approach does not exempt the operator from the requirement to apply enhanced measures where it has identified higher risk factors as detailed in Chapter 8 of this guidance.

3.9 Schedule 4 and this guidance do not prohibit the offering of any products or services or the acceptance of any customer, unless it is known, or there are reasonable grounds to suspect, that the customer, or the beneficial owner thereof, is undertaking or associated with ML or FT. The risk-based approach, as defined in Schedule 4 and this guidance, instead requires that the risks posed by customers (and the beneficial owners of customers), countries and geographic areas, products, services, transactions and delivery channels are identified, assessed, managed and mitigated and that evidence of such is documented and reviewed on an on-going basis.

3.10 By adopting a risk-based approach the operator should ensure that measures to prevent or mitigate ML and FT are commensurate with the risks identified. In this respect, the business risk assessments will also serve to enable the operator to make decisions on how to allocate its resources in the most efficient and effective way and to determine its appetite and tolerance for risk.

3.11 No system of checks will detect and prevent all ML and FT. A risk-based approach will, however, serve to balance the cost burden placed upon the operator and its customers with a realistic assessment of the threat of the operator being used in connection with ML and/or FT. It focuses the effort where it is needed and has most impact.

3.12 The benefits of a risk-based approach include:

(a) recognising that the ML and FT threats to the operator vary across its customers, countries/geographic areas, products/services and delivery channels;
(b) providing for the board to apply its own approach to the policies, procedures and controls of the operator in particular circumstances, enabling the board to differentiate between its customers in a way that matches the risk to its particular business;
(c) helping to produce a more cost-effective system of risk management;
(d) promoting the prioritisation of effort and activity by reference to the likelihood of ML and/or FT occurring;
(e) reflecting experience and proportionality through the tailoring of effort and activity to risk;
(f) enabling the application of the requirements of Schedule 4 and this guidance sensibly and in consideration of all relevant risk factors; and
(g) allowing for the consideration of the accumulation of identified risks and the determination of the level of overall risk, together with the appropriate level of mitigation to be applied.

3.13 It is important to acknowledge that types of business, whether in terms of products/services, delivery channels or types of customers, can differ materially. An approach to preventing ML and FT that is appropriate for one business may be inappropriate in another.

Risks in eGambling

3.14 A number of vulnerabilities have been found in the eGambling sector including:-

(a) The cross border nature of online gambling
(b) The rapidity and cross border nature of transactions

(c) The non face to face nature of online gambling
(d) The low number of investigations and prosecutions of ML/TF cases
(e) Crediting winnings to different accounts
(f) The use of multiple accounts
(g) The use of master agents
(h) VIP accounts
(i) Mixed gambling chains
(j) The use of alternative methods of payments
(k) The deposit of funds through financial intermediaries
(l) The use of prepaid (stored value cards)
(m) Unregulated operators

3.15 MONEYVAL has identified that vulnerabilities increase with unregulated operators. Whilst vulnerabilities can be mitigated via effective and robust regulatory frameworks, the AGCC considers it important that operators are aware of these vulnerabilities in order to mitigate them effectively through their business and customer risk assessments and internal controls, policies and procedures.

3.16 The AGCC undertakes its own assessments of risk in eGambling. These reviews take into account information from a number of sources including the AGCC's knowledge and understanding of current issues, published research on the subject, operator experiences, SAR data, MLA data and the NRA.

3.17 The Commission identifie the most significant risks of ML and TF in the eGambling sector in the risk reviews it prepares. These are placed on the AML/CFT area of the Commission's website and in addition the Commission will issue an Instruction drawing the attention of operators to the findings of the Risk Review.

3.18 Other areas of risk include unknown customers or player information mismatches and insufficient CDD tools.

Identification and Mitigation of Risks

3.19 Risk can be seen as a function of three factors and a risk assessment involves making judgements about all three of the following elements:

(a) threat – a person or group of persons, an object or an activity with the potential to cause harm;
(b) vulnerability – an opportunity that can be exploited by the threat or that may support or facilitate its activities; and
(c) consequence – the impact or harm that ML and FT may cause.

3.20 Having identified where it is vulnerable and the threats that it faces, the operator should take appropriate steps to mitigate the opportunity for those risks to materialise. This will involve determining the necessary controls or procedures that need to be in place in order to reduce the risks identified. The documented risk assessments that are required to be undertaken by Schedule 4 will assist the operator in developing its risk-based approach.

3.21 In accordance with Paragraph 3(8) of Schedule 4, the operator shall have regard to:

(a) any relevant notice, instruction or guidance issued by the AGCC, and
(b) the NRA, in determining what constitutes high or low risk, what its risk appetite is, and what constitutes appropriate measures to manage and mitigate risks.

3.22 In addition to those noted above, information on ML and FT risk factors could come from a variety of other sources, whether these are accessed individually or through commercially available tools or databases that pool information from several sources. The sources could include:

(a) national and supranational risk assessments, such as those published by the EU, the UK and other countries or territories similar to the Bailiwick;
(b) information published by law enforcement agencies (for example, the FIS) such as threat reports, alerts and typologies;
(c) information published by the AGCC, such as thematic reports;
(d) information on the purpose and rationale of UK, UN and EU sanctions regimes;

(e) Guidance on ML, FT and preventing the proliferation of weapons of mass destruction published by the States of Guernsey Policy and Resources Committee;

(f) information from international standard-setting bodies, including the FATF, such as guidance papers and reports on specific threats or risks, as well as mutual evaluation reports when considering the risks associated with a particular country or geographic area;

(g) information provided by industry bodies, such as typologies and emerging risks;

(h) information published by non-governmental organisations (for example, Global Witness or Transparency International); and

(i) information published by credible and reliable commercial sources, (for example, risk and intelligence reports) or open sources (for example, reputable newspapers).

3.23 Retaining documentation on the results of the operator's risk assessment framework will assist the operator to demonstrate how it:

(a) identifies and assesses the risks of being used for ML and FT;

(b) agrees and implements appropriate and effective policies, procedures and controls to manage and mitigate ML and FT risk;

(c) monitors and improves the effectiveness of its policies, procedures and controls; and

(d) ensures accountability of the board in respect of the operation of its policies, procedures and controls.

Accumulation of risk

3.24 In addition to the individual consideration of each risk factor, the operator must also consider all such factors holistically to establish whether their concurrent or cumulative effect might increase or decrease the operator's overall risk exposure and the dynamic that this could have on the controls implemented by the operator to mitigate risk.

3.25 Such an approach is relevant not only to the operator in its consideration of the risks posed to its business as a whole as part of undertaking its business risk assessments, but also in the consideration of the risk that individual business relationships pose.

3.26 There are also other operational factors which may increase the overall level of risk. These factors should be considered in conjunction with the operator's ML and FT risks. Examples of such factors could be the outsourcing of AML and CFT controls or other regulatory requirements to an external third party or another member of the same group as the operator or the use of on-line or web-based services and cyber-crime risks which may be associated with those service offerings.

Weighing Risk Factors

3.27 In considering the risk of a business relationship holistically, the operator may decide to weigh risk factors differently depending on their relative importance.

3.28 When weighing risk factors, the operator should make an informed judgement about the relevance of different risk factors in the context of a business. This will likely result in the operator allocating varying 'scores' to different factors; for example, the operator may decide that a customer's personal links to a country, territory or geographic area associated with higher ML and/or FT risk is less relevant in light of the features of the product they seek.

3.29 Ultimately, the weight given to each risk factor is likely to vary from product to product and customer to customer (or category of customer). When weighing risk factors, the operator should consider that:

(a) the risk rating is not unduly influenced by just one risk factor;
(b) economic or profit considerations do not influence the risk rating;
(c) the weight assigned does not lead to a situation where it is impossible for any business relationship to be classified as a high risk relationship;
(d) the provisions of Paragraph 4(1) of Schedule 4 setting out the situations which will always present a high risk (for example, the involvement of foreign PEPs) cannot be over-ruled; and

(e) it is able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

3.30 Where the operator uses automated IT systems to allocate overall risk scores to business relationships and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. The operator should be able to satisfy itself that the scores allocated reflect the operator's understanding of ML and FT risk and it should be able to demonstrate this.

Policies, Procedures and Controls

3.31 In accordance with Paragraph 2(7) of Schedule 4, the operator shall –

(a) have in place policies, procedures and controls approved by its board that are appropriate and effective, having regard to the assessed risk, to enable it to mitigate and manage:
  (i) risks identified in the business risk assessments, and relationship risk assessments undertaken under Paragraph 2(5)(a) of Schedule 4; and
  (ii) risks relevant, or potentially relevant, to the operator identified in the NRA (which risks shall be incorporated into the business risk assessments);
(b) regularly review and monitor the implementation of those policies, controls and procedures and enhance them if such enhancement is necessary or desirable for the mitigation and management of those risks; and
(c) take additional measures to manage and mitigate higher risks identified in the business risk assessments and in relationship risk assessments undertaken under Paragraph 2(5)(a) of Schedule 4.

3.32 The operator's policies, procedures and controls must take into account the nature and complexity of the operator's operation, together with the risks identified in its business risk assessments, and must be sufficiently detailed to allow the operator to demonstrate how the conclusion of each relationship risk assessment has been reached.

Deviation from the Risk Based Approach

3.33 For the avoidance of doubt it should be noted that screening for the subjects of TFS and PF sanctions must be conducted within 24 hours of the person or entity being sanctioned. The risk based approach does NOT apply to such screening and operators should note that the 24 hour period for screening to take place commences at the time the person or entity is sanctioned and not from the receipt of any notice or alert that may be issued via THEMIS. Operators must ensure that their BRA takes into account the risks of such screening not taking place within the required 24 hour time period.

Chapter 4

Business Risk Assessments

Introduction

4.1 A key component of a risk-based approach involves the operator identifying areas where its products and services could be exposed to the risks of ML and FT and taking appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls.

4.2 The business risk assessments are designed to assist the operator in making such an assessment and provide a method by which the operator can identify the extent to which its business and its products and services are exposed to ML and FT. Good quality business risk assessments are therefore vital for ensuring that the operator's policies, procedures and controls are proportionate and targeted appropriately. In addition the business risk assessment must consider the risks of the operator failing to comply with the requirement to identify the subject of TFS or PF sanctions within 24 hours of their being made the subject of TFS or PF sanction.

4.3 The board must ensure that the operator's business risk assessments, together with details of the operator's risk appetite, are communicated to all relevant employees.

4.4 In communicating the operator's business risk assessments and risk appetite, the operator should ensure that relevant employees understand the implications of these on the day-to-day functions of relevant employees and their effect on the strategic objectives of the operator, in particular those relevant employees with customer-facing or business development roles.

Content and Structure

4.5 In accordance with Paragraph 2(1)(a) of Schedule 4, the operator shall carry out and document a suitable and sufficient ML business risk assessment and a suitable and sufficient FT business risk assessment, which are specific to the operator. The operator shall also assess

the risk of failing to identify the subject of TFS or PF sanctions within 24 hours of their being made the subject of a sanction.

4.6 In carrying out the business risk assessments in accordance with Paragraph 2(1) of Schedule 4, the operator must ensure that the assessments of the risks of ML and FT are distinct from one another, clearly addressing the different threats posed by each risk and should reflect that appropriate steps have been taken in order to identify and assess the specific risks posed to the operator.

4.7 The format of the business risk assessments is a matter to be decided by the operator. However, regardless of the format used, it is important that the business risk assessments are documented in accordance with Paragraph 2(1)(a) of Schedule 4 prior to the application for an ICS being submitted in order to provide clear evidence to demonstrate the basis upon which they have been conducted. Notwithstanding the requirement for the ML and FT business risk assessments to be distinct, there is nothing to prevent them being contained within one over-arching document recording, in its entirety, the operator's assessment of ML and FT risk.

4.8 In accordance with Paragraph 2(4) of Schedule 4, the business risk assessments shall be appropriate to the nature, size and complexity of the operator, and be in respect of:

(a) customers, and the beneficial owners of customers,
(b) countries and geographic areas, and
(c) products, services, transactions and delivery channels (as appropriate), and in particular in respect of the ML or FT risks that may arise in relation to:
    (i) the development of new products and new business practices, before such products are made available and such practices adopted; and
    (ii) the use of new or developing technologies for both new and pre-existing products, before such technologies are used and adopted.
(d) banking methods and payment methods.
(e) employee risks encompassing risks of inadequate training as well as criminal infiltration.

In addition the operator must consider the risks to their business of failing to identify the subject of TFS or PF sanctions within 24 hours of their being placed on the sanctions list.

4.9 The business risk assessments must also take account of the findings of the NRA and reflect the operator's assessment of whether the risks identified in the NRA are relevant, or potentially relevant, to the operator, and where they are, identify the measures for mitigating those risks.

4.10 The operator should have regard to the ML and FT threats relevant to its business as articulated in the NRA, assess how those threats are relevant to the products and services it offers, and assess its vulnerability to ML and FT after taking into account mitigating measures. The sections of the NRA which discuss the modalities of ML and FT, and the case studies contained within, are particularly relevant. Despite there being no FT case studies in the NRA, some of the countries and patterns of behaviour involved in the ML case studies will be relevant to possible FT activity, especially in relation to secondary FT i.e. where the proceeds of crime are used to fund terrorism. Additionally the operator should have regard to FT typologies issued by the FATF.

FATF FT Guidance

4.11 In accordance with Paragraph 2(2) of Schedule 4, in carrying out its business risk assessments, the operator shall consider all relevant risk factors before determining:

(a) the level of overall risk to the operator;
(b) the appropriate level and type of mitigation to be applied.

4.12 The business risk assessments should contain references as to how the operator manages or mitigates the risks which it has identified and the policies, procedures and controls which have been established in this regard.

4.13 Industry sectors will have inherent and/or generic risk factors and these should be referenced in the operator's business risk assessments. Business risk assessments are likely to be deficient if the risks to the operator's sector identified in the NRA are not considered or if the irrelevance of those risks to its business is not explained in the assessments. Additionally, the operator will also have risk factors particular to its own business which should be analysed in the business risk assessments.

4.14 The operator must not copy the business risk assessments prepared by another business, or use 'off the-shelf' assessments which pre-identify suggested ML and FT risks without the operator ensuring the assessments have been tailored to its business and the specific risks that it faces.

4.15 Such an approach in adopting an 'off-the-shelf' assessment can lead to the operator failing to accurately identify the ML and FT risks specific to its business. This in turn can lead to inadequate or inappropriate policies, procedures and controls that are either ill-suited to the operator or fail to appropriately mitigate the operator's risks.

4.16 In addition to the above, the business risk assessments should not:

(a) be a 'cut and paste' version of the relevant sections of any guidance and/or the NRA. This does not demonstrate that the board has given serious consideration to the vulnerabilities specific to the products, services and customers of the operator;
(b) be generic assessments which have simply been populated with general information. Again, this does not demonstrate that the board has given serious consideration to the vulnerabilities particular to its business;
(c) contain unsubstantiated, highly generalised references to the risks faced by the operator, for example, a reference to all business being low risk or statements such as 'there is a risk that our products could be used to finance terrorism'. Such statements would not be acceptable unless they are backed-up with specific information evidencing how this assessment had been made;
(d) copy statements about a sector's risks from the NRA without substantiating why those risks are relevant (or not relevant) to the operator; or
(e) focus upon isolated risk factors, for example, concentrating solely upon a geographic location or product.

4.17 There may be occasions where threats span a number of risk categories, for example, there may be operational risks associated with a piece of customer-facing technology in addition to ML and FT or other financial crime risks. Where the operator wishes to combine its ML and FT business risk assessments with assessments of other risks, such as conduct risk

or credit risk, the operator should ensure that the assessments of ML and FT risk are clearly identified.

Review

4.18 In accordance with Paragraph 2(1)(b) of Schedule 4, the operator shall regularly review its business risk assessments, when changes to the business of the operator occur, so as to keep them up to date and seek approval for any corresponding changes to its approved ICS in accordance with regulations 191 and 192.

4.19 The NRA process is an iterative one, which will involve the exercise being repeated over time. Therefore, the operator must take into account the findings of any updated NRA and reflect the operator's assessment of whether the risks identified in any updated NRA are relevant, or potentially relevant, to the operator, and where they are, identify the measures for mitigating those risks. This must form part of the next review of the operator's business risk assessment, unless the AGCC calls upon operators to do this sooner in accordance with Regulation 189.

4.20 Just as the activities of the operator can change, so too can the corresponding ML and FT risks. Mergers, acquisitions, the purchase or sale of a book of business, the adoption of a piece of technology or technological solution, the introduction of a new product or service, a restructuring, a change of external service provider or changes to eGambling regimes in other jurisdictions are just some of the events which can affect both the type and extent of the risks to which the operator could be exposed. In light of any such changes the business risk assessments should be reviewed to consider whether the risks to the operator have changed and to ensure that the controls to mitigate those risks remain effective.

4.21 Other operational changes, for example, a change in employee numbers or a change to group policies, can all have an impact upon the resources required to effectively manage ML and FT risks.

4.22 Where, as a result of the operator's review, changes to the business risk assessments are required, in accordance with Paragraph 2(1)(b) of Schedule 4, the operator shall make those changes and seek approval to make any corresponding changes to its approved ICS in accordance with regulations 191 and 192.

4.23 Where changes to the business risk assessments are made, the operator must give consideration to whether the policies, procedures and controls of the operator remain appropriate and effective in light of the revised business risk assessments and make any changes it considers appropriate in a timely manner.

Example risk factors

4.24 Below are example risk factors that may be considered by the operator as part of the assessment of its ML and FT risks. The examples given are not intended to be exhaustive or to be used by the operator as checklists of risks.

4.25 Customer risk:

(a) The countries, territories and geographic areas with which customers (and the beneficial owners of customers) have a relevant connection;
(b) The complexity of customer and beneficial ownership structures;
(c) The complexity of legal persons and legal arrangements;
(d) The number of business relationships assessed as high risk;
(e) The countries and geographic areas targeted by the operator and from which the operator will accept new customers (including the beneficial owners of customers);
(f) The number of customers and beneficial owners assessed as PEPs and their associated countries or territories; and
(g) The customer being made the subject of a TFS or PF sanction.

4.26 Product/service risk:

(a) The nature, scale, diversity and complexity of the products and services of the operator;

(b) The target markets, both in terms of geography and class of customer;

(c) The distribution channels utilised by the operator;

(d) Whether the value of transactions is expected to be particularly high;

(e) The nature, scale and countries/geographic areas associated with funds sent and received on behalf of customers including player to player transfers where offered*;*

(f) Whether payments to any unknown or un-associated third parties are allowed;

(g) Whether the products/services/structure are of particular, or unusual, complexity; and

(h) The ability of customers to select tables or counterparty.

4.27 Other potential sources of risk to consider:

(a) Internal and/or external audit findings; and

(b) Typologies and findings of ML and FT case studies.

4.28 New Products and Business Practices

4.29 In accordance with Paragraph 2(4)(c)(i) of Schedule 4, the operator shall, before making available or adopting new products or business practices, ensure that its business risk assessments have identified and assessed the ML and FT risks arising from those products or practices.

4.30 References to new products should be read as referring to products or services which the operator has not previously offered and which present new or differing ML or FT risks to the operator. This will include new games but not necessarily cloned games.

4.31 References to new business practices relate to new ways in which the operator's products or services are offered or delivered. For example, a new business practice could include the development of a customer-facing portal or other software where customers can interact with the operator.

4.32 If the operator decides to proceed with the offering or adoption of a new product or business practice, the board of the operator must approve the risk assessment undertaken in

accordance with Paragraph 2(4)(c)(i) of Schedule 4 and that approval must be documented and an application made in accordance with regulation 191 or 192 for a change to the approved ICS.

4.33 New Technologies

4.34 In accordance with Paragraph 2(4)(c)(ii) of Schedule 4, the operator shall, before adopting and using a new or developing technology for a new or pre-existing product, ensure that its business risk assessments have identified and assessed the risks arising from the technology's use or adoption.

4.35 It may be that these technologies are likely to fall within the Financial Technology ("FinTech") arena, which includes technology aimed at disrupting the delivery or transaction channels of traditional products and services, as well as the creation of new products or services utilising enhancements in technology.

4.36 The risk assessment of a new or developing technology must include, as a minimum, an assessment of the ML and FT risks and vulnerabilities inherent in the use or adoption of the technology in order that appropriate controls can be implemented. This includes evaluating the technology itself, together with the anticipated use of the technology and the threats posed by this use.

4.37 It is not essential that the risk assessment of a technology extends to a highly technical, comprehensive report on the specifications and functionality. The objective of the risk assessment is to evaluate the ML and FT risks and vulnerabilities inherent in the use of the technology and to identify the controls necessary to mitigate and limit the operator's exposure. In the event that the adoption of such a change represents a change to gambling equipment, approval shall be sought pursuant to regulation 209.

4.38 If the operator decides to proceed with the adoption or use of a new or developing technology for a new or pre-existing product, the board of the operator must approve the risk assessment undertaken in accordance with Paragraph 2(4)(c)(ii) of Schedule 4 and that

approval must be documented and an application made in accordance with regulation 191 or 192 for a change to the approved ICS.

4.39 Following the initial risk assessment of a new or developing technology, the operator should periodically review its assessment in conjunction with its responsibility for the review of its wider ML and FT business risk assessments as described in chapter 4 of this guidance.

Relationship Risk Assessment

4.40 The purpose of this Section is to set out the AGCC guidance surrounding the assessment of risk in a business relationship, i.e. customer relationship ("relationship risk assessment") at the point of take-on, as well as the ongoing requirement to ensure that any relationship risk assessment remains appropriate and relevant as the relationship evolves.

4.41 The operator's business risk assessments will assist in determining the take-on of any new business. The relationship risk assessment is the assessment of a new or existing business relationship against the parameters determined and the ML and FT risks identified in the business risk assessments.

4.42 There may be circumstances where the risks of ML and FT are high and ECDD measures are to be applied. Further information on the relationship risk assessment process, including examples of higher risk factors, can be found in this Section.

Management and Mitigation

4.43 In order to consider the extent of its potential exposure to the risks of ML and FT, in accordance with Paragraph 2(5) of Schedule 4 the operator shall –

(a) prior to the establishment of a business relationship undertake a risk assessment of that proposed business relationship, and

(b) regularly review any risk assessment carried out under (a) so as to keep it up to date and, where changes to that risk assessment are required, it shall make those changes.

4.44 Based on the outcome of its risk assessment, the operator must decide whether or not to accept (or continue) each business relationship.

4.45 When undertaking or reviewing a risk assessment, in accordance with Paragraph 2(6)(a) of Schedule 4 the operator shall take into account risk factors relating to:

(i) the type or types of customer (and the beneficial owners of the customer);
(ii) the country or geographic area; and
(iii) the product, service, transaction and delivery channel that are relevant to the business relationship.

4.46 The FATF publishes two lists identifying jurisdictions with weak measures to combat ML and FT. The first list is of "High risk jurisdictions subject to a call for action" which identifies a number of countries and territories with significant strategic deficiencies in their regimes to counter ML, FT and financing of proliferation. Business from Sensitive Sources Notices (BSSN's) issued by the AGCC identifies those countries and territories which the FATF has listed as high risk and has called on jurisdictions to apply enhanced due diligence. In the most serious cases, it will also call upon jurisdictions to apply counter-measures to protect the international financial system from the ongoing ML, FT and proliferation financing risks emanating from that country.

4.47 The second list issued by the FATF is a statement of those "jurisdictions under increased monitoring". These jurisdictions are actively working with the FATF to address strategic deficiencies in their AML/CFT regimes. The FATF does not call for the application of enhanced due diligence to be applied to these jurisdictions, but encourages members to take into account the information it publishes about these jurisdictions in their risk analysis. These jurisdictions will be communicated to operators by way of BSSNs which lists these countries. The BSSNs also list countries and territories that are identified by the UK, US governments, intergovernmental and supranational organisations as presenting certain ML and FT risks. Alongside these sources, information is presented reflecting assessments of a country or territory by non-governmental organisations which operators may also find useful when they are determining the level of country risk presented by a business relationship. The inclusion of a country or territory in a BSSN does not automatically imply that a business relationship with a relevant connection to a country or territory on the BSSN is high risk.

4.48 For the purposes of Paragraph 2(6)(a) of Schedule 4, when considering country or geographical area risk factors, the operator should:

(a) take into account risk variables relating to the type or types of customer, country or geographic area, and product, service, transaction or delivery channel that are relevant to the business relationship in question, and
(b) understand that such risk variables, and any other risk variables, either singly or in combination, may increase or decrease the potential risk posed by the business relationship.

4.49 In addition to the risk factors set out above, the operator must also give consideration to the following when undertaking or reviewing a risk assessment:

(a) the purpose and intended nature of the business relationship including the possibility of legal persons and legal arrangements forming part of the relationship;
(b) the type, volume, value and regularity of activity expected; and
(c) the expected duration of the business relationship.

4.50 For the purposes of Paragraph 2(6)(a) of Schedule 4 and the guidance above, the operator's consideration of the type or types of customer, beneficial owner or beneficiary should incorporate whether they are a natural person, legal person or legal arrangement, as well as their identity and background.

4.51 In accordance with Paragraph 2(6)(b) of Schedule 4, when undertaking or reviewing a relationship risk assessment, the operator shall understand that the risk factors noted in Paragraph 2(6)(a) of Schedule 4 as set out above and any other risk factors, either singly or in combination, may increase or decrease the potential risk posed by the business relationship.

4.52 In light of the above, when undertaking a risk assessment the operator must ensure that all relevant risk factors are considered, both singly and in combination, before making a determination as to the level of overall assessed risk.

4.53 Consideration of the purpose and intended nature of a business relationship in accordance with this guidance should include an assessment of the economic or other commercial rationale for the business relationship.

4.54 The operator's procedures may provide for standardised profiles to be used for risk assessments where the operator has satisfied itself, on reasonable grounds, that such an approach effectively manages the risk for each particular business relationship. However, where the operator has a diverse customer base, or where a wide range of products and services are offered, it must develop a more structured and rigorous system to show that judgement has been exercised on an individual basis rather than on a generic or categorised basis.

4.55 Whatever method is used to assess the risk of a business relationship the operator must maintain clear documented evidence as to the basis on which the risk assessment has been made.

4.56 Where, despite there being high risk factors identified, the operator does not assess the overall risk as high because of strong and compelling mitigating factors, the operator must identify the mitigating factors and, along with the reasons for the decision, document them and retain them on the relevant business relationship file.

4.57 The results of the risk assessment will assist the operator to determine the extent of CDD to be obtained and how this will be verified as well as the extent of ongoing monitoring that will be required during the business relationship to ensure that those made subject to TFS and PF sanctions are identified within 24 hours of their being made the subject of a sanction.

Notices, Instructions or Warnings

4.58 From time to time the AGCC issues Notices, Instructions or Warnings which highlight potential risks. This information, together with sanctions legislation applicable in the Bailiwick, must be considered when undertaking or reviewing a risk assessment.

4.59 Further information on the Bailiwick's sanctions regime and legislation can be found in Chapter 10 of this guidance.

Mandatory High Risk Factors

4.60 In accordance with Paragraph 4(1) of Schedule 4, where the operator is required to carry out CDD measures, it must also carry out ECDD measures in relation to high risk customer relationships, including, without limitation -

(a) a relationship in which the customer or any beneficial owner or underlying principal is a foreign politically exposed person,

(b) a relationship where the customer is established or situated in a country or territory -

  (i) that provides funding or support for terrorist activities, or does not apply (or insufficiently applies) the FATF Recommendations, or

  (ii) is a country otherwise identified by the FATF Recommendations as a country for which such measures are appropriate,

(c) a relationship which has been assessed as a high risk relationship pursuant to regulation 227(2) or 229, and

(d) a relationship which the Category 1 eGambling licensee or Category 1 associate certificate holder considers to be a high risk relationship, taking into account any notices or warnings issued from time to time by the Commission pursuant to regulation 4(l) and having regard to the NRA.

4.61 Chapter 8 of this guidance sets out the requirements of Schedule 4 in relation to high risk relationships and includes details of sources which may assist in the assessment of risk.

4.62 The operator is required to have regard to the NRA in determining what constitutes a high or standard risk and what constitutes appropriate measures to manage and mitigate risks.

4.63 The sections of the NRA report which discuss the modalities of ML and FT, and the case studies contained within, are particularly relevant to the operator when assessing and mitigating customer, product, service, transaction and delivery channel risk factors.

Risk factors

4.64 The risk factors included within the following sections are purely for guidance and are provided as examples of factors that the operator might consider when undertaking a risk assessment. The following factors are not exhaustive and are not prescribed as a checklist. It is for the operator to assess and decide what is appropriate in the circumstances of the business relationship and it is not expected that all factors will be considered in all cases.

4.65 The example indicators do not remove the ability of the operator to apply a risk-based approach. In this respect the operator should take a holistic view of the risk associated with each business relationship as set out in this chapter. The presence of isolated risk factors does not necessarily move a business relationship into a higher risk category; however certain risk factors could have a bigger contribution to the overall risk assessment than others.

4.66 If it is determined, through a risk assessment, that there are types of customer, activity, or business that are at risk of abuse from ML and/or FT, then the operator should apply higher AML and CFT requirements as dictated by the relevant risk factor(s).

Customer Risk Factors

4.67 When identifying the risk associated with its customers, including the beneficial owners of customers, the operator should consider the risk related to the customer (and/or beneficial owners) occupation, reputation or nature and behaviour.

4.68 Risk factors that should be considered are whether the customer or beneficial owner has links to industries may be perceived as having higher risks of corruption such as construction (including overseas), healthcare, pharmaceuticals, arms and defence contracting, mining and public procurement. Other sectors that have a higher ML or TF risk would include MSPs and dealers in metals, both precious and scrap and whilst cash is not accepted in eGambling, extra care may be appropriate when dealing with those connected to businesses with strong cash associations. PEPs and other high profile individuals may also pose greater risks of ML, TF and PF.

4.69 If the customer is a legal person then the purpose of the relationship should be established and confirmation obtained that the nature of the business includes gambling.

4.70 The following list of risk factors is not exhaustive and is provided to some examples factors which raise the risks of ML and TF:-

(a) Customers who are PEPs of have high profiles, for example those in positions of influence in business or sporting bodies
(b) Customers about whom there are adverse media reports
(c) Customers who have been the subject of increased internal monitoring or scrutiny
(d) Customers whose source of funds and wealth cannot easily be identified

Countries and Territories Risk Factors

4.71 Internationally, it is recognised that ML often involves using the financial systems of a number of jurisdictions. Analysis was undertaken as part of the NRA as to how the Bailiwick typically fits into this pattern. The findings from this analysis were that in the majority of cases the Bailiwick's involvement is distant from or peripheral to the criminal enterprises. This indicates in turn that in most cases involving foreign criminal proceeds, the Bailiwick is likely to be some way removed from the criminality itself and to come a considerable distance down the chain of laundering activity, therefore, the operator should consider country risk in the round, where risks are higher ensuring it fully understands the source of those funds.

4.72 When identifying the risk associated with countries and territories, the operator should consider the risk related to those countries and territories with which the customer or beneficial owner has a relevant connection.

4.73 The operator should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors. For example:

(a) Where the funds used in the business relationship have been generated abroad, the level of predicate offences to ML and the effectiveness of a country's or territory's legal system will be particularly relevant.
(b) Where funds are received from, or returned to, countries or territories where groups committing terrorist offences are known to be operating, the operator should consider to what extent this could be expected to, or might give rise to,

suspicion based on what the operator knows about the purpose and nature of the business relationship.

(c) Where the customer or beneficial owner is a legal person or legal arrangement, the operator should take into account the extent to which the country or territory in which the customer or beneficial owner is registered effectively complies with international tax transparency standards.

4.74 Risk factors the operator should consider when identifying the effectiveness of a country's or territory's AML and CFT regime include:

(a) Has the country or territory been identified by a mutual evaluation as having strategic deficiencies in its AML and CFT regime? In accordance with Paragraph 4(1)(b)(i) of Schedule 4, ECDD measures shall be applied where the customer or beneficial owner has a relevant connection to a country or territory that does not apply (or insufficiently applies) the FATF Recommendations.

(b) Is there information from more than one credible and reliable source about the quality of the country's or territory's AML and CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the FATF or FATF-style regional bodies (in particular Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund ("IMF") assessments and Financial Sector Assessment Programme reports. The operator should note that membership of the FATF or a FATF-style regional body (for example, MONEYVAL) does not, of itself, mean that the country's or territory's AML and CFT regime is adequate and effective.

(c) Information in BSSNs issued by the AGCC which lists a number of countries and territories that are identified by relevant and external sources as presenting a higher risk of ML and FT.

4.75 Risk factors the operator should consider when identifying the level of FT risk associated with a country or territory include:

(a) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities from official sources or from organised groups or organisations within that country or territory?

(b) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that groups committing terrorist offences are known to be operating in the country or territory?

(c) Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU?

(d) Are there communities within the country or territory that may be actively targeted by terrorist organisations for support or cover or who may be sympathetic to terrorist actors because of diaspora links or other connections?

(e) Is the country or territory rich in natural/environmental resources and known to have active terrorist organisations operating within it?

(f) Is the country or territory a regional or international financial centre in close proximity to a conflict zone or to a country or territory identified as funding or supporting terrorist activities which could increase the risk of that finance centre being used as a transit jurisdiction to move funds linked with terrorist activity?

(g) Is FT criminalised or inadequately criminalised in the country or territory? Information on this may be found in its FATF or equivalent mutual evaluation report.

4.76 Risk factors the operator should consider when identifying the risk associated with the level of predicate offences to ML in a country or territory include:

(a) Is there information from credible and reliable public sources about the level of predicate offences to ML in the country or territory, for example, corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UN Office on Drugs and Crime World Drug Report.

(b) Is there information from more than one credible and reliable source about the capacity of the country's or territory's investigative and judicial system to effectively investigate and prosecute these offences?

4.77 When identifying the risk associated with its products, services or transactions, the operator should consider the risk related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords;
(b) the complexity of the product, service or transaction; and
(c) the value or size of the product, service or transaction.

4.78 Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

(a) To what extent is the transaction complex and does it involve multiple parties or multiple countries or territories? Are transactions straightforward?
(b) To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the operator know the third party's identity, for example, is it a state benefit authority or a guarantor? Or are products and services funded exclusively by fund transfers from the customer's own account at a FSB that is subject to AML and CFT standards and oversight that are comparable to those in the Bailiwick?
(c) Does the operator understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

Delivery Channel Risk Factors

4.79 When identifying the risk associated with the way in which the customer obtains the products or services they require, the operator should consider the risk related to the way in which the business relationship is conducted on a non-face-to-face basis; and

4.80 When assessing the risk associated with the way in which the customer obtains the products or services, the operator should consider a number of factors including, as the customer is not physically present for identification purposes, has the operator used a reliable form of identification data? Has it taken steps to prevent impersonation or identity fraud?

Chapter 5

Customer Due Diligence

Introduction

5.1 The application of CDD measures to customer relationships is important for two key reasons:

(a) to help the operator, at the time that CDD measures are applied, to be satisfied that customers (and the beneficial owners of customers) are who they say they are; to know whether the customer is acting on behalf of another; and that there is no legal barrier (for example, government sanctions) to providing them with the product or service requested; and

(b) to enable the operator to assist law enforcement, by providing available information on customers, beneficial owners or activities being investigated.

5.2 This chapter sets out the AGCC requirements and provides guidance in respect of the CDD measures to be applied to customer relationships, including details of the policies, procedures and controls required by the operator in order to meet the relevant requirements of Schedule 4 and this guidance.

Overriding Obligations

5.3 In accordance with Paragraph 3(2) of Schedule 4, the Category 1 operator shall apply CDD measures when:

(a) subject to paragraph 5, before registering a customer in accordance with regulation 227,

(b) immediately after a registered customer, in accordance with regulation 230, makes a deposit –

(i) of €3,000 or more, or

(ii) that results in the total value of his deposits in the course of any period of 24 hours reaching or exceeding €3,000,

(c) when it knows or suspects or has reasonable grounds for knowing or suspecting -

(i) that, notwithstanding any exemptions or thresholds pursuant to Schedule 4, any party to a customer relationship is engaged in money laundering or terrorist financing, or

(ii) that it is carrying out a transaction on behalf of a person, including a beneficial owner or underlying principal, who is engaged in money laundering or terrorist financing, and

(d) when it has doubts about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification of a registered customer.

5.4 In accordance with Paragraph 3(5) of Schedule 4, where the Category 1 operator:

(a) forms a suspicion of ML or FT by a customer or other person, and

(b) reasonably believes that carrying out the steps in subparagraph (2), paragraph 4(2) or paragraph 9 would tip off that customer or person, it shall not carry out those steps, but shall instead make a disclosure pursuant to Part I of the Disclosure Law, or Section 15 or 15A, or Section 12 (as appropriate) of the Terrorism Law.

5.5 In accordance with regulation 228, in relation to all customers the Category 1 operator shall:

(a) not set up or keep anonymous accounts or accounts in fictitious names;

(b) maintain accounts in a manner which facilitates the meeting of the requirements of the regulations and Schedule 4, and the relevant ICS Guidelines and this guidance.

5.6 Sound CDD policies and procedures are a key component of an effective AML and CFT framework and are vital for the operator because they:

(a) constitute an essential part of risk management, providing the basis for identifying, assessing, mitigating and managing risk;
(b) help to protect the operator and the integrity of the Bailiwick by reducing the likelihood of the operator becoming a vehicle for, or a victim of, financial crime and/or FT;
(c) help the operator, at the time CDD is carried out, to take comfort that the customer and other parties included in a customer relationship are who they say they are and that it is appropriate to provide them with the product or service requested; and
(d) help the operator to identify, during the course of a continuing customer relationship, factors which are unusual and which may lead to knowing or suspecting or having reasonable grounds for knowing or suspecting that the parties involved in a customer relationship may be carrying out ML or FT.

5.7 Accordingly, CDD is an on-going and cumulative process, the extent of which is determined by both the risk attributed to, and the particular circumstances of, a customer relationship.

5.8 Paragraph 3(2) of Schedule 4 defines the four categories of party which may be associated with a customer relationship (collectively referred to in the guidance as "key principals") and sets out the extent of the CDD measures that are to be applied to each of them, specifically:

(a) the customer;
(b) any person purporting to act on behalf of the customer;
(c) the beneficial owner of the customer; and
(d) any person on behalf of whom the customer is acting.

The Customer

5.9 In accordance with Paragraph 3(2)(a) of Schedule 4, the customer shall be identified and the identity of the customer verified using identification data.

A Person Purporting to Act on Behalf of the Customer

5.10 In accordance with Paragraph 3(2)(b) of Schedule 4, any person purporting to act on behalf of the customer shall be identified and that person's identity and authority to so act shall be verified.

5.11 Examples of such persons will include the authorised signatories (or equivalent) acting for or on behalf of a legal person or legal arrangement, those to whom powers of attorney have been granted, the directors (or equivalent) who are acting on behalf of a legal person, and any other person acting on behalf of the customer within the relationship or.

5.12 In taking measures to verify the identity of any person purporting to act on behalf of the customer, the operator should take into account the risk posed by the business relationship, the materiality of the authority delegated to the individual and the likelihood of that person giving the operator instructions concerning the use or transfer of funds or assets.

5.13 Examples of the measures the operator could take to verify the authority of a person to act could include obtaining a copy of the authorised signatories list, power of attorney or other authority or mandate providing the person with the authority to act on behalf of the customer.

The Beneficial Owner of the Customer

5.14 In accordance with Paragraph 3(2)(c) of Schedule 4, the beneficial owner shall be identified and reasonable measures shall be taken to verify such identity using identification data and such measures shall include, in the case of a customer which is a legal person or legal arrangement, measures to understand the nature of the customer's business and its ownership and control.

5.15 Paragraph 15 of Schedule 4 sets out the definition of beneficial owner. It should be noted that the definition varies based upon the type of legal person or legal arrangement involved in a business relationship.

5.16 For the purposes of Paragraph 3(2)(c) of Schedule 4, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the ML and FT risks which have been identified within the business relationship, to understand the nature of the business and the ownership and control structure of the customer and to verify that the beneficial owner of the customer is who he or she is claimed to be.

5.17 Where the business relationship is a high risk relationship, the measures to understand the ownership and control structure of the customer will be greater than for standard risk relationships and may require the operator to ask more questions of the customer and require additional information about the customer's beneficial ownership. Similarly the extent of the measures considered to be reasonable to verify the identity of the beneficial owner will be greater for high risk relationships and may require the operator to undertake more rigorous checks on the beneficial owner or obtain more robust forms of identification data to satisfy the operator that it has accurately verified the beneficial owner's identity.

A Person on Behalf of Whom the Customer is Acting

5.18 In accordance with Paragraph 3(2)(d) of Schedule 4, a determination shall be made as to whether the customer is acting on behalf of another person and, if the customer is so acting, reasonable measures shall be taken to identify that other person and to obtain sufficient identification data to verify the identity of that other person.

5.19 For the purposes of Paragraph 3(2)(d) of Schedule 4, 'reasonable measures' should be read as referring to the taking of measures, which are commensurate with the ML and FT risks which have been identified within the business relationship, to establish the identity of any natural person on whose behalf the operator has determined the customer is acting. Where the risk of the business relationship is high, the extent of the measures considered to be reasonable will naturally be greater than those applied to standard risk relationships.

Policies, Procedures and Controls

5.20 The operator must have take-on policies, procedures and controls in place which explain how to identify, and verify the identity of, the customer, beneficial owner and other key principals identified by Paragraph 3(2) of Schedule 4 to a level appropriate to the characteristics and assessed risk of the business relationship.

5.21 The operator must assess, on the basis of risk, how much identification information to request, what to verify, and how to verify it, in order to be satisfied as to the identity of a customer, beneficial owner or other key principal.

5.22 The operator's policies, procedures and controls in respect of its CDD measures should:

(a) be risk-based to differentiate between what is expected in standard risk relationships and in high risk relationships;
(b) provide for enhanced measures to be applied in the circumstances where such measures are required in accordance with Paragraph 4(2) of Schedule 4;
(c) impose the least necessary burden on customers, beneficial owners and other key principals consistent with meeting the requirements of Schedule 4 and the AGCC's guidance;

5.23 Identification data providing evidence to verify identity and address can come from a range of sources, including physical or digital documents, databases and electronic data sources. These sources may differ in their integrity, suitability, reliability and independence, for example, some identification data is issued by governments after due diligence has been undertaken on an individual's identity, i.e. national identity cards and passports, while other identification data may be issued with few or no checks undertaken on the subject. Accordingly the suitability of new sources of identification data should be considered and an assessment made of its susceptibility to forgery.

5.24 In the event that the operator is unfamiliar with the source of identification data consideration should be given to:-

(a) evidencing the steps taken to understand the document or identification data

(b) record and retain the basis of the understanding

(c) retain any translations made

(d) where the data is accepted and contains the individuals signature, ensure that the signature and/or photograph are clearly legible on copy of scan

(e) assess and record the susceptibility of this identification data to manipulation.

Timing

5.25 In accordance with Paragraph 5 of Schedule 4 there may be occasions when the circumstances are such that the verification of the identity of a customer or beneficial owner, cannot commence or be completed until such time as a business relationship has been established. This may be acceptable in certain circumstances, provided the operator is satisfied as to the reasons causing the delay.

5.26 In this respect, Paragraph 5(c) of Schedule 4 provides that the verification of the identity of a customer and any of the beneficial owners may be completed following the establishment of a business relationship provided that to do so would be consistent with the risk assessment of the business relationship conducted pursuant to Paragraph 2(2) of Schedule 4, and:

(a) the verification is completed as soon as reasonably practicable thereafter;

(b) the need to do so is essential not to interrupt the normal conduct of business; and

(c) appropriate and effective policies, procedures and controls are in place which operate so as to manage risk, including, without limitation, a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed or the monitoring of large or complex transactions being carried outside the expected norms for that business relationship.

5.27 Where the verification of the identity of a customer or beneficial owner takes place after the establishment of a business relationship, the operator must have appropriate and effective policies, procedures and controls in place so as to manage the risk arising from the delay. These policies, procedures and controls must include:

(a) establishing that it is not a high risk relationship;

(b) monitoring by senior management of the business relationship to ensure verification of identity is completed as soon as reasonably practicable;

Failure to Complete Customer Due Diligence

5.28 In accordance with Paragraph 6 of Schedule 4, where the operator cannot comply with any of Paragraph 4) or Paragraph 9(1)(a) to (c) of Schedule 4 it shall:

(a) in the case of a person wishing to become a registered customer, not register that person as a customer,
(b) in the case of an existing registered customer, terminate that customer relationship, and
(c) consider whether making a disclosure is required pursuant to Part I of the Disclosure Law or section 15 or 15A, or section 12 (as appropriate) of the Terrorism Law.

5.29 The operator should be mindful that the termination of a customer relationship does not amount to tipping off.

5.30 Where termination of a business relationship cannot be completed (for example, because the operator has lost contact with the customer) the operator should have procedures and controls in place to ensure that funds held are 'blocked' or placed on a 'suspense' account until such time as contact with the customer is re-established or the operator has otherwise dealt with the funds in accordance with its policy for dormant accounts.

5.31 Where the immediate termination of a business relationship is not possible for whatever reason, the operator must ensure that the risk is managed and mitigated effectively until such time as the business relationship can be terminated.

5.32 The operator must ensure that where funds have already been received, they are returned to the source from which they originated. Where the operator has been unable to return the funds to the account from which they were received, for instance because the originating bank account has been closed, the operator must take appropriate steps to return the funds to the same party in another form.

5.33 Where the operator has terminated, or not proceeded with establishing, a business relationship, it must consider the circumstances giving rise to the failure to complete CDD measures and whether these warrant a disclosure to the FIS.

Chapter 6

Natural Persons

Introduction

6.1 The purpose of this chapter is to set out the information to be obtained, as a minimum, for a natural person who acts as a key principal in one or more of the following capacities within a business relationship:

(a) the customer;
(b) the beneficial owner of the customer;
(c) a natural person purporting to act on behalf of the customer; or
(d) a natural person on behalf of whom the customer is acting.

6.2 Establishing that a natural person falling within Paragraph 3(2) of Schedule 4 as set out above is the person that they claim to be is a combination of being satisfied that:

(a) the person exists, based on the accumulation of information about the person's identity; and
(b) the customer, beneficial owner or other key principal is that person, by verifying from identification data, satisfactory confirmatory evidence of that person's identity.

6.3 This chapter sets out the aspects of a natural person's identity which must be established, together with the characteristics of that natural person's identity to be verified using identification data, in order to comply with the requirements of Schedule 4.

6.4 The requirements of this chapter apply:

(a) when establishing a business relationship; and
(b) where any of the parties set out above to a customer relationship change throughout the life of that relationship.

Identifying natural persons

6.5 Where the operator is required to identify a natural person falling within the above provisions, it must collect relevant information on the identity of that natural person which includes legal name, date of birth and residential address. In addition, as a result of the customer risk assessment, the operator may wish to obtain place of birth and nationality.

6.6 Furthermore obtaining employment information will facilitate the determinations necessary with regards to PEPs.

6.7 In accordance with Paragraph 3(2)(f) of Schedule 4, as part its CDD measures the operator shall make a determination as to whether the customer or beneficial owner is a PEP and, if so, whether they are a foreign PEP or a domestic PEP.

Verifying the identity of Natural Persons

6.8 Subject to Chapter 5 of this guidance, the operator must verify a natural person's identity using identification data, the extent of which is to be determined based on the conclusion of the customer risk assessment. On the basis of that customer risk assessment the operator must verify:

(a) legal name;
(b) date of birth;
(c) residential address.

6.9 In addition, the operator may also be required to verify the place of birth and nationality of the customer if the customer risk assessment requires it.

6.10 In order to verify the above and other information collected, the following identification data is considered to be the best possible:

(a) current passport, bearing a photograph of the natural person;
(b) current national identity card, bearing a photograph of the natural person;

(c) armed forces identity card, bearing a photograph of the natural person;

(d) driving licence, bearing a photograph of the natural person; or

(e) independent data sources (including electronic sources).

6.11 The examples quoted above are not exclusive. There may be other forms of identification data of an equivalent nature which may be produced as satisfactory evidence of the identity of a natural person.

6.12 Regardless of its form, the operator must be satisfied as to the validity and veracity of the identification data used to verify the identity of a natural person and its evidential value should be based on the assessed risk of the customer relationship. In this respect, the operator should be aware that certain documents may be more susceptible to fraud than others, or have less robust controls in respect of their issue, for example, some jurisdictions may issue driving licences without due diligence being undertaken on the holder.

6.13 When changes occur which result in a modification to a natural person's profile (for example, a change of name or address) the operator should apply a risk-based approach to updating that person's CDD records and consider what, if any, additional identification data is required to verify the change.

6.14 In addition to the measures set out above, where the operator has determined that a customer relationship is high risk, in accordance with Paragraph 4(2) of Schedule 4 the operator shall also apply ECDD measures to that relationship. Those ECDD measures shall include, inter alia, taking one or more steps as would be appropriate to the particular customer relationship and could include, in accordance with Paragraph 4(2)(e)(ii) of Schedule 4, verifying additional aspects of the customer's identity.

6.15 Examples of additional aspects of the customer's identity that the operator could verify, where that customer is a natural person, include their occupation or any former name(s). Further detail in respect of ECDD measures can be found in Chapter 8 of this guidance.

Verification of Residential Address

6.16 The following are examples of suitable methods to verify the residential address of a natural person:

(a) a recent bank/credit card statement or utility bill;
(b) correspondence from an independent source such as a central or local government department or agency
(c) commercial or electronic data sources;
(d) a tenancy agreement;
(e) photocard driving licence

6.17 Where a natural person's principal residential address changes during the course of the customer relationship, operators should consider how to identify such changes and meet the needs of section 3(1)(d) of Schedule 4.

Overseas natural persons

6.18 There may be occasions when a natural person who is not resident in the Bailiwick is unable to provide evidence of their residential address using the means set out above. Examples of such individuals include residents of countries without postal deliveries or street addresses who rely on post office boxes or employer's addresses for the delivery of mail. Operators should consider the impact of this upon their customer risk assessment.

6.19 Notwithstanding the above, it is essential for law enforcement purposes that a record of a natural person's residential address (or details of how that person's place of residence can be reached) is held by the operator. As such, it is not acceptable to simply record details of a post office box number as a natural person's address.

6.20 Where the operator has determined that an individual has a valid reason for being unable to produce more usual documentation to verify their residential address and who would otherwise be excluded from establishing a customer relationship with the operator, the residential address can be verified by other means, provided the operator is satisfied that the

method employed adequately verifies the address of the natural person and any additional risk has been appropriately mitigated.

Online Bank Statements or Utility Bills

6.21 Where the residential address of a natural person is to be verified through the use of a bank/credit card statement or utility bill, the default option is to obtain a form of verification which has been delivered to that natural person by post. However, the receipt of such items via the traditional postal system is being replaced by the use of online billing or the delivery of bank or utility statements via e-mail (an "electronic statement").

6.22 Examples of electronic statements include:

(a) an online statement from a recognised bank, building society, credit card company or recognised lender bearing the name and residential address of the natural person; or

(b) an online bill in relation to rates, council tax or utilities bearing the name and residential address of the natural person.

6.23 Where the operator wishes to accept an electronic statement as verification of a natural person's address, it must be satisfied as to the validity and veracity of the electronic statement presented.

6.24 The operator should recognise that some electronic sources may be more easily tampered with, i.e. the data contained within them subject to amendment, than others. If suspicions are raised in relation to the integrity of any electronic statement obtained, the operator should take whatever practical and proportionate steps are available to establish whether these suspicions are substantiated, and if so, whether the relevant electronic statement should be accepted.

6.25 An example of a step the operator could take where it has concerns over the veracity of a document is to corroborate the content of that document using an independent source, for example, a commercial or electronic data source such as a land registry, electoral roll or similar.

Electronic Verification

6.26 Electronic verification is the use of an electronic method or system to verify, in whole or in part, the identity of a natural person by matching specified personal information against electronically captured physical documentation and/or independent electronic data sources.

6.27 Electronic verification can be used to verify all or any combination of the mandatory data points required. Where an electronic verification system does not fulfil all of these requirements, the operator must use one or more other methods to ensure that a natural person is fully verified in accordance with the requirements of this guidance.

6.28 Electronic verification systems range in scope from the electronic capture of identity information and identification data on a face-to-face basis through to the self-capture of uncertified documentation by a natural person using an interactive application ("App") on a tablet or mobile phone. In the latter example, a photograph (or a series of photographs or a video) of the natural person are obtained through the App, together with photographs of identification data and address verification documents. The photographs are then independently reviewed and corroborated.

6.29 Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and identification data for a natural person, the operator should be mindful of any additional risks posed by placing reliance on an electronic method or system. This should include understanding the method and level of review and corroboration within the system and the potential for the system to be abused.

6.30 Knowledge and understanding of the functionality and capabilities of a system can help provide assurance of its suitability. In particular, there should be certainty of the methods applied to corroborate identification data. The use of more than one confirmatory source to match data enhances the assurance of authenticity.

Independent Data Sources

6.31 Identification data does not have to be in paper form. Independent data sources can provide a wide range of confirmatory material on natural persons and are becoming

increasingly accessible, for example, through improved availability of public information and the emergence of commercially available data sources such as electronic databases and research firms. Sources include:

(a) electoral roll;
(b) telephone directories;
(c) credit reference agency checks;
(d) business information services; and
(e) electronic checks provided by commercial agencies.

6.32 Where the operator is seeking to verify the identity of a natural person using an independent data source, whether by accessing the source directly or by using an independent third party organisation (such as a credit reference agency), an understanding of the depth, breadth and quality of the data is important in order to determine that the method of verification does in fact provide satisfactory evidence of identity.

When relying on independent data sources to verify identity, the operator should ensure that the source, scope and quality of that data is suitable and sufficient and that the process provides for the information to be captured and recorded.

Chapter 7

Legal Persons

Introduction

7.1 The purpose of this section is to set out the information to be obtained, as a minimum, for a legal person or legal arrangement which acts as a key principal in one or more of the following capacities within a customer relationship as set out in Paragraph 3(3) of Schedule 4:

(a) the customer;
(b) the beneficial owner of the customer;
(c) a legal person or legal arrangement purporting to act on behalf of the customer; or
(d) a legal person or legal arrangement on behalf of which the customer is acting.

7.2 The identification and verification requirements in respect of legal persons and legal arrangements are different from those for natural persons. While a legal person or legal arrangement has a legal status which can be verified, each customer relationship involving a legal person or legal arrangement will also contain a number of associated natural persons, for example, as beneficial owners. This section should therefore be read in conjunction with chapters 5 and 8which set out the CDD measures to be applied to natural persons acting for or on behalf of, or otherwise associated with, a customer which is a legal person or legal arrangement.

7.3 Legal person refers to any entity, other than a natural person, which is treated as a person for limited legal purposes, i.e. it can sue and be sued, it can own property and it can enter into contracts in its own right. This can include companies, other bodies, corporate, foundations, anstalts, associations, or other similar entities which are not legal arrangements.

7.4 Legal arrangements do not have separate legal personality and therefore form business or customer relationships through their trustees (or equivalent). With regard to trusts, it is the

trustee of the trust who will enter into a customer relationship on behalf of the trust and should be considered, along with the trust, as the operator's customer.

7.5 It is not anticipated that many operators will register customers who are not natural persons and within the category of non-natural person customers the scope of a trust having capacity to conduct such activity should be verified.

7.6 The operator should be alive to, and take measures to prevent, the misuse of legal persons and legal arrangements for ML and FT. It is imperative that when compiling a customer risk assessment, the operator considers the breadth of ML and FT risks that the differing size, scale, activity and structure of the legal person or legal arrangement could pose. Less transparent and/or more complex structures present higher risks which could require additional information or research to determine an appropriate risk classification.
Based on the outcome of its customer risk assessment, the operator must consider how the customer and any other legal persons or legal arrangements falling within the requirements of Paragraph 3(2)(a)-(f) of Schedule 4 are to be identified and the identification data in respect of those legal persons or legal arrangements which must be obtained to verify that identity, including ECDD measures and/or enhanced measures where necessary.

Transparency of Beneficial Ownership

7.7 It is crucial that the operator has a full picture of its customer, including those natural persons with ownership or control over the customer's affairs. This is important so as to identify, firstly the various legal obligations that fall due within the Bailiwick and beyond and, secondly, whether the legal person or legal arrangement is being abused for criminal purposes. As financial crime legislation, including tax legislation, becomes ever more sophisticated, so too do the ways in which a person may structure his, her or its affairs in order to mask the true beneficial ownership.

7.8 When applying CDD measures in relation to customers that are legal persons or legal arrangements, in accordance with Paragraph 3(2)(c) of Schedule 4, the operator shall identify and take reasonable measures to verify the identity of the beneficial owner of the legal person or legal arrangement as well as the nature of its business.

7.9 The definition of beneficial owner in the context of legal persons is to be distinguished from the concepts of legal ownership and control. On one hand, legal ownership means the natural or legal person(s) who, according to applicable law, own the legal person. On the other hand, control refers to the ability to make relevant decisions within the legal person, for example, by owning a controlling block of shares.

7.10 An essential element of the definition of beneficial owner is that it extends beyond legal ownership and control and focusses on ultimate (actual) ownership and control. In other words, the definition identifies the natural (not legal) persons who actually own and take advantage of the capital or assets of the legal person, as well as those who really exert effective control over it (whether or not they occupy formal positions within that legal person), rather than just the natural or legal persons who are legally (on paper) entitled to do so.

7.11 In the context of a trust, beneficial ownership includes both the natural persons receiving benefit from the trust (for example, a beneficiary, those in a class of beneficiaries or any other person who benefits from the trust) as well as those connected with, or having control over, the trust's affairs, including the settlor(s), trustee(s), protector(s) and enforcer(s).

7.12 Paragraph 3(2)(c) of Schedule 4 also requires that, in the case of a customer relationship within which the customer is a legal person or legal arrangement, the operator shall take measures to understand the nature of the customer's business as well as the ownership and control structure of that customer.

7.13 When identifying, and taking reasonable measures to verify the identity of, the beneficial owner of a legal person or legal arrangement as required by the sections of this chapter, the operator must act in accordance with the identification and verification requirements of Schedule 4 and this guidance for natural persons, legal persons and legal arrangements.

Chapter 8

Enhanced due diligence

Objectives

8.1 This section relates to customer relationships which have been assessed by the operator as presenting a high risk of ML and/or FT taking into account the requirements of Paragraph 4(1) of Schedule 4 and should be read in conjunction with Chapters 3 and 4 of this guidance on the assessment of risk and Chapters 5 to 7 of this guidance which set out the CDD measures to be applied.

8.2 In accordance with Paragraph 4(1) of Schedule 4, where the operator is required to carry out CDD, it shall also carry out ECDD in relation to high risk customer relationships, including, without limitation -

(a) a customer relationship in which the customer or any beneficial owner is a foreign PEP ,

(b) a business relationship where the customer or beneficial owner has a relevant connection with a country or territory that -

  (A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) the FATF Recommendations, or

  (B) is a country otherwise identified by the FATF as a country for which such measures are appropriate (see Chapter 10 of this guidance),

(c) which the operator's assessment is, or it considers to be, a high risk relationship pursuant to regulation 227(2) or 229 or taking into account any notices, instructions or warnings issued from time to time by the AGCC pursuant to regulation 4(l) and having regard to the NRA.

Policies, Procedures and Controls

ECDD Measures (High Risk Relationships)

8.3 The operator must ensure that its policies, procedures and controls require the application of ECDD measures where the operator has determined, taking into account the circumstances set out in Paragraph 4(1) of Schedule 4 and the risk factors provided in Chapter 3 of this guidance, that a business relationship is high risk.

8.4 In accordance with Paragraph 4(2)(a) of Schedule 4, references to ECDD shall mean -

(i) obtaining senior management approval for establishing a customer,

(ii) obtaining senior management approval for, in the case of an existing customer relationship with a foreign PEP, continuing that business relationship,

(iii) taking reasonable measures to establish and understand the source of any funds and of the wealth of –

  (A) the customer, and

  (B) the beneficial owner, where the beneficial owner is a PEP,

(iv) carrying out more frequent and more extensive ongoing monitoring, including increasing the number and timing of controls applied and selecting patterns of activity or transactions that need further examination in accordance with Paragraph 9 of Schedule 4 (see Chapter 9of this guidance), and

(v) taking one or more of the following steps as would be appropriate to the particular customer relationship,

  (A) obtaining additional information about the customer, such as the customer's occupation, the volume of the customer's assets, and publicly available information about the customer,

  (B) verifying additional aspects of the customer’s identity,

  (C) obtaining additional information to understand the purpose and intended nature of each business relationship.

8.5 Examples of steps the operator could take in accordance with Paragraphs 5(2)(e)(i)-(iii) of Schedule 4 could include:

(a) supplementing the operator's understanding of the purpose and intended nature of the customer relationship by obtaining information on the reasons for intended or performed transactions;

(b) obtaining independent evidence by a specialist operator or consultant pertaining to the purpose and objective of the customer relationship and/or evidencing information in relation to the customer and/or the beneficial owner;

(c) where the customer is a legal person, identifying, and verifying the identity of, other directors (or equivalent) of the customer in addition to those senior managing officials identified as beneficial owners.

Source of Funds and Source of Wealth

8.6 In accordance with Paragraph 4(2)(c) of Schedule 4, as part of its ECDD measures the operator shall take reasonable measures to establish and understand the source of any funds and of the wealth of –

(A) the customer, and

(B) the beneficial owner, where the beneficial owner is a PEP.

8.7 The taking of reasonable measures to establish and understand a customer's source of wealth (and that of any beneficial owner who is a PEP), together with measures to establish and understand the source of any funds used in a customer relationship, are important aspects of the due diligence process. These steps serve to assist the operator in satisfying itself that such wealth and funds are not the proceeds of criminal activity and are consistent with the operator's knowledge of the customer and beneficial owner, and the nature of the business relationship.

ECDD Measures

Politically Exposed Persons

Introduction

8.8 Due to their position and influence, PEPs may have the potential to abuse their positions for the purpose of committing ML and related predicate offences, including bribery and corruption, as well as conducting activity related to FT. Where a PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

8.9 PEP status itself does not incriminate individuals or their associates and connected entities. However, it will mean that a customer or beneficial owner who is a foreign PEP is subject to ECDD measures and that a domestic PEP or international organisation PEP may, on the basis of risk, be subject to ECDD measures.

8.10 There is no 'one-size fits all' approach to applying ECDD measures for PEPs. The nature of the measures applied will be commensurate with the type of PEP, the specific risks that are identified and the nature of the PEP's position and ability to influence.

Identification of PEPs

8.11 In accordance with Paragraph 3(2)(f) of Schedule 4, as part of its CDD measures the operator shall make a determination as to whether the customer or beneficial owner is a PEP, and if so, whether they are a foreign PEP, a domestic PEP or an international organisation PEP.

8.12 As referenced above, Paragraph 4(3) of Schedule 4 defines three categories of PEP, referred to as follows for the purpose of this guidance:

(a) "foreign PEP" – a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, in a country or territory other than the Bailiwick;

(b) "domestic PEP" – a natural person who has, or has had at any time, a prominent public function, or who has been elected or appointed to such a function, within the Bailiwick; and

(c) "international organisation PEP" – a natural person who is, or has been at any time, entrusted with a prominent function by an international organisation.

8.13 In accordance with the definition of PEP contained within Paragraph 4(3) of Schedule 4, prominent public function includes, without limitation -

(i) heads of state or heads of government;
(ii) senior politicians and other important officials of political parties;
(iii) senior government officials;
(iv) senior members of the judiciary;
(v) senior military officers; and
(vi) senior executives of state owned body corporates.

8.14 When seeking to establish whether a natural person falls within the definition of a PEP, 'prominent' should be interpreted as relating only to those persons in positions of seniority in the areas covered above. Middle ranking or more junior individuals in the foregoing categories are explicitly excluded from the definition.

8.15 Notwithstanding the above, the term 'prominent' is not defined either in Schedule 4 or this guidance as the precise level of seniority which triggers the requirement to treat an individual as a PEP will depend upon a range of factors, including the role held by the individual, the particular organisational framework of the government or international organisation concerned, and the powers, responsibilities and influence associated with particular public functions.

8.16 In accordance with Paragraph 4(4) of Schedule 4, a person is not a PEP for the purposes of Schedule 4 if that person –

(a) was not a PEP within the meaning of Schedule 16 of the Regulations when those regulations were in force, and

(b) ceased to be entrusted with a prominent public function in respect of the Bailiwick before the coming into force of Schedule 4.

8.17 To assist in the identification of natural persons falling within the definition of domestic PEP, Appendix E to the GFSC Handbook provides a list of those positions in Guernsey, Alderney and Sark deemed to fall within the categories listed above. A person is not a domestic PEP for the purposes of Schedule 4 if they were not a politically exposed person within the meaning of Schedule 16 to the Alderney eGambling Regulations, 2009 when that Schedule was in force, and ceased to be entrusted with a prominent public function in respect of the Bailiwick before the coming into force of Schedule 4. A Category 1 operator may treat a domestic PEP as not being a PEP five years after the person ceased to be entrusted with a public function if the senior management of the operator has documented that the business is satisfied that –

(a) it understands the source of the funds within the business relationship, and
(b) there is no reason to continue to treat the person as a PEP.

8.18 Authorities in other jurisdictions may publish lists, similar to that referred to above, of those natural persons considered to fall within the definition of a PEP within their jurisdiction. These could be helpful for the operator in determining whether to treat an individual as a PEP. However, the operator should be mindful that these classifications will be based upon perceptions of risk applicable within other jurisdictions and that these may not necessarily be appropriate perceptions from the perspective of the operator. Accordingly the operator should make their own determination adopting a risk based approach.

8.19 In determining whether a customer or beneficial owner is a PEP, the operator could consider:

(a) using sources such as the UN, the European Parliament, the UK Foreign and Commonwealth Office and the Group of States Against Corruption to establish, as far as is reasonably possible, whether or not a customer or beneficial owner, is a natural person who is the current or former holder of a prominent public function in a foreign country or territory, or for an international organisation;

(b) using sources such as the States of Guernsey, States of Alderney and Chief Pleas of Sark to establish, as far as is reasonably possible, whether or not a customer or beneficial owner is a natural person who is the current or former holder of a prominent public function within the Bailiwick;

(c) seeking confirmation from a customer or beneficial owner, for example through a question within an application form, as to whether they hold, or have held, a prominent public function either within the Bailiwick or beyond, or for an international organisation; or

(d) using commercially available databases to identify such persons.

8.20 In accordance with Paragraph 4(1)(a) of Schedule 4, where the operator determines that an individual who is the customer or beneficial owner to a customer relationship is a foreign PEP, it shall carry out ECDD in relation to that customer relationship.

8.21 Where the operator identifies that a customer or beneficial owner is a domestic PEP or international organisation PEP, it must gather sufficient information to understand the particular characteristics of the public function that the natural person has been entrusted with and factor this information into the risk assessment conducted in accordance with Paragraph 2(5)(a) of Schedule 4 and this guidance.

8.22 Where, having conducted a risk assessment, the operator concludes that the customer relationship involving a domestic PEP or international organisation PEP is high risk, the operator must apply ECDD measures in accordance with Paragraph 4(3)(a) or 4(3)(b) of Schedule 4 and chapter 8 of this guidance.

8.23 Where the operator concludes that the customer relationship with the domestic PEP or international organisation PEP does not present a high level of risk, it is not necessary to apply ECDD measures, provided that the operator has applied CDD measures in accordance with Paragraph 2 of Schedule 4.

International Organisation PEPs

8.24 In accordance with Paragraph 3(2)(f) of Schedule 4, the definition of a PEP includes a natural person who is, or has been, entrusted with a prominent public function by an

international organisation. This includes members of senior management or individuals who have been entrusted with equivalent functions, for example, directors, councillors and members of the board or equivalent of an international organisation.

8.25 Paragraph 15 of Schedule 4 defines an international organisation as an entity:

(a) which was established by a formal political agreement between its member states that has the status of an international treaty;
(b) the existence of which is recognised by law in its member states; and
(c) which is not treated as a resident institutional unit of the country in which it is located.

8.26 Examples of international organisations covered by Schedule 4 and this Guidance include the UN, the World Bank and the North Atlantic Treaty Organization ("NATO").

8.27 There may be other examples of international organisations, for example, international sporting federations and governing bodies, which do not fall within the Schedule 4 definition, but where the operator considers that ECDD measures should be applied to a customer relationship. There are no prescribed requirements in this regard and any decision taken should be based on the operator's assessment of risk. Operator's should also be cognisant that many such sports federations or governing bodies may place limitations on the ability of their members to gamble.

Immediate Family Members

8.28 In addition to the specific risks posed by PEPs, the operator should be alive to the potential for the abuse of a customer relationship with or by a family member of a PEP. This abuse could be for the purpose of moving the proceeds of crime or facilitating the placement and concealment of such proceeds without specific connection to the PEP themselves.

8.29 In accordance with Paragraph 4(3)(c) of Schedule 4, an immediate family member of a PEP shall include, without limitation:

(a) a spouse;

(b) a partner, being a person who is considered by the law of the country or territory in which the relevant public function is held as being equivalent to a spouse;
(c) a parent;
(d) a child;
(e) a sibling;
(f) a parent-in-law; and
(g) a grandchild.

8.30 The list of immediate family members included within Paragraph 4(3)(c) of Schedule 4 as set out above is without limitation and the operator should take a proportionate, risk-based approach to the treatment of wider family members. This determination will depend on the social, economic and cultural structure of the country of the PEP. It should also be noted that the number of persons who qualify as immediate family members is fluid and may change over time.

8.31 In deciding whether a member of a wider family unit would be considered as an immediate family member of a PEP, the operator should determine the extent of the influence that a particular PEP relationship or association has and assess the level of risk that exists through the particular connection with a PEP.

8.32 This determination will include such relevant factors as the influence that particular types of family members generally have and how broad the circle of close family members and dependents tends to be. In some cultures, the number of family members who are considered to be close or who have influence may be quite small, while in others the circle of family members may be broader and extend to cousins or even clans.

Close Associates

8.33 In accordance with Paragraph 4(3)(d) of Schedule 4, a close associate of a person referred to in Paragraphs 4(3)(a) or (b) shall include, without limitation -

(i) a person who is widely known to maintain a close business relationship with such a person, or

(ii) a person who is in a position to conduct substantial financial transactions on behalf such a person.

8.34 Those persons considered to be close associates could include known partners outside the family unit who would not qualify as immediate family members (for example, girlfriends, boyfriends and extra-marital partners), prominent members of the same political party, civil organisation, labour or employee union as the PEP, and business partners or associates, especially those that share beneficial ownership of a legal person or legal arrangement with the PEP, or who are otherwise connected (for example, through joint membership of a company board where the PEP and/or close associate is a beneficial owner).

8.35 As with an immediate family member, the interpretation of whether an individual should be considered to be a close associate will depend upon the social, economic and cultural context of the relationship.

8.36 Where the operator determines that a natural person who is the customer or beneficial owner to a business relationship is an immediate family member or close associate of a domestic PEP or international organisation PEP, the operator should treat that person in accordance with the requirements set out in Schedule 4 and this guidance for the category of PEP to which they are connected. For example, the child of a domestic PEP should be treated in accordance with the provisions for domestic PEPs.

Former PEPs

8.37 On the basis of the potential for PEPs to abuse their prominent positions for the purpose of committing various financial crimes, the default position on the treatment of PEPs in the FATF Recommendations is that once you are a foreign PEP, or a family member or close associate of such a person, the relationship should always be subject to ECDD measures.

8.38 Notwithstanding the above, there may be situations where a customer relationship involves persons who have held prominent public positions historically but who would otherwise not be considered to be high risk.

8.39 Accordingly, Paragraphs 4(5) and (6) of Schedule 4 provide flexibility in respect of the timeframe within which certain natural persons are to be classified as PEPs. Domestic PEPs may be considered to lose that status five years after they cease to be entrusted with a public function provided the senior management of the operator understands the source of funds within the business relationship and there is no reason to continue to treat that person as a PEP. For international organisation PEPs, the period is seven years from the time that person ceases to be entrusted with a prominent function provided the senior management of the operator understands the source of funds within the business relationship and there is no reason to continue to treat that person as a PEP

8.40 With regards to other PEPs, the period is seven years from the time that person ceases to be entrusted with a public function provided that the senior management of the operator has documents that it is satisfied that it has established and understands the source of the person's wealth, and that of the funds within the business relationship, and there is no reason to continue to treat the person as a PEP.

High Risk Countries and Territories

8.41 In accordance with Paragraph 4(1)(b) of Schedule 4, the operator shall apply ECDD measures to a customer relationship where the customer or beneficial owner is situated in or established in a country or territory that -

(A) provides funding or support for terrorist activities, or does not apply (or insufficiently applies) the FATF Recommendations, or

(B) is a country otherwise identified by the FATF as a country for which such measures are appropriate.

8.42 The operator must have policies, procedures and controls in place which enable it to determine those countries or territories falling within Paragraph 4(1)(b)(i) of Schedule 4.

8.43 The FATF regularly updates its public statement, “High Risk Jurisdictions subject to a Call for Action” for which it calls on all members and urges all jurisdictions to apply enhanced due diligence, and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing ML, FT, and

proliferation financing risks emanating from the country. This list is often externally referred to as the “black list”. For the purposes of applying Paragraph 4(1)(b)(i) of Schedule 4, BSSNs issued by the AGCC identify those countries and territories in relation to which the FATF has listed as high risk.

8.44 As part of its policies, procedures and controls, the operator must:

(a) be aware of concerns about weaknesses in the AML and CFT systems of other countries or territories; and

(b) consider any BSSNs and other Notices, Instructions and Warnings issued from time to time by the AGCC as well as any other guidance published by the AGCC.

Chapter 9

Monitoring transactions and activity

Introduction

9.1 The regular monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing CDD measures. In addition operators are required to ensure that they are able to identify customers who are the subject of TFS and PF sanctions within 24 hours of them being made the subject of a sanction.

9.2 It is vital that the operator understands a customer's background and is aware of changes in the circumstances of the customer and beneficial owner throughout the life-cycle of a business relationship. The operator can usually only determine when it might have reasonable grounds for knowing or suspecting that ML and/or FT is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular business relationship.

9.3 There are two strands to effective ongoing monitoring:

(a) The first relates to the transactions and activity which occur on a day-to-day basis within a business relationship and which need to be monitored to ensure they remain consistent with the operator's understanding of the customer and the product or service it is providing to the customer.

(b) The second relates to the customer themselves and the requirement for the operator to ensure that it continues to have a good understanding of its customers and their beneficial owners. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing screening.

9.4 This chapter deals with the requirement for the operator to monitor business relationships on an ongoing basis, including the application of scrutiny to large and unusual or complex transactions or activity so that ML and FT may be identified and prevented.

Objectives

9.5 A key prerequisite to managing the risk of a business relationship is understanding the customer, and beneficial owner, and where changes to those parties occur. It is also important to maintain a thorough understanding of the business relationship and to appropriately monitor transactions in order to be in a position to detect, and subsequently report, suspicious activity.

9.6 The type of monitoring applied by the operator will depend on a number of factors and should be developed with reference to the operator's business and customer risk assessments. The factors forming part of this consideration will include the size and nature of the operator's business, including the characteristics of its customer-base and the complexity and volume of expected transactions or activity.

9.7 The monitoring of business relationships should involve the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions or activity, to ensure that such transactions and activity are consistent with the operator's knowledge of the customer, their business and risk profile, including where necessary, the source of funds. Particular attention should be paid to high risk relationships (for example, those involving foreign PEPs), high risk countries and territories and high risk transactions.

9.8 An unusual transaction or activity may be in a form that is inconsistent with the expected pattern of activity within a particular business relationship, or with the normal business activities for the type of product or service that is being delivered. For example, unusual patterns of transactions with no apparent or visible economic or lawful purpose.

9.9 The nature of the monitoring in any given case will depend on the business of the operator, the frequency of activity and the types of business. Monitoring may include reference to: specific types of transactions; the relationship profile; a comparison of activities or profiles with that of a similar customer or peer group; or a combination of these approaches.

Obligations

9.10 In accordance with Paragraph 9(1) of Schedule 4, the Category 1 operator shall perform ongoing and effective monitoring of any customer relationship, which shall include –

(a) reviewing identification data and records to ensure they are kept up to date, accurate and relevant, in particular as regards any beneficial owner, or registered customers in respect of whom there is a high risk,

(b) updating identification data and records on a timely basis,

(c) without prejudice to the Category 1 eGambling licensee's or Category 1 associate certificate holder's obligations under regulation 236, scrutinising any transactions or other activity to ensure that the transactions are consistent with the Category 1 eGambling licensee's or Category 1 associate certificate holder's knowledge of the registered customer and his risk profile (including, where necessary, the sources of funds) and paying particular attention to all -

(i) complex transactions,

(ii) transactions which are both large and unusual,

(iii) unusual patterns of activity or transactions, and

(iv) transactions arising from a country or territory that does not apply or insufficiently applies the FATF Recommendations, which have no apparent economic purpose or no apparent lawful purpose and recording its findings thereon in writing, and

(d) ensuring that the way in which identification data are recorded and stored is such as to facilitate the ongoing monitoring of each customer relationship.

9.11 A Category 2 eGambling licensee or, as the case may be, a Category 2 Associate Certificate holder shall perform ongoing and effective monitoring of all gambling transactions, paying particular attention to all –

(a) complex transactions,

(b) transactions which are both large and unusual, and

(c) unusual patterns of activity or transactions, which have no apparent economic purpose or no apparent lawful purpose and recording its findings thereon in writing.

9.12 Examples of the additional monitoring arrangements for high risk relationships could include:

(a) undertaking more frequent reviews of high risk relationships and updating CDD information on a more regular basis;
(b) undertaking more regular reviews of transactions and activity against the profile and expected activity of the business relationship;
(c) applying lower monetary thresholds for the monitoring of transactions and activity;
(d) reviews being conducted by persons not directly involved in managing the relationship, for example, the MLCO;
(e) ensuring that the operator has adequate MI systems to provide the board and MLCO with the timely information needed to identify, analyse and effectively monitor high risk relationships and accounts;
(f) appropriate approval procedures for high value transactions in respect of high risk relationships; and/or
(g) a greater understanding of the personal circumstances of high risk relationships, including an awareness of sources of third party information.

9.13 The operator must consider the possibility for legal persons and legal arrangements to be used as vehicles for ML and FT.

PEP Relationships

9.14 The system of monitoring used by the operator must provide for the ability to identify where a customer or beneficial owner becomes a PEP during the course of the business relationship and whether that person is a foreign PEP, domestic PEP or international organisation PEP.

9.15 In accordance with Paragraph 4(2)(b) of Schedule 4, where a customer or beneficial owner becomes a foreign or domestic PEP during the course of an existing business relationship, as part of the ECDD measures subsequently applied the operator shall obtain senior management approval to continue that relationship.

9.16 Where the operator identifies during the course of a business relationship that the customer or beneficial owner is a domestic PEP or international organisation PEP, it must gather sufficient information to understand the particular characteristics of the public function that the natural person has been entrusted with and factor this information into the relationship risk assessment conducted in accordance with Paragraph 2 of Schedule 4 and Chapter 4 of this guidance.

9.17 It is not expected that the operator will have a thorough knowledge of, or fully research (or be able to fully research), a family connection. The extent to which a connection is researched should be based upon the size, scale, complexity and involvement of the person in the context of the business relationship and the profile of the business relationship, including its customer value.

9.18 It is possible that family members and/or associates may not inform the operator, or even be aware, of their PEP status and therefore independent screening and monitoring should be conducted. It is also possible that an individual's PEP status may not be present at take-on, for example, where that person takes office during the life of a business relationship. It is therefore important that ongoing monitoring exists in order to identify changes of status and risk classification.

High Risk Transactions or Activity

9.19 When conducting ongoing monitoring, the following are examples of red flags which may indicate high risk transactions or activity within a business relationship:

(a) an unusual transaction in the context of the operator's understanding of the business relationship (for example, abnormal size or frequency for that customer.)
(b) funds originating from an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;
(c) the unexpected dormancy of an account or transactions or activity unexpectedly occurring after a period of dormancy;
(d) unusual patterns of transactions or activity, which have no apparent economic or lawful purpose; or

(e) a relevant connection with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

9.20 Transactions or activity having a connection with jurisdictions specified in BSSNs issued by the AGCC and any other AGCC Notices, Instructions or Warnings and those covered by sanctions legislation applicable in the Bailiwick must be subject to a greater level of caution and scrutiny.

Real-Time and Post-Event Transaction Monitoring

9.21 Monitoring procedures should involve a combination of real-time and post-event monitoring. Real-time monitoring focuses on transactions and activity where information or instructions are received before or as the transaction takes place – be this the deposit or withdrawal of funds or undertaking of gambling activity. Post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.
Real-time monitoring of activity can be effective at reducing exposure to ML, FT and predicate offences such as bribery and corruption, whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

9.22 In this respect, regardless of the split of real-time and post-event monitoring, the over-arching purpose of the monitoring process employed should be to ensure that unusual transactions and activity are identified and flagged for further examination.

Automated and Manual Monitoring

9.23 The operator's monitoring processes should be appropriate having regard to its size, activities and complexity, together with the risks identified by the operator within its business risk assessments.

9.24 Notwithstanding the method of monitoring used, in accordance with the requirements of Paragraph 11(4) of Schedule 4, the operator should adapt the parameters of its processes, in particular the extent and frequency of monitoring, on the basis of materiality and risk, including, without limitation, whether or not a business relationship is a high risk relationship.

9.25 In establishing the expected norms of a business relationship and in turn the appropriate parameters for its monitoring processes to be effective, the operator should consider, as a minimum, the nature and level of expected transactions and activity and the assessed risk of the business relationships that are being monitored.

9.26 The rationale for deciding on how to supplement automated monitoring is a decision for the operator to determine having regard to their operations and the issues identified in their business risk assessment. The decision made by the operator should be documented as part of this process, together with an explanation demonstrating why the board consider the chosen methods to be appropriate and effective.

Automated Monitoring Methods

9.27 Where the operator has a larger number of business relationships or a high level of activity, effective monitoring is likely to necessitate greater automation of the monitoring process. Such automated systems may be used to facilitate the monitoring of significant volumes of transactions or business relationships, and associated customers and beneficial owners. Automated systems are necessary for operations in an environment where the opportunity for human scrutiny of individual transactions and activity is limited either by the volume of transactions or their rapidity.

9.28 The use of automated monitoring methods is effective in both strands of ongoing monitoring:

(a) identifying a transaction and/or activity which warrant further scrutiny; and
(b) screening customers and beneficial owners to business relationships or connections to persons subject to sanction or posing an increased risk. For example, PEPs, those convicted of criminal acts, or those persons in respect of whom adverse media exists.

9.29 With regard to the monitoring of transactions and activity, exception procedures and reports can provide a simple but effective means of monitoring all incoming and outgoing transactions and activity to identify those involving, amongst other things:

(a) particular countries, territories or geographical locations;
(b) particular products, services and/or accounts; or
(c) transactions or activity falling outside of predetermined parameters within a given time frame.

9.30 Whatever automated monitoring method is used, whether bespoke to the operator or a more generic system, the operator must:

(a) understand how the system works and how to use the system (for example, making full use of guidance);
(b) understand when changes are to be made to the system (including the nature and extent of any changes);
(c) understand the system's coverage (including the extent of the transactions, activity and/or parties monitored);
(d) understand the sources of data used (including both the source(s) of internal data fed into the system and the source(s) of external data to which it is compared);
(e) understand the nature of the system's output (exceptions, alerts etc.);
(f) set clear procedures for dealing with potential matches, driven on the basis of risk rather than resources; and
(g) record the basis for discounting alerts (for example, false positives) to ensure there is an appropriate audit trail.

9.31 Subject to the paragraph below, the operator must ensure that the parameters of any automated system allow for the generation of alerts for large and unusual, complex, or higher risk transactions or activity which must be subject to further investigation.

9.32 Where the operator is a branch office or subsidiary of an international group and uses group-wide systems for transaction and activity monitoring, the ability for the operator to dictate the particular characteristics of the monitoring conducted by the system may be limited. Where this is the case, notwithstanding the group-wide nature of the system, the operator must be satisfied that it provides adequate mitigation of the risks applicable to the business of the operator.

9.33 The operator should be aware that the use of computerised monitoring systems does not remove the requirement for relevant employees to remain vigilant. It is essential that the operator continues to attach importance to human alertness. Factors such as a person's intuition; direct contact with a customer either via email, chat or on the telephone; and the ability, through practical experience, to recognise transactions and activities which do not seem to have a lawful or economic purpose, or make sense for a particular customer, cannot be automated.

Examination

9.34 In accordance with Paragraph 9(6) of Schedule 4, where within an existing business relationship there are complex, or large and unusual, transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, the operator shall:

(a) examine the background and purpose of those transactions, and
(b) increase the degree and nature of monitoring of the business relationship.

9.35 As part of its examination, the operator should give consideration to the following:

(a) reviewing the identified transaction or activity in conjunction with the relationship risk assessment and the CDD information held;
(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by the operator as to whether the transaction or activity has a rational explanation and economic purpose;
(c) reviewing the appropriateness of the relationship risk assessment in light of the unusual transaction or activity, together with any supplemental CDD information obtained; and
(d) considering the transaction or activity in the context of any other connected business relationships and the cumulative effect this may have on the risk attributed to those relationships.

9.36 For the purposes of Paragraph 9(6) of Schedule 4, what constitutes a large and unusual or complex transaction will be based on the particular circumstances of a business relationship and will therefore vary from customer to customer.

The operator must ensure that the examination of any large and unusual, complex, or otherwise higher risk transaction or pattern of transactions or other activity is sufficiently documented and that such documentation is retained in a readily accessible manner in order to assist the AGCC, the FIS, other domestic competent authorities and auditors.

9.37 The operator must ensure that procedures are maintained which require that an internal disclosure is filed with the MLRO in accordance with the requirements of Chapter 11 of this guidance where the circumstances of the transaction or activity raise a suspicion of ML and/or FT.

9.38 Following the conclusion of its examination, the operator should give consideration to whether follow-up action is necessary in light of the identified transaction or activity. This could include, but is not limited to:

(a) applying ECDD measures where this is considered necessary or where the operator has re-assessed the business relationship as being high risk as a consequence of the transaction or activity;
(b) considering whether further employee training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;
(c) considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or
(d) applying increased levels of ongoing monitoring for particular relationships.

Ongoing Customer Due Diligence

9.39 The requirement to conduct ongoing CDD will ensure that the operator is aware of any changes in the development of a business relationship. The extent of the operator's ongoing CDD measures must be determined on a risk-sensitive basis. However, the operator must be aware that as a business relationship develops, the risks of ML and FT may change.

9.40 The AGCC would expect ongoing CDD to be conducted on a periodic basis in line with the requirement to review relationship risk assessments in accordance with Paragraph 2(5)(b) of Schedule 4, or where a trigger event occurs in the intervening period.

9.41 It should be noted that it is not always necessary to re-verify or obtain current identification data unless an assessment has been made that the identification data held is not adequate for the assessed risk of the business relationship or there are doubts about the veracity of the information already held. Examples of such could include a material change in the way that the business of the customer is conducted, which is inconsistent with its existing business profile or where the operator becomes aware of changes to a customer's or beneficial owner's circumstances, such as a change of address.

9.42 Changes to an existing business profile could be where a customer who has hitherto only engaged in one form of gambling activity, such as bingo starts to place large bets on sporting activity or where a customer who makes regular, low stakes bets on sporting activity starts to make significant deposits for casino games.

Oversight of Monitoring Controls

9.43 The MLCO should have access to, and familiarise themself with, the results and output from the operator's monitoring processes. Such output should be reviewed by the MLCO who in turn should report regularly to the board, providing relevant MI, such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

9.44 The board should consider the appropriateness and effectiveness of the operator's monitoring processes as part of its annual review of the operator's business risk assessments and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and risk as set out in the business risk assessments.

Chapter 10

UN, EU, Targeted financial sanctions, PF and Other Sanctions

Introduction

10.1 A sanction is a measure imposed by a government using laws and regulations to apply restrictive measures against a country, regime, individual, entity, industry or type of activity believed to be violating international law and could include one or more of the following:

(a) the freezing of funds;
(b) the withdrawal of financial services;
(c) a ban or restriction on trade;
(d) a ban or restriction on travel; or
(e) suspension from international organisations.

In undertaking its functions the AGCC will take account of strategic objective 8 of the CONTEST Strategy. Where it is considered appropriate for the Guernsey Policy & Resources Committee to use its powers of designation under the Sanctions Law to designate a person/entity as a terrorist or terrorist financier, and/or to request the UK or the UN to use their powers of designation, to provide full information on this to the Committee. The AGCC is mindful of the importance of preventing asset flight and therefore of urgent action in these circumstances.

10.2 The ultimate objective of a sanction varies according to the situation. Sanctions of this kind are a tool used increasingly for enforcing foreign policy by putting pressure on a state or entity in order to maintain or restore international peace and security. Often, sanctions are used as an alternative to force. All recent UN and EU sanctions contain information as to their intended aim or purpose.

10.3 This section outlines the statutory provisions applicable to operators within the Bailiwick concerning UN, EU and other sanctions. It also covers the policies, procedures and controls required in order to comply with the Bailiwick's sanctions regime and the provisions for the disclosure of information to the relevant authorities in respect of designated persons and

the freezing of funds. Operators should remember that that their operations are likely to cause them to be subject to the legislative regimes of a number of jurisdictions and this will require them to ensure that they meet the sanctions regimes in respects of all aspects of their operations. Within the Bailiwick operators must ensure that they identify those who have been sanctioned within 24 hours of their having been made the subject of a sanction.

Overview

10.4 The two key supranational bodies to determine sanctions measures relevant to the sanctions regime within the Bailiwick are currently the UN and the EU.

The UN Security Council can take measures to maintain, or restore, international peace or security. Such measures range from economic sanctions to international military action. Each UN member state is then called upon to implement the requirements of a sanctions measure in its own territory.

10.5 The EU applies sanctions in pursuit of the specific objectives of the Common Foreign and Security Council as set out in the Treaty of the European Union. EU sanctions are either adopted to ensure compliance with UN sanctions requirements or enacted autonomously by the EU to advance specific EU objectives. European Council ("EC") regulations imposing sanctions apply directly in member states. However, further legislation is required in each member state to impose penalties for sanctions breaches under EC regulations.

10.6 EC regulations impose restrictive measures in respect of designated persons, that is, persons, groups or entities designated by the UN Sanctions Committee or the EU's Security Council. These designated persons are listed in Annex 1 to EC regulations.

10.7 A country may also impose sanctions unilaterally as an extension of its own foreign policy, for example, the UK via HM Treasury or the US via OFAC and can request that other jurisdictions implement sanctions against a person, group or entity.

The Bailiwick's Sanctions Regime

10.8 The Bailiwick has enacted numerous pieces of legislation, which implement sanctions measures, many dealing specifically with FT, the aim of which is to limit the availability of funds and financial services to terrorists and terrorist organisations:

- The Sanctions (Bailiwick of Guernsey) Law, 2018
- The Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey)(Brexit) Regulations, 2020
- The Terrorist Asset-Freezing (Bailiwick of Guernsey) Law, 2011
- The Afghanistan (Restrictive Measures) Ordinance, 2011
- The Al-Qaida (Restrictive Measures) Ordinance, 2013
- The Terrorism Law
- The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002

10.9 The Sanctions (Bailiwick of Guernsey) Law, 2018 is now the main legislation pertaining to the implementation of sanctions in the Bailiwick with the Sanctions (Implementation of UK Regimes) (Bailiwick of Guernsey) (Brexit) Regulations, 2020 giving force to those sanctions that have been imposed by the UK following Brexit.

10.10 While the Bailiwick's sanctions regime is based upon legislation that broadly mirrors equivalent legislation in the UK, it is completely separate from, and operates independently of, the UK regime.

10.11 Whilst not directly enforceable in the Bailiwick, the operator should be aware, in particular, of sanctions implemented by OFAC. OFAC regulations apply to any persons or entities, wherever based, trading in US Dollars, as well as:

(a) US citizens and permanent resident immigrants regardless of where they are located;
(b) persons and entities within the US;
(c) US incorporated entities and their foreign branches;
(d) in the cases of certain sanctions, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by US companies; and
(e) in certain cases, foreign persons in possession of US origin goods.

The Bailiwick's Sanctions Regime – Sanctions Committee

10.12 The Bailiwick has established a Sanctions Committee to co-ordinate sanction activities, ensure information is distributed publicly and to provide advice on sanctions. The Sanctions Committee reports to the External Relations Group of the States of Guernsey's Policy and Resources Committee and to the Bailiwick's AML/CFT Advisory Committee.

The Bailiwick's Sanctions Regime – External Relations Group

10.13 The External Relations Group is mandated on behalf of the Policy and Resources Committee to:

(a) agree to implement new sanctions measures;
(b) licence frozen funds; and
(c) administer notifications and authorities, for example, those under specific ordinances.

10.14 The External Relations Group also works with HM Treasury and the Foreign Commonwealth Office.

Obligation to Report

10.15 Under the Terrorist Asset-Freezing Law, together with the Afghanistan (Restrictive Measures) Ordinance, 2011 and the Al-Qaida (Restrictive Measures) Ordinance, 2013 (collectively "the Restrictive Ordinances"), it is a criminal offence for the operator to fail to disclose to the Policy and Resources Committee any knowledge or suspicion it may have that a customer or potential customer is a designated person or has committed any of the offences set out in the Terrorist Asset-Freezing Law or the Restrictive Ordinances. This requirement is in addition to the reporting obligations in the Disclosure Law and the Terrorism Law.

10.16 Similar requirements apply to orders and ordinances implemented under the aforementioned EU and UN implementation mechanisms.

10.17 The operator should be aware that the effects of failing to comply with sanctions orders could have serious repercussions. This could include prosecution for criminal offences and/or financial penalties, levied not only against the operator but potentially also personally against the senior management of the operator. Any such prosecution is likely to result in extensive reputational damage for the operator, its board and the Bailiwick as an international finance centre.

Designated Persons

10.18 For the purposes of the Terrorist Asset-Freezing Law, a designated person means any natural or legal person, group or entity which is:

(a) designated by the Policy and Resources Committee under the Terrorist Asset-Freezing Law;
(b) the subject of a designation under and within the meaning of the UK's Terrorist Asset-Freezing etc. Act, 2010; or
(c) included in the list provided for by Article 2(3) of Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (as amended from time to time).

Policies, Procedures and Controls

10.19 The operator must have in place appropriate and effective policies, procedures and controls to identify, in a timely manner, whether a prospective or existing customer, or any beneficial owner, key principal or other connected party, is the subject of a sanction issued by the UN, the EU or the States of Guernsey's Policy and Resources Committee. In the case of an existing customer this identification must be made within 24 hours of them having been made the subject of a sanction.

10.20 Examples of other connected parties for the purposes of the above include individuals or groups not deemed to be beneficial owners but who own rights or interests in a legal person customer and third party recipients of transactions.

10.21 For this purpose, HM Treasury maintains a list, which includes all persons whose designations are effective in the Bailiwick (including designations by the EU and UN), other than those persons specifically designated by the Policy and Resources Committee under the Terrorist Asset-Freezing Law who are separately listed by the States of Guernsey. Both lists can be found through the below links:

https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets
https://www.gov.gg/sanctionsmeasures

10.22 It should be noted that the UN and EU do not have a notification facility for advising when the lists of designated persons maintained by them are updated. However, HM Treasury (including UN and EU designations) and OFAC both offer facilities for notification by e-mail when a financial sanctions related release is published. Below are links to both facilities:

https://ofsi.blog.gov.uk/subscribe/
https://ofac.treasury.gov/faqs/topic/1511

10.23 In addition, as referenced previously, OFAC sanctions apply to all transactions in US Dollars. Therefore, where the operator is deals in US dollars it should be mindful of the US sanctions regime. OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups and entities, such as terrorists and narcotics traffickers designated under programmes that are not country specific. Collectively, such individuals and companies are called Specially Designated Nationals ("SDNs"). The assets of SDNs are blocked and US entities are prohibited from dealing with them. The list of SDNs and a free OFAC search facility can be found through the below links:

https://www.gov.uk/government/publications/the-uk-sanctions-list
https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

10.24 The operator must have in place a system and/or control to detect and block transactions connected with those natural persons, legal persons and legal arrangements designated by the Bailiwick's sanctions regime within 24 hours.

10.25 The transaction monitoring systems and/or controls used should enable the operator to identify transactions, both incoming and outgoing, involving designated persons.

Customer Screening

10.26 In order to comply with the provisions set out above, as a minimum the operator should undertake sanctions screening for all new business relationships, including the customer, beneficial owner and other key principals, at the time of take-on, during periodic reviews and when there is a trigger event generating a relationship review.

10.27 Following changes to the lists of persons designated by the UN or EU, the States of Guernsey Policy and Resources Committee may issue sanctions notices to alert operators to such changes. These sanctions notices are issued by the FIS via THEMIS but operators must be aware that they are obliged to identify the subject of sanction within 24 hours of their being sanctioned irrespective of whether a notice is issued via THEMIS or not.

10.28 The operator should have appropriate procedures and controls in place to ensure that the those who have been made the subject of a sanction are identified within 24 hours of their designation.

10.29 Where the operator utilises an automated method of sanctions screening, the operator should maintain, or have access to, an audit trail of the screening conducted by the system. The audit trail should enable the operator to demonstrate the dates on which screening checks have been undertaken and the results of those checks, thus allowing the operator to satisfy itself, and demonstrate to third parties, that the system is operating effectively. Where the operator is part of a wider group and utilises a group-wide screening system, the operator should seek written confirmation from its head office that such an audit trail exists and that the operator can have access to any specific records upon request.

Compliance Monitoring Arrangements

10.30 The operator must ensure that its compliance monitoring arrangements include an assessment of the effectiveness of the operator's sanctions controls and their compliance with the Bailiwick's sanctions regime.

10.31 Testing undertaken in respect of any sanctions screening system should cover the following:

(a) ensuring that the screening system has been correctly configured and that the relevant pre-set rules have been activated;
(b) assessing the accuracy of the screening system or method utilised, for example, through an analysis of the alerts generated, to ensure that designated persons are promptly identified;
(c) determining the appropriateness of the operator's controls for the business undertaken, including the method and frequency of testing;
(d) where upgrades have been applied, ensuring that the system performs as expected;
(e) where reliance is placed upon a third party for sanctions screening, the operator should verify the effectiveness of the screening being undertaken by that party; and
(f) determining the appropriateness of the action taken by the operator where a sanctions match has been identified to ensure that the proceeds associated with designated persons are controlled and the necessary reporting undertaken in compliance with applicable regulatory requirements.

10.32 As part of its compliance testing, the operator should give consideration to assessing the sensitivity of any screening tools used, i.e. testing the system's 'fuzzy logic'. Such tests could be conducted by using real-life case studies, entering the name of sanctioned natural or legal persons to ensure that the expected results are achieved.

Chapter 11

Reporting suspicion

Introduction

11.1 This chapter outlines the statutory provisions concerning the disclosure of information; the policies, procedures and controls necessary for reporting and disclosing suspicion; and the provision of information for the purposes of the reporting and disclosing of suspicion.

11.2 The obligations to report and disclose suspicion are set out within the Disclosure Law and the Terrorism Law (together "the Reporting Laws"). Additional obligations are set out in the Disclosure (Bailiwick of Guernsey) Regulations, 2007 as amended ("the Disclosure Regulations") and the Terrorism and Crime (Bailiwick of Guernsey) Regulations, 2007 as amended (together "the Reporting Regulations"), together with Schedule 4.

11.3 References in this chapter to suspicion are references to suspicion that another person is engaged in ML or FT, or that certain funds are derived from, the proceeds of criminal conduct or terrorist activity, as the case may be.

11.4 References in this chapter to criminal conduct are references to any conduct which constitutes a criminal offence under the law of any part of the Bailiwick, or is, or corresponds to, conduct which, if it took place in any part of the Bailiwick, would constitute an offence under the law of that part of the Bailiwick.

11.5 References in this chapter to ML are references to offences under Sections 38, 39 and 40 of the Law or Part IV of the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 as amended ("the Drug Trafficking Law").

11.6 The overall purpose of Sections 38, 39 and 40 of the Law and Part IV of the Drug Trafficking Law is to create extremely wide ranging 'all crime' prohibitions on ML, covering the following activities:

(a) concealing or transferring the proceeds of criminal conduct or drug trafficking;

(b) assisting another person to retain the proceeds of criminal conduct or drug trafficking; and

(c) the acquisition, possession or use of the proceeds of criminal conduct or drug trafficking.

11.7 References in this chapter to FT are references to offences under Sections 8, 9, 10 or 11 of the Terrorism Law, Sections 9, 10, 11, 12 or 13 of the Terrorist Asset-Freezing Law or under Ordinances implementing international sanctions measures in respect of terrorism that are listed at Section 79 of the Terrorism Law. These offences apply not only to the financing of terrorist acts, but also to the financing of terrorist organisations, or individual terrorists, even in the absence of a link to a specific terrorist act or acts. The offences cover the following activities:

(a) fundraising for the purpose of terrorism;

(b) using or possessing money or other property that is intended to be, or may be, used for the purposes of terrorism;

(c) funding arrangements for the purposes of terrorism;

(d) money laundering of terrorist property; and

(e) making funds or other economic resources available to persons included in terrorism-related sanctions lists.

11.8 The ML offences in Sections 38 to 40 of the Law and Part IV of the Drug Trafficking Law are expressed as not applying to acts carried out with the consent of a police officer, where that consent is given following a disclosure of suspicion. The same applies in respect of the FT offences at Sections 9 to 11 of the Terrorism Law. The effect of these provisions is that if, following the making of a report and disclosure of suspicion under the Reporting Laws, the FIS consents to the operator or person in question carrying out a relevant act, the operator or person will have a defence to a possible charge of ML or FT, as the case may be, in relation to that act. This is referred to informally as the consent regime and is covered further at Section 11.51 *et seq* of this chapter.

11.9 Pursuant to the Reporting Regulations, the operator shall report and disclose suspicion to the FIS using the prescribed manner, specifically the online reporting facility THEMIS.

Further information on the form and manner of disclosing suspicion can be found obtained from the FIS.

11.10 The operator should note that the court will take account of the AGCC Regulations and guidance provided in this guidance in considering compliance with the disclosure requirements of the Reporting Laws, the Reporting Regulations and Schedule 4.

11.11 References to a transaction or activity include an attempted or proposed transaction or activity, or an attempt or proposal to enter into a business relationship.

Obligation to Disclose

11.12 In accordance with the requirements of the Reporting Laws, all suspicious transactions and activity, including attempted transactions and activity, are to be reported regardless of the value of the transaction.

11.13 A suspicion may be based upon:

(a) a transaction or attempted transaction or activity which is inconsistent with a customer's (or beneficial owner's) known legitimate business, activities or lifestyle or is inconsistent with the normal business for that type of product/service; or

(b) information from other sources, including law enforcement agencies, other government bodies (for example, Income Tax), the media, intermediaries, or the customer themselves.

11.14 An important precondition for the recognition of suspicious activity is for the operator to know enough about the business relationship to recognise that a transaction or activity is unusual in the context. Such knowledge would arise mainly from complying with the monitoring and ongoing CDD requirements in Paragraph 9 of Schedule 4 and chapter 9 of this guidance.

11.15 The board of the operator and all employees should appreciate and understand the significance of what is often referred to as the objective test of suspicion. It is a criminal

offence for anyone employed by the operator to fail to report where they have knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is laundering the proceeds of any criminal conduct or is carrying out terrorist financing.

11.16 What may constitute reasonable grounds for knowledge or suspicion will be determined from facts or circumstances from which an honest and reasonable person employed by the operator would have inferred knowledge or formed the suspicion that another was engaged in ML or FT.

11.17 A transaction or activity which appears unusual is not necessarily suspicious. An unusual transaction or activity is, in the first instance, likely to be a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. As an example, an out of the ordinary transaction or activity within a business relationship should prompt the operator to conduct enquiries about the transaction or activity.

11.18 There may be a number of reasons why the operator is not entirely happy with CDD information or where the operator otherwise needs to ask questions. Examples of such are provided within this chapter. Where the operator has queries, regardless of the level of suspicion, to assist them in formulating or negating a suspicion, any enquiries of the customer or other key principal should be made having due regard to the tipping off provisions.

11.19 The operator should consider whether the nature of a particular suspicion is such that all of the assets of the business relationship are potentially suspect. Where it is not possible to separate assets which are suspicious from those which are legitimate, it will be necessary to carefully consider all future transactions or activity and the nature of the continuing relationship. The operator should also consider implementing an appropriate risk-based strategy to deal with any risk associated with the business relationship.

11.20 It should be noted that suspicion of ML or FT could relate to funds whether they directly or indirectly relate to criminal conduct.

11.21 While the operator is not expected to conduct the kind of investigation carried out by law enforcement agencies, it must act responsibly when asking questions to satisfy any gaps in

its CDD, or its understanding of a particular transaction or activity or proposed transaction or activity.

Attempted Transactions

11.22 The definition of ML and FT in the Reporting Laws includes an attempt to carry out an offence of ML or FT. This means that attempted transactions fall within the scope of the reporting obligations. An attempted transaction could be classified as one that a customer intended to conduct with the operator and took some form of action or activity to do so but failed to complete.

11.23 The obligation to report suspicion applies to all types of activity and attempted transactions or activity, including circumstances where there is no existing business relationship with the customer and no such business relationship is subsequently established.

11.24 During the course of attempting to set up a new business relationship, due consideration should be given during the CDD process to key points raised with or by the customer, for example, if the customer fails to explain the source of funds; if the purpose of the account or advice required does not make sense. Depending upon the information received, the operator may form a suspicion of ML and/or FT in which case a disclosure shall be submitted to the FIS in accordance with the Disclosure Law or the Terrorism Law.

11.25 The FIS has published a guidance document concerning 'Attempted Transactions'. The objective of the document is to assist operators in the determination of whether a disclosure should be submitted to the FIS.

https://guernseyfiu.gov.gg/article/176702/FIU-Guidance

Potential Red Flags

11.26 The following is a non-exhaustive list of possible ML and FT red flags that the operator should be mindful of when dealing with a business relationship. The list is not exhaustive and its content is purely provided to reflect examples of possible red flags. The existence of one or more red flag does not automatically indicate suspicion and there may be a legitimate reason why a customer has acted in the manner identified.

11.27 Red flag indicators can be specific to eGambling as well as general. A MONEYVAL research report identified that the following factors may indicate possible ML through eGambling:-

(a) Information provided by the customer contains a number of mismatches (e.g. email domain, telephone or postcode details do not correspond to the country);
(b) The registered credit card or bank details do not match the customer's registration details;
(c) The customer is situated in a higher-risk jurisdiction or is identified as being listed on the international sanctions list;
(d) The customer is identified as a politically exposed person;
(e) The customer seeks to open multiple accounts under the same name (operators should also note that this may raise issues with regards to player protection and should have regard to ICS guideline 3.2.5);
(f) The customer opens several accounts under different names using the same IP address;
(g) The withdrawals from the account are not commensurate with the conduct of the account, such as for instance where the customer makes numerous deposits and withdrawals without engaging in significant gambling activity;
(h) The customer deposits large amounts of funds into his online gambling account;
(i) The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds;
(j) The customer logs into the account from multiple countries;
(k) A deposit of substantial funds followed by very limited activity;
(l) The customer has links to previously identified accounts; different players are identified as sharing banks accounts from which deposits or withdrawals are made.

Policies, Procedures and Controls

11.28 In accordance with Paragraph 10(1)(f) of Schedule 4, the operator shall ensure that it establishes and maintains such other appropriate and effective procedures and controls as are necessary to ensure compliance with requirements to make disclosures under Part I of the Disclosure Law, and Sections 15 and 15A or Section 12 (as appropriate) of the Terrorism Law.

11.29 In establishing appropriate and effective policies, procedures and controls to facilitate compliance with the requirements of the Reporting Laws and the Reporting Regulations, the operator's policies, procedures and controls must ensure that:

(a) each suspicion of ML or FT is reported to the MLRO, or in their absence a Nominated Officer, regardless of the amount involved and regardless of whether, amongst other things, it is thought to involve tax matters, in a manner sufficient to satisfy the statutory obligations of the employee;

(b) where an employee of the operator knows or suspects, or has reasonable grounds for knowing or suspecting, that someone is engaged in ML and/or FT, an internal disclosure is made to the MLRO, or in their absence a Nominated Officer, of the operator;

(c) the MLRO or Nominated Officer promptly considers each internal disclosure and determines whether it results in there being knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in ML and/or FT or that certain property represents, or is derived from, the proceeds of criminal conduct or terrorist property;

(d) where the MLRO or Nominated Officer has determined that an internal disclosure does result in there being such knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that someone is engaged in ML and/or FT, that the MLRO or Nominated Officer discloses that suspicion to the FIS; and

(e) all internal and external disclosures made in the above manner are of a high quality and meet the standards set out in this guidance and in any feedback and guidance notices issued by the FIS and the AGCC.

Internal Disclosures

11.30 In accordance with Paragraph 10(1)(c) Schedule 4, the operator shall ensure that where an employee, other than the MLRO, is required to make a disclosure under Part I of the Disclosure Law, or Section 15 or Section 12 (as appropriate) of the Terrorism Law, that this is done by way of a report to the MLRO, or, in that officer's absence, to a Nominated Officer.

11.31 The operator must have appropriate and effective internal disclosure policies, procedures and controls to ensure that:

(a) all employees know to whom within the operator and in what format their suspicions must be disclosed;
(b) all internal disclosures are considered by the MLRO, or in their absence a Nominated Officer, and where the MLRO or Nominated Officer makes a decision not to make an external disclosure to the FIS, the reasons for the decision not to disclose are documented and retained;
(c) enquiries made by an MLRO or Nominated Officer in respect of disclosures are recorded and documented; and
(d) once an external disclosure has been made to the FIS, the MLRO or Nominated Officer immediately informs the FIS where subsequent relevant information or documentation is received.

11.32 The MLRO should consider whether to include within the operator's procedures the provision of an acknowledgment to evidence the submission of an internal disclosure. Such an acknowledgement would provide confirmation to the submitter that their statutory obligations have been fulfilled.

Form and Manner of Disclosure to the FIS

11.33 In accordance with the requirements of the Reporting Laws, suspicion of ML shall be disclosed under the provisions of the Disclosure Law and suspicions relating to FT shall be disclosed under the Terrorism Law.

11.34 The Reporting Laws require that information contained in an internal disclosure made to an MLRO or Nominated Officer is disclosed to the FIS where the MLRO or Nominated

Officer knows or suspects, or has reasonable grounds for knowing or suspecting, as a result of the internal disclosure, that a person is engaged in ML and/or FT.

11.35 In accordance with Paragraph 10(1)(d) of Schedule 4, the operator shall ensure that the MLRO, or in that officer's absence a Nominated Officer, in determining whether or not they are required to make a disclosure under Part I of the Disclosure Law, or Section 15A or Section 12 (as appropriate) of the Terrorism Law, takes into account all relevant information.

11.36 The Reporting Regulations provide that disclosures to the FIS are to be made in the prescribed manner, specifically through the online reporting facility THEMIS.
In exceptional circumstances, a disclosure can be made using the form set out in the Schedule to the Disclosure Regulations. However, in accordance with Regulation 1(2) of the Disclosure Regulations, the operator shall obtain the consent of an authorised officer (SIO, Inspector or above) prior to submitting such a form.

11.37 In accordance with Paragraph 10(1)(e) of Schedule 4, the operator shall ensure that the MLRO, or, in their absence, a Nominated Officer, is given prompt access to any other information which may be of assistance to them in considering any report.

11.38 Prior to making a disclosure to the FIS, the operator should consider all available information in respect of the business relationship. Notwithstanding this consideration, disclosures to the FIS should be made promptly following a determination by the MLRO or Nominated Officer that a disclosure is appropriate.

11.39 Where the MLRO or Nominated Officer considers that a disclosure should be made urgently, for example, where the customer's product is already part of a current investigation, initial notification to the FIS may be made by telephone on +44(0) 1481 714081.

https://guernseyfiu.gov.gg/article/175901/Contact

Information to be Provided with a Disclosure

11.40 The operator should provide the FIS with a full account of the circumstances and grounds (suspected underlying criminality) for suspicion. In providing such detail, the operator should include as much relevant information and documentation as possible (for example, CDD information, statements, chat logs, minutes, transcripts, etc.) to demonstrate why suspicion has been raised and to enable the FIS to fully understand the purpose and intended nature of the business relationship.

11.41 The operator should examine all connected accounts and/or relationships and provide detailed, current balances of such to the FIS. Research of connected accounts or relationships should not delay the operator making a disclosure to the FIS.

11.42 The Reporting Laws provide that a disclosure made in good faith to a police officer does not contravene any obligation as to confidentiality or other restriction on the disclosure of information imposed by statute, contract or otherwise. Additionally, the Reporting Laws require that disclosures made under them include information or documentation relating to the knowledge, suspicion, or reasonable grounds for suspicion, that the person in respect of whom the disclosure is made is engaged in ML and/or FT, and any fact or matter upon which such knowledge, suspicion, or reasonable grounds for suspicion, is based.

11.43 The operator is also required to provide the FIS with the reasons for suspicion. The operator should clearly define the grounds for suspicion and any specific indicators or suspected criminality within the main body of the disclosure. The operator may have multiple grounds, i.e. ML and tax evasion or bribery and corruption and fraud.

11.44 For the purposes of the above, 'information' or 'document' includes any information or document relating to:

(a) any funds ;
(b) any transaction concerning such money or property; or
(c) the parties to any such transaction.

Group Reporting

11.45 It is for each operator or group to consider whether, in addition to any disclosure made in the Bailiwick, the MLRO should report suspicions within the operator or group, for example, to the compliance department at head office. A report to head office, the parent or group does not remove the requirement to disclose suspicions to the FIS. Given the cross border nature of eGambling, it is possible that a report may need to be made to satisfy legal requirements in other jurisdictions. It may also be the case that where the operator is part of a larger group with operations in a number of jurisdictions a report will be initially made in a different jurisdiction and also submitted to the FIS. Where this is the case the report should state that a report has been made in another jurisdiction and provide the unique reference number generated by that report to the FIS.

11.46 When deciding whether to report within the operator or group, consideration should be given to the sensitivity of the disclosure and the risks involved in the sharing of this information, for example, if the subject of the disclosure is under ongoing investigation by the FIS. In this respect, consideration should be given by the operator to anonymising disclosures prior to onward reporting.

The Response of the FIS

11.47 Upon submitting a disclosure to the FIS via THEMIS, a response acknowledging receipt will be sent automatically. Similarly if, following appropriate permission from the FIS, a paper disclosure has been submitted, a response acknowledging receipt will be sent to the operator.

11.48 If the FIS consider that the disclosure, whether through THEMIS or in paper form, contains information that is not of a qualitative nature as detailed above, the operator will be notified and sufficient additional information should be provided to the FIS.

11.49 Access to disclosures will be restricted to appropriate authorities and any information provided by the FIS emanating from such disclosures will normally be anonymous. In the event of a prosecution, the source of the information will be protected as far as the law allows.

11.50 In addition, the FIS will, so far as is possible, supply on request and through planned initiatives, information as to the current status of any investigations emanating from a disclosure as well as more general information regarding identified trends and indicators.

Consent Requests

11.51 It is for each operator, group or person to consider whether any disclosure of suspicion made to the FIS concerns an 'act' that would constitute an ML offence as detailed above.

11.52 If the operator, group or person suspects such an 'act' may be committed and the operator, group or person intends to carry out such an 'act', a request should be submitted as part of the operator's disclosure to the FIS outlining the suspected 'act' and seeking consent from a police officer to undertake the 'act'. Operator's should note that a consent request may have a different name in other jurisdictions, for example it may be known as a Defence against Money Laundering (DAML) request.

11.53 Upon receipt of a request, the FIS will consider whether or not to grant consent under the provisions of the relevant legislation:

(a) If the disclosure and/or request does not contain sufficient information to demonstrate why suspicion has been raised and to enable the FIS to fully understand the purpose and intended nature of the business relationship, a reply may be sent stating that:

'Based upon the information provided the FIS does not consider the request made to be a consent issue'.

Such a response does not imply that the intended transaction or activity could not constitute an offence, only that the FIS has not received sufficient information in order to make that determination and therefore if consent would apply.

(b) If consent is granted a response may be sent stating that:

'Based upon the information provided you have consent to continue or maintain the account(s) or other relationship'.

It should be noted that a consent to continue or maintain an account or relationship, granted by a police officer, only provides a criminal defence to the offence in relation to the 'act' specified in the request. It should also be noted that such a consent does not release the operator, group or person from their obligation in respect of all future transactions and activity on the account or arising from the relationship.

(c) If there are cogent grounds to suspect that the funds represent the proceeds of crime, the FIS may withhold consent and advise the operator accordingly.

11.54 The operator, group or person may wish to consider submitting a further disclosure should the circumstances detailed in the original disclosure change in such a way as to give rise to further knowledge or suspicion of ML or FT not already disclosed to the FIS.

11.55 The FIS will endeavour to reply to a consent request as soon as practicable. Nevertheless, it should be noted that the FIS is not mandated by law to respond within a specified timeframe. The operator should not continue with the intended transaction or activity until a response from the FIS has been received.

Tipping Off

11.56 The Reporting Laws provide that it is a criminal offence for a person, who knows or suspects that an internal disclosure to an MLRO or an external disclosure to the FIS has been or will be made, or any information or other matter concerning a disclosure has been or will be communicated to an MLRO or the FIS, to disclose to any other person information or any other matter about, or relating to, that knowledge or suspicion unless it is for a purpose set out in the Reporting Laws.

11.57 The purposes detailed in the Reporting Laws include, but are not limited to, the prevention, detection, investigation or prosecution of criminal offences, whether in the Bailiwick or elsewhere.

11.58 Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity, which has given rise to the suspicion is prudent practice, forms an integral part of CDD and ongoing monitoring and should not give rise to tipping off.

11.59 If the operator identifies open source information on the customer (for example, a media article indicating that the customer is or has been subject to criminal proceedings) this should not give rise to tipping off. However, the operator should consider disclosing the matter to the FIS.

11.60 HM Procureur has issued a paper entitled 'Guidance on Prosecution for Tipping Off', which permits disclosures to be made to members of the same organisation or linked organisations to discharge their AML and CFT responsibilities, save where there are grounds to believe that this may prejudice an investigation.

https://www.guernseylawofficers.gg/article/161432/Publications-and-Policies

11.61 The operator's policies, procedures and controls must enable the MLRO to consider whether it is appropriate to disclose a suspicion to the FIS or to make a request for consent or whether, in assessing the circumstances, it would in the first instance be more appropriate to obtain more information to assist with the decision. Such procedures must also provide for the MLRO to consider whether it would be more appropriate to decline to proceed with a transaction and to give due thought to the future of the business relationship as a whole before proceeding.

Terminating a Business Relationship

11.62 Whether or not to terminate a business relationship is a commercial decision, except where required by law, for example, where the operator cannot obtain the required CDD information (see chapter 5 of this guidance and Paragraph 6 of Schedule 4).

11.63 There will be occasions where it is feasible for the operator to agree a joint strategy with the FIS but the FIS will not seek to influence what is ultimately a decision for the operator regarding the future of its business relationship with the customer and the online reporting facility cannot be used for this purpose.

11.64 Where the operator takes the decision to terminate a business relationship after it has made a disclosure or requested FIS consent and is concerned that, in doing so, it may prejudice an investigation or contravene the tipping off obligations, it should engage with the FIS accordingly. However, the decision whether or not to terminate a business relationship is a decision that ultimately rests with the operator.

FIS Requests for Additional Information

11.65 Under Regulation 2 of the Reporting Regulations, the FIS may serve a written notice on a person who has made a disclosure requiring that person to provide additional information relating to the disclosure. Such additional information may provide clarification of the grounds for suspicion and allow the person to whom the disclosure has been made to make a judgement as to how to proceed.

11.66 An amendment to the Reporting Regulations came into force on 7 August 2014 providing that, if a disclosure has been made, the FIS can request information relating to that disclosure from a third party if it is satisfied that there are reasonable grounds to believe that the third party possesses relevant information and that there are reasonable grounds to believe that the information is necessary for the FIS to properly discharge its functions.

11.67 Regulation 2A of the Reporting Regulations applies where a person has made a disclosure under Section 1, 2 or 3 of the Disclosure Law and/or under Section 12, 15 or 15C of the Terrorism Law and the police officer to whom the disclosure was made believes, as a result, that a third party may possess relevant information.

11.68 A police officer may, by notice in writing served upon a third party, require that third party to provide the police officer or any other specified officer with such additional information relating to the initial disclosure as it may require. Any such additional information will be requested in writing.

11.69 Ordinarily, the information requested under Regulation 2 or Regulation 2A of the Reporting Regulations shall be provided within seven days, though the FIS may extend that time period when justification is provided by the operator regarding the need to extend the period. The time period may also be reduced if the information is required urgently.

11.70 The operator has a statutory obligation to provide additional information pursuant to Regulation 2 or Regulation 2A of the Reporting Regulations. The police officer would have obtained authority from the Head of the FIS or an officer of the rank of SIO or Inspector (or above) for a notice to be served. Failure without reasonable excuse to comply with a notice (including within the specified time frame) is a criminal offence.

Management Information

11.71 The regular receipt of adequate and appropriate MI is beneficial in helping the board ensure that the operator can discharge its responsibilities fully under Paragraph 10(1)(f) of Schedule 4.

11.72 The MI provided to the board should include:

(a) the number of internal disclosures received by the MLRO or a Nominated Officer;
(b) the number of external disclosures reported onward to the FIS;
(c) an indication of the length of time taken by the MLRO or Nominated Officer in deciding whether or not to externalise an internal disclosure; and
(d) the nature of the disclosures.

THEMIS Notices

11.73 THEMIS has the facility to provide operators with notices which are sent via a generic email address to individual users. These notices are a mechanism through which the FIS provides information to all THEMIS users or to specific 'targeted' distribution groups or operators, dependent upon the information or guidance that is being issued.

11.74 Notices sent via THEMIS include updates on changes to the legislative framework, news of forthcoming presentations or seminars and updates in respect of EU, UN and other sanctions. In addition to generic updates, the FIS may specifically 'target' certain distribution groups or operators in respect of a notification that a certain entity or group of entities is under

investigation by the FIS or other law enforcement agencies. In this respect, THEMIS is the mechanism by which specific 'targeted' notices will be distributed to MLROs.

11.75 The MLRO should refer to the THEMIS portal whenever a notification is issued by the FIS and additionally at regular intervals on an ad hoc basis. Where targeted notices are issued, the operator should establish if it maintains a business relationship with the entities listed on the notice or if it has information which may assist the FIS. The operator should consider whether the receipt of a targeted notice from law enforcement is sufficient grounds for suspicion to make an external disclosure to the FIS in accordance with this guidance. It should be noted that the FIS have the facility to monitor whether notices have been received and/or read by the recipient.

AGCC Notices

11.76 Notices and Instructions that are issued by the Commission will be placed on the Commission's website. In addition each Relationship Manager will draw the operators attention to Notices and Instructions as they are issued. Where appropriate Notices and Instructions will form part of the discussion at any outreach session conducted by the Commission.

Chapter 12

Employee screening and training

Introduction

12.1 One of the most important tools available to the operator to assist in the prevention and detection of financial crime is to have appropriately screened employees who are alert to the potential risks of ML, FT and the risks of breaching TFS and PF sanctions and who are well trained in the requirements concerning CDD and the identification of unusual activity, which may prove to be suspicious.

12.2 The effective application of even the best designed systems, policies, procedures and controls can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, the appropriate policies, procedures and controls or are not adequately trained.

12.3 The term employee is defined in Schedule 4 as an individual working, including on a temporary basis, for an eGambling licensee, Category 1 Associate Certificate holder or Category 2 Associate Certificate holder, whether under a contract of employment, a contract for services or otherwise. This includes directors, both executive and non-executive and persons employed by external parties fulfilling a function in relation to the operator under an outsourcing agreement or a contract for services.

Board oversight

12.4 The board needs to be aware of the obligations of the operator in relation to employee screening and training.

12.5 The operator must ensure that the training provided to relevant employees is comprehensive and ongoing and that employees are aware of ML, FT, the risks of breaching TFS and PF sanctions the risks and vulnerabilities of the operator to it, and their obligations in relation to it.

12.6 The operator must establish and maintain mechanisms to measure the effectiveness of the AML and CFT training provided to relevant employees.

12.7 In order to measure the effectiveness of AML and CFT training, the operator could consider it appropriate to incorporate an exam, test or some form of assessment into its ongoing training programme, either as part of the periodic training provided to relevant employees or during the intervening period between training.

12.8 Regardless of the methods utilised, the board should ensure that it is provided with adequate information on a sufficiently regular basis in order to satisfy itself that the operator's relevant employees are suitably trained to fulfil their personal and corporate responsibilities.

12.9 Where the operator outsources its MLRO and/or MLCO functions to a third party, it should also consider the content of chapters 2 and 13 of this guidance, which set out the steps the operator should take to ensure that the outsourced service provider has appropriate policies, procedures and controls surrounding the hiring and training of employees.

Screening requirements

12.10 In accordance with Paragraph 11(1)(a) of Schedule 4, the operator shall maintain appropriate and effective procedures proportionate to the nature and size of the operator and to its risks when hiring employees for the purpose of ensuring high standards of employee probity and competence.

12.11 In order to ensure that employees are of the required standard of competence and probity, which will depend on the role of the employee, the operator must give consideration to the following prior to, or at the time of, recruitment:

(a) obtaining and confirming appropriate references;
(b) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
(c) obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record (subject to

the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 as amended); and

(d) obtaining and confirming details of employment history, qualifications and professional memberships.

12.12 The operator must ensure that its consideration under the above, together with the results of any checks undertaken, are documented and retained.

Training requirements

12.13 In accordance with Paragraph 11(1) of Schedule 4, the operator shall ensure that relevant employees receive comprehensive ongoing training (at a frequency which has regard to the ML and FT risks to the operator).

12.14 The requirements of Schedule 4 concerning training apply to relevant employees, being those employees whose duties relate to actual specified business activities, including board members and senior management, and not necessarily to all employees.

12.15 When determining whether an employee is a relevant employee for the purposes of Schedule 4 and this guidance, the operator should take into account the following:

(a) whether the employee is undertaking any customer facing functions or handles, or is responsible for the handling of, business relationships, or transactions conducted in respect of such;

(b) whether the employee is directly supporting a colleague who carries out any of the above functions;

(c) whether an employee is otherwise likely to be placed in a position where they might see or hear anything which may lead to a suspicion; and

(d) whether an employee's role has changed to involve any of the functions mentioned above.

Training Requirements for Other Employees

12.16 There may be some employees who, by virtue of their function, fall outside of the definition of a relevant employee, for example, receptionists, artists, graphic designers and possibly coders. The operator should consider, on a case-by-case basis, whether an employee falls within the definition of a relevant employee as the scope of a person's role and the tasks undertaken will vary from person to person. The operator should also be aware that an employee's function may change over time. In addition the operator may want to consider the impact of the work of artists, designers and coders has on other facets of eGambling and that AML/CFT training and the awareness this brings enables them to incorporate AML/CFT measures into products by design.

12.17 Where the operator has concluded that an individual's role does not make them a relevant employee, it should be aware that those employees will still have obligations under the Law, the Disclosure Law, the Terrorism Law and other legislation. As a consequence, all employees, regardless of their function, should have a basic understanding of ML and FT, together with an awareness of the operator's internal reporting procedures and the identity of the MLRO and Nominated Officer(s).

12.18 In order to achieve this the operator must as a minimum:

(a) provide any employee who has not been classified as a relevant employee with a written explanation of the operator's and the employee's obligations and potential criminal liability under the Relevant Enactments, including the implications of failing to make an internal disclosure; and

(b) require the employee to acknowledge that they understand the operator's written explanation and the procedure for making an internal disclosure.

Methods of training

12.19 While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

12.20 The guiding principle of all AML and CFT training should be to encourage relevant employees, irrespective of their level of seniority, to understand and accept their responsibility

to contribute to the protection of the operator against the risks of ML, FT and the risks of breaching TFS and PF sanctions.

12.21 The precise approach adopted will depend upon the size, nature and complexity of the operator's business. Classroom training, videos and technology-based training programmes can all be used to good effect, depending on the environment and the number of relevant employees to be trained.

12.22 Training should highlight to relevant employees the importance of the contribution that they can individually make to the prevention and detection of ML and FT and the risks of breaching TFS and PF sanctions. There is a tendency, in particular on the part of more junior employees, to mistakenly believe that the role they play is less pivotal than that of more senior colleagues. Such an attitude can lead to failures in the dissemination of important information because of mistaken assumptions that the information will have already been identified and dealt with by more senior colleagues.

Frequency of training

12.23 The operator must provide the appropriate level of AML and CFT induction training, or a written explanation, to all new relevant employees or other employees respectively, before they become actively involved in the day-to-day operations of the operator.

12.24 Consideration should be given by the operator to establishing an appropriate minimum period of time by which, after the start of their employment, new employees should have completed their AML and CFT induction training. Satisfactory completion and understanding of any mandatory induction training should be a requirement of the successful completion of a relevant employee's probationary period.

12.25 The operator must provide ongoing AML and CFT training to all relevant employees. Training will need to be more frequent to meet the requirements of Schedule 4 if new legislation or significant changes to this guidance are introduced, or where there have been significant technological developments within the operator or industry or the introduction of new products, services or practices.

Content of training

12.26 The operator must, in providing the training required pursuant to Schedule 4 and this guidance:

(a) provide appropriate training to relevant employees to enable them to competently analyse information and documentation so as to enable them to form an opinion on whether a business relationship is suspicious in the circumstances;
(b) provide relevant employees with a document outlining their own obligations and potential criminal liability and those of the operator under Schedule 4 and the Relevant Enactments;
(c) prepare and provide to relevant employees a copy, in any format, of the operator's policies, procedures and controls manual for AML and CFT; and
(d) ensure relevant employees are fully aware of all applicable legislative requirements.

12.27 In accordance with Paragraph 11(2) of Schedule 4, the ongoing training provided by the operator shall cover –

(a) the Relevant Enactments, Schedule 4 and this guidance,
(b) the personal obligations of employees, and their potential criminal liability under Schedule 4 and the Relevant Enactments,
(c) the implications of non-compliance by employees with any rules, guidance, instructions, notices or other similar instruments made for the purposes of Schedule 4,
(d) the operator's policies, procedures and controls for the purposes of forestalling, preventing and detecting ML and FT: and
(e) the risks of breaching TFS and PF sanctions

12.28 In addition the operator must ensure that the ongoing training provided to relevant employees in accordance with Schedule 4 and this guidance also covers, as a minimum:

(a) the requirements for the internal and external disclosing of suspicion;

(b) the criminal and regulatory sanctions in place, both in respect of the liability of the operator and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the operator;

(c) the identity and responsibilities of the MLRO, MLCO and Nominated Officer;

(d) dealing with business relationships subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;

(e) those aspects of the operator's business deemed to pose the greatest ML and FT risks, together with the principal vulnerabilities of the products and services offered by the operator, including any new products, services or delivery channels and any technological developments;

(f) new developments in ML and FT, including information on current techniques, methods, trends and typologies;

(g) the operator's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;

(h) the identification and examination of unusual transactions or activity outside of that expected for a customer;

(i) the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related;

(j) the vulnerabilities of the operator to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs;

(k) UN, EU and other sanctions and the operator's controls to identify and handle natural persons and legal persons subject to sanction; and

(l) the risks of breaching TFS and PF sanctions

12.29 The list above is not exhaustive and there may be other areas that the operator deems it appropriate to include based on the business of the operator and the conclusions of its business risk assessments.

12.30 In accordance with Paragraph 11(1)(c) of Schedule 4, the operator shall also identify relevant employees who, in view of their particular responsibilities, should receive additional

and ongoing training, appropriate to their roles, in the matters set out above and it shall provide such additional training.

12.31 The paragraphs below set out those categories of relevant employee who are to be provided with additional training, together with the particular focus of the additional training provided. The categories below are not exhaustive and the operator may identify other relevant employees who it considers require additional training.

The Board and Senior Management

12.32 The board and senior management are responsible for ensuring that the operator has appropriate and effective policies, procedures and controls to counter the risk of ML and FT. In accordance with Paragraph 11(2)(c) of Schedule 4, the board and senior management must therefore be identified as relevant employees to whom additional training must be given in order that they remain competent to give adequate and informed consideration as to the effectiveness of those policies, procedures and controls.

12.33 The additional training provided to the board and senior management should include, at a minimum, a clear explanation and understanding of:

(a) Schedule 4, this guidance and the Relevant Enactments, including information on the offences and related penalties, including potential director and shareholder liability;
(b) the conducting and recording of ML and FT business risk assessments and the formulation of a risk appetite, together the establishment of appropriate, relevant and effective policies, procedures and controls; and
(c) methods to assess the effectiveness of the operator's systems and controls and its compliance with Schedule 4, this guidance and other Relevant Enactments.

The Money Laundering Reporting Officer and Nominated Officer

12.34 The MLRO and Nominated Officer are responsible for the handling of internal and external disclosures and are relevant employees to whom additional training must be given.

12.35 The additional training provided to the MLRO and Nominated Officer must include, at a minimum:

(a) the handling of internal disclosures of suspicious activity;
(b) the making of high quality external disclosures to the FIS;
(c) the handling of production and restraining orders including, but not limited to, the requirements of the Relevant Enactments and how to respond to court orders;
(d) liaising with the AGCC and law enforcement agencies; and
(e) the management of the risk of tipping off.

The Money Laundering Compliance Officer

12.36 The MLCO is responsible for monitoring and testing the effectiveness and appropriateness of the operator's policies, procedures and controls to counter the risk of ML and FT and is a relevant employee to whom additional training must be given.

12.37 The training provided to the MLCO must address the monitoring and testing of compliance systems and controls (including details of the operator's policies and procedures) in place to prevent and detect ML and FT.

Chapter 13

Record Keeping

Introduction

13.1 This chapter outlines the requirements of Schedule 4 and the AGCC Rules in relation to record keeping and provides guidance to the operator for the purpose of countering the threat of ML and FT.

13.2 Record keeping is an essential component required by Schedule 4 in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the appropriate authorities. If law enforcement agencies, either in the Bailiwick or elsewhere, are unable to trace criminal property due to inadequate record keeping, then prosecution for ML and FT and confiscation of criminal property may not be possible. Likewise, if the funds used to finance terrorist activity cannot be traced back through the financial system, then the sources and destinations of terrorist financing will not be identifiable.

13.3 Sound record keeping is also essential to facilitate effective supervision, allowing the AGCC to supervise compliance by the operator with its statutory obligations and regulatory requirements. For the operator, sound record keeping provides evidence of the work it has undertaken to comply with those statutory obligations and regulatory requirements, as well as allowing for it to make records available on a timely basis, i.e. promptly to domestic competent authorities pursuant to Schedule 4 or the Relevant Enactments and to auditors.

13.4 To ensure that the record keeping requirements of Schedule 4 and this guidance are met, the operator must have appropriate and effective policies, procedures and controls in place which require that records are prepared, kept for the stipulated period and in a readily retrievable form.

Relationship and Customer Records

13.5 In accordance with Paragraph 12(2) of Schedule 4, the operator shall keep:

(a) all transaction documents, relationship risk assessments, and any CDD information, or
(b) copies thereof,

for five years after the cessation of the customer relationship.

13.6 In order to meet the requirements of Paragraph 12(2) of Schedule 4 in relation to transaction documents and CDD information, the operator must keep the following records:

(a) copies of the identification data obtained to verify the identity of all customers, beneficial owners and other key principals (for example, copies of records of official identification documents such as passports, identity cards, driving licences or similar);
(b) copies of any relationship risk assessments carried out in accordance with Paragraph 2(5) of Schedule 4 and this guidance; and
(c) copies of any customer files, account files, business correspondence and information relating to the business relationship, including the results of any analysis undertaken (for example, inquiries to establish the background and purpose of complex, unusual or large transactions); or
(d) information as to where copies of the CDD information may be obtained.

13.7 In accordance with Paragraph 12 of Schedule 4, the minimum retention period in the case of any CDD information is:

(i) a period of five years starting from the date where the customer has established a business relationship with the operator, that relationship ceased, or
(ii) such other longer period as the Commission may direct.

Transaction Records

13.8 In accordance with Paragraph 12(2) of Schedule 4, the operator shall keep a comprehensive record of each transaction with a customer, including the amounts and types of currency involved in the transaction (if any); and such a record shall be referred to as a "transaction document".

13.9 In order to meet the requirements of Paragraph 12(1) of Schedule 4 to keep each transaction document, all transactions carried out on behalf of or with a customer in the course of business, both domestic and international, must be recorded by the operator. In every case, sufficient information must be recorded to permit the reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

13.10 The operator must ensure that, in order to meet the record keeping requirements for a transaction, documentation is maintained which must include:

(a) the name and address of the customer and beneficial owner;
(b) the amounts and types of currency involved in the transaction;
(c) the account name and number or other information by which it can be identified;
(d) details of the counterparty, including account details;
(e) the nature of the transaction; and
(f) the date of the transaction.

13.11 Records relating to unusual and complex transactions and high risk transactions must include the operator's own reviews of such transactions.

13.12 In accordance with Paragraph 12(2) of Schedule 4, the minimum retention period is, in the case of any transaction document –

(i) a period of five years starting from the date that the transaction and any related transaction were completed, or
(ii) such other longer period as the AGCC may direct.

13.13 In accordance with Paragraph 12(3) of Schedule 4, where the operator is required by any enactment, rule of law or court order to provide a transaction document or any CDD information to any person before the end of the minimum retention period, the operator shall –

(a) keep a copy of the transaction document or CDD information until the period has ended or the original is returned, whichever occurs first, and
(b) maintain a register of transaction documents and CDD information so provided.

Internal and External Disclosures

13.14 In accordance with Paragraph 12(4) of Schedule 4, the operator shall keep records of any internal disclosures made to the MLRO or a Nominated Officer and of any external disclosures made under Part I of the Disclosure Law or Section 15 or 15A, or Section 12 (as appropriate), of the Terrorism Law made other than by way of an internal disclosure to the MLRO.

13.15 In meeting the requirements of Paragraph 12(4) of Schedule 4 related to disclosures, the operator must keep:

(a) the internal disclosure and any supporting documents;
(b) records of actions taken under the internal and external reporting requirements;
(c) evidence of the enquiries made in relation to that internal disclosure;
(d) where the MLRO (or a Nominated Officer) has considered information or other material concerning possible ML and FT, but has not made an external disclosure to the FIS, a record of the other material that was considered and the reason for the decision; and
(e) where an external disclosure has been made to the FIS, evidence of the MLRO's (or Nominated Officer's) decision and copies of all relevant information passed to the FIS.

13.16 In addition to the above, the operator must maintain a register covering both internal disclosures and external disclosures made to the FIS and include the following as a minimum:

(a) the date the internal disclosure was received by the MLRO (or the Nominated Officer);
(b) the name of the person submitting the internal disclosure;
(c) the date of the disclosure to the FIS (if applicable);
(d) the name of the person who submitted the disclosure to the FIS (if applicable);
(e) the value of the transaction or activity subject to the disclosure (where available);
(f) a reference by which supporting evidence is identifiable; and
(g) the date(s) of any update(s) (additional information) submitted to the FIS.

13.17 In accordance with Paragraph 12(4) of Schedule 4, the minimum retention period for disclosures is five years starting from –

(a) in the case of an internal or external disclosure in relation to a business relationship, the date the business relationship ceased,
(b) in any other case, the event in respect of which the internal or external disclosure was made.

Training Records

13.18 In accordance with Paragraph 12(4)(c) of Schedule 4, the operator shall keep records of any training carried out under Paragraph 11 of Schedule 4 for five years starting from the date the training was carried out.

13.19 In order to meet the requirements of Paragraph 12(4)(c) of Schedule 4 to keep records of AML and CFT training undertaken, the operator must record the following as a minimum:

(a) the dates training was provided;
(b) the nature of the training; and
(c) the names of the employees who received the training.

13.20 Operators may also find it useful to maintain copies of the training delivered.

Business Risk Assessments

Policies, Procedures, Controls and Compliance Monitoring

13.21 In accordance with Paragraph 12(4)(d)-(e) of Schedule 4, the operator shall keep any minutes or other documents prepared pursuant to Paragraph 15(1) of Schedule 4, until –

(i) the expiry of a period of five years starting from the date they were finalised, or
(ii) they are superseded by later minutes or other documents prepared under that paragraph,

whichever occurs later, and its policies, procedures and controls which it is required to establish and maintain pursuant to Schedule 4, until the expiry of a period of five years starting from the date that they ceased to be operative.

13.22 In order to meet the requirements Paragraph 12(4)(d)-(e) of Schedule 4, the operator must retain:

(a) reports made by the MLRO and MLCO to the board and senior management;
(b) records or minutes of the board's consideration of those reports and of any action taken as a consequence; and
(c) any records made within the operator or by other parties in respect of the operator's compliance with Schedule 4 and this guidance.

Ready Retrieval

13.23 In accordance with Paragraph 12(5) of Schedule 4, documents and CDD information, including any copies thereof, kept in accordance with Schedule 4, may be kept in any manner or form, provided they are readily retrievable.

13.24 Periodically the operator must review the ease of retrieval, and condition, of paper and electronically retrievable records.

13.25 In accordance with Paragraph 12(5)(b) of Schedule 4, documents and CDD information, including any copies thereof, kept in accordance with Schedule 4, shall be made available promptly:

(i) to an auditor; and

(ii) to any police officer, the FIS, the AGCC, the MLRO, NO or any other person, where such documents or CDD information are requested pursuant to Schedule 4 or any of the Relevant Enactments or the Regulations.

13.26 The operator must consider the implications for meeting the requirements of Schedule 4 where documentation, data and information is held overseas or by third parties, such as under outsourcing arrangements.

13.27 The operator must not enter into outsourcing arrangements to retain records where access to those records is likely to be restricted.

13.28 Where the FIS or another domestic competent authority requires sight of records, either under Schedule 4 or another of the Relevant Enactments, which according to the applicable procedures would ordinarily have been destroyed, the operator must nonetheless conduct a search for those records and provide as much detail to the FIS or other domestic competent authority as possible.

Manner of Storage

13.29 The record keeping requirements are the same regardless of the format in which the records are kept, or whether the transaction or activity was undertaken by paper or electronic means.

13.30 Records may be retained:

(a) by way of original documents;

(b) by way of photocopies of original documents (certified where appropriate);

(c) on microfiche;

(d) in a scanned form; or

(e) in a computer or electronic form (including cloud storage).

13.31 The use of technology to collect and/or store data and documents does not alter the obligations and requirements described in this guidance.

13.32 Where the operator utilises an electronic method of gathering identification data, a CDD Utility, the operator should include within its risk assessment of that technology an evaluation of the policy for the retention of documents. This evaluation should enable the operator to ensure that its use of the technology complies with the requirements of Schedule 4 and this guidance and that the operator will not incur legal evidential difficulties (for example, in civil court proceedings).