Anti-Money Laundering and Counter-Terrorist Financing Policy

Approved by the Board of Directors

May 2020

CONFIDENTIAL

CONTENTS

1. About this Policy

1.1. Policy Statement

1.1.1. Playtech is committed to conducting its business in a lawful and ethical manner. Playtech takes a zero-tolerance approach to money laundering ('ML') and terrorist financing ('TF') and is committed to upholding all laws relevant to anti-money laundering and counter-terrorist financing ('AML/CTF') in all the jurisdictions in which Playtech operates.

1.1.2. ML and TF pose risks to Playtech's business. Playtech takes a measured approach to identify, assess and understand the ML and TF risks it is exposed to, and has established a tailored AML/CTF programme (the 'AML/CTF Programme') to manage and mitigate the risks it identifies.

1.1.3. Playtech's AML/CTF Programme is shaped by current applicable legislation, regulations and best-practice anti-money laundering standards ('Regulations' detailed in Appendix A) and has been tailored to effectively manage and mitigate the ML and TF risks Playtech is exposed to. It includes establishing Board-approved policies, appropriate procedures and implementing and enforcing effective systems and controls.

1.1.4. Not only will the effective implementation of Playtech's AML/CTF Programme help to counter ML and TF, it will help to protect Playtech, its employees, shareholders, customers and suppliers from the risks of ML and TF, maintain confidence in Playtech and provide for continued, successful business operations.

1.2. Purpose of this Policy

1.2.1. The purpose of this Policy is to:

- set out the responsibilities and obligations on Playtech, its directors, officers and employees ('Personnel') to observe and uphold AML/CTF measures; and
- provide information and guidance to personnel on how to recognise activities that may be related to ML and TF and instruct them on how to proceed in such cases.

1.3. Application of this Policy

1.3.1. This Policy applies to Playtech Plc and all of its subsidiaries ('Playtech Group'). 'Playtech' is used in this document to mean any entity in the Playtech Group.

1.3.2. This Policy applies to all persons working for, or on behalf of, Playtech in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers and interns ('Personnel'). Where appropriate, the Policy applies to agents, contractors, external consultants, third-party representatives, business partners, sponsors, or any other person associated with Playtech, wherever located.

1.3.3. From time to time Playtech will engage third party specialists to advise on ML and TF matters. This does not, however, absolve Personnel from their obligations and responsibilities in relation to ML and TF.

1.3.4. Where local AML/CTF laws and regulations apply in any country in which Playtech operates, those laws and regulations must be followed in addition to the requirements of this Policy. If any such local laws are not as strict as the terms of this Policy (including

the laws and regulations referenced in it), then the terms of this Policy must be applied to the extent permitted by local law.

1.3.5. Regulated entities within Playtech's Financial Division ('Tradetech Group') implement additional specific AML/CTF policies (detailed in Appendix C). Relevant employees of those entities shall follow and abide by these policies, which are amended from time to time.

1.3.6. Any breach of this Policy may result in disciplinary action, or the cessation of the business relationship as appropriate. Moreover, it may constitute a criminal offence under applicable laws which could result in prosecution.

1.3.7. This Policy does not form part of any employee's contract of employment and Playtech may amend it at any time.

1.4. Oversight of this Policy

1.4.1. Playtech has designated the Chair of the Risk Committee as the member of the board of directors and of its senior management to be responsible for compliance with all applicable laws relevant to countering ML and TF in all the jurisdictions in which Playtech operates.

1.4.2. Playtech's Risk and Compliance Committee has overall responsibility for ensuring this Policy complies with Playtech's legal and ethical obligations, and that all those under its control comply with it. The Risk and Compliance Committee is also responsible for approving this Policy, monitoring its effectiveness, raising risks to the Board of Directors and ensuring that appropriate actions are taken to mitigate such risks.

1.4.3. Playtech has appointed a Money Laundering Reporting Officer ('MLRO') and Deputy MLRO ('DMLRO') at group level. Additional MLROs have been appointed for certain Playtech entities. More detail on the appointment of the MLRO is set out in section 4.5.

1.4.4. The MLRO, or DMLRO in the MLRO's absence, has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective, amongst other things.

1.4.5. Management at all levels are responsible for ensuring those reporting to them understand and comply with this policy and are given adequate and regular training on it.

1.4.6. Personnel are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to Compliance.

1.4.7. Exceptions to this Policy are not permitted.

1.5. Related Documents

1.5.1. Appendix C lists all documents which relate to or reference this Policy.

1.6. Compliance Management

1.6.1. Playtech must monitor the use and effectiveness this Policy and its procedures, controls and systems to manage and mitigate the ML and TF risks it faces, and enhance them where necessary.

1.6.2. Playtech must implement an effective review process to evaluate the effectiveness of this Policy and its implementation.

1.6.3. Playtech must maintain this Policy so that its contents are relevant to the business, up-to-date and in compliance with current legislation and regulations.

1.6.4. Any risks of non-compliance must be escalated to senior management, who are responsible for mitigating such risks. Where appropriate, risks must be escalated to the Board of Directors.

2. Money Laundering

2.1. Money Laundering

2.1.1. ML can be defined as 'the process by which the proceeds of criminal activity are dealt with in a way to conceal or disguise their illicit criminal origins'. Typically, ML consists of three stages:

Placement: the physical disposal of criminal proceeds where the money launderer attempts to place cash into the financial system.

Layering: the separation of criminal proceeds from their source by the creation of 'layers' or a sequence of transactions designed to disguise the audit trail and provide the appearance of legitimacy.

Integration: the conversion of the criminal proceeds, for example, into real estate, property or investments, so that they appear to be legitimate funds or assets.

2.1.2. Criminal activity can include any kind of conduct that would be a criminal offence in the United Kingdom or any other country in which Playtech operate, including but not limited to terrorism, drug trafficking, activities of criminal organisations, corruption, fraud, theft and tax evasion or other tax related offences.

2.2. Examples of Money Laundering Risks in the Industry

2.2.1. There is the potential for a money launderer to use gambling at each of the above stages. For instance, in online gambling, where electronic transfers are required for placements, identity theft and identity fraud may enable a money launderer to move criminal proceeds with anonymity.

2.2.2. The use of multiple internet transactions may facilitate the layering stage of ML.

2.2.3. ML may also arise from simple criminal spend ('Proceeds of Crime').

2.2.4. Personnel may also facilitate ML by colluding with customers or other third parties, or dishonestly manipulating records or processes.

2.3. Money Laundering Offences

2.3.1. ML offences criminalise both the process of overt ML as well as the failure to report knowledge or suspicion of ML.

2.3.2. The offences described below are those that apply under UK law. Similar offences apply in other countries in which Playtech does business.

2.3.3. Primary offences

It is an offence to:

- conceal, disguise, convert or transfer the proceeds of crime or to remove the proceeds of crime from the jurisdiction of England and Wales;
- enter into, or become concerned in, an arrangement which you know or suspect facilitates the acquisition, retention, use or control of the proceeds of crime by another person; or
- acquire, use or possess proceeds of crime.

2.3.4. All three offences require either a knowledge or suspicion that the monies involved constitute the proceeds of crime.

2.4. Knowledge or Suspicion

2.4.1. Personnel must report any knowledge, suspicion or grounds for knowing or suspecting ML or TF to the MLRO.

2.4.2. 'Knowledge' here means having actual knowledge that the monies in question originated from criminal activity. For example, knowing that a customer is depositing monies received from the sale of drugs or monies obtained by deception.

2.4.3. Having a 'suspicion', on the other hand, is subject to a much lower threshold. The information causing suspicion of money laundering does not have to be clear, firmly grounded or targeted on specific facts. The suspicion need only be 'more than fanciful' in order for the requirement to report to arise and for the MLRO to consider making a report to the relevant authorities.

2.4.4. Having 'grounds for knowing or suspecting' ML or TF is an objective test that applies to Playtech as it operates in the regulated sector. If circumstances exist that would cause a reasonable person to know or suspect the existence of ML or TF, these should be reported to the MLRO, even if they do not, for whatever reason, cause the reporter personally to know or suspect ML or TF. For ease of reference throughout this Policy, reference is made to the requirement to report knowledge or suspicion of ML or TF. This should be taken to also include having grounds for knowing or suspecting.

2.5. Examples of Activities Which May Lead to Knowledge or Suspicion

2.5.1. A non-exhaustive list of examples of conduct which may raise suspicion of ML or TF are set out below.

2.5.1.1. The existence of such conduct does not necessarily mean that ML or TF is taking place; however, it does mean that greater scrutiny is required. In these circumstances, or if you have any other cause to know or suspect that ML or TF may be taking place, a report should be made to the MLRO so that they can take any further steps that may be required. Where there is any doubt, contact the MLRO.

2.5.1.2. Evidence is not required to report to the MLRO, suspicion is enough.

2.5.1.3. Business-to-business ('B2B') relationships:

- a potential customer is unwilling to provide due diligence documentation;
- a potential customer presents unusual, inconsistent or suspicious due diligence documentation;

- a potential customer is not willing to disclose its ultimate beneficial owner;
- a potential customer's financial resources do not appear to match those indicated in its reported figures;
- a potential customer wishes to use numerous entities when formulating an agreement;
- a customer pays a large sum of money to Playtech and requests it back for no valid, understandable reason;
- there is a mismatch between the customer's country of establishment and the location of their method of payment, such as their bank account.
- frequent changes of ownership in unusually short time periods, with no apparent business, economic or other legitimate reason and between related persons;
- a customer repeatedly changes lawyer or corporate service providers within a short period of time without any reasonable explanation; or
- a customer's documents are provided by an intermediary who has no apparent reason to be involved (the intermediary may be the real client).

2.5.1.4. Business-to-consumer ('B2C') relationships:

- a potential customer is reluctant to provide evidence to verify their identity;
- a customer, or potential customer, is reluctant to provide information in relation to their source of wealth or source of funds;
- a customer uses multiple credit cards to deposit money within a short period of time (which may suggest the use of stolen cards);
- a customer deposits a large sum of money and makes a request to withdraw it, having engaged in minimal or no gameplay;
- there is a mismatch between the customer's country of residence and the location of their method of payment, such as their bank or credit card account;
- where a customer uses one payment method to make a deposit and requests a withdrawal to be made to a different account;
- a customer engages in unusual or inconsistent gameplay activity; or
- a customer uses a number of anonymous payment methods, such as pre-paid cards.

3. Terrorist Financing

3.1. Terrorist Financing

3.1.1. TF means the provision or collection of funds or assets, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out terrorist activities.

3.2. Terrorist Financing Offences

3.2.1. It is an offence:

- to use or possess money or other property for the purposes of terrorist activity;
- to possess money or other property and intending that it should be used, or having reasonable cause to suspect that it may be used, for the purposes of terrorist activity;
- to enter into, or become concerned in, an arrangement as a result of which money or other property is made available, or is to be made available, to another if you know or have reasonable cause to suspect that the money or other property will, or may, be used for the purposes of terrorist activity;
- enter into, or become concerned in, an arrangement which facilitates the retention or control, by, or on behalf of, another person, of terrorist property (being money or other property likely to be used for the purposes of terrorism) in the following ways:
  - by concealment;
  - by removal from the jurisdiction;
  - by transfer to nominees; or
  - in any other way.

3.2.2. It is a defence for a person charged with this offence to prove that they did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

3.2.3. Other offences

3.2.4. It is an offence to know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in a TF offence and to fail to disclose that knowledge or suspicion to the nominated officers (MLRO and/or DMLRO).

3.3. Examples of Terrorist Financing Risks in the Industry

3.3.1. Terrorist organisations may make use of the online gambling industry to assist in obtaining the funds required for them to plan and carry out attacks, train militants, pay their operatives and promote their ideologies.

3.3.2. Non-exhaustive examples of conduct which may raise suspicion of TF are set out below.

- the parties to the transaction (beneficial owners or directors) are from countries known to support terrorist activities and organisations;

- use of false corporations, including shell-companies;
- inclusion of the individual or entity in the sanctions lists;
- media reports that the account holder is linked to known terrorist organisations or is engaged in terrorism;
- the use of funds by the organisation is not consistent with the purpose for which it was established;
- the transaction is not economically justified considering the account holder's business or profession;
- a series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds;
- transactions which are inconsistent with the account's normal activity;
- deposits structured to avoid detection;
- multiple cash deposits and withdrawals with suspicious references; or
- use of multiple foreign bank accounts.

4. Playtech's Obligations

4.1. Obligations

4.1.1. Playtech operates in the gambling and financial services industries, both of which are vulnerable to ML and TF risks.

4.1.2. Playtech, as a regulated business, is subject to AML/CTF regulations and must identify, assess and understand the ML and TF risks it is exposed to, and establish a tailored AML/CTF Programme to manage and mitigate the risks it identifies.

4.1.3. Playtech must not commit, or assist others in committing, any ML or TF offences.

4.1.4. Playtech must comply with its obligations under the applicable AML/CTF regulations. They include, but are not limited to:

- carrying out an annual risk assessment;
- establishing appropriate policies and procedures;
- conducting relevant Compliance training for its Personnel;
- appointing an MLRO; and
- implementing internal controls.

These obligations are set out in detail in the following sections.

4.1.5. Playtech must ensure that it has appropriate procedures in place to ensure that employees who report breaches to the MLRO or externally to the relevant authority are protected from exposure to threats or hostile action and, in particular, from adverse or discriminatory employment actions.

4.1.6. In the event that a person subject to this Policy breaches it, or commits an ML or TF offence, Playtech must take appropriate action.

4.2. Risk Assessment

4.2.1. Playtech must carry out an annual risk-assessment to identify, assess and understand the ML and TF risks its business faces. Taking into account the nature and size of the business, the risk assessment must, among other things:

- take into account information made available by the Gambling Commission or other relevant supervisory authorities;
- assess risk factors related to:
  - governance
  - customers;
  - countries or geographic areas in which it operates;
  - employees;
  - products or services; and
  - payments.

4.2.2. Playtech must keep an up-to-date record in writing of the steps it has taken in its risk assessment. Appendix C details Playtech's risk assessment, which is reviewed annually and updated from time to time as necessary.

4.3. Policies and Procedures

4.3.1. Playtech must establish and maintain appropriate group-wide policies and procedures and implement and enforce effective internal systems and controls to manage and mitigate ML and TF risks effectively. They must be approved by senior management and be proportionate to the nature and size of Playtech's business.

4.3.2. Playtech must regularly review and update where necessary the policies, controls and procedures.

4.3.3. Playtech must maintain a written record of:

- the policies, controls and procedures established;
- any changes to those policies, controls and procedures made as a result of the regular reviews completed; and
- the steps taken to communicate those policies, controls and procedures, or any changes to them.

4.4. Training and Awareness

4.4.1. All Personnel must be aware of their obligations and responsibilities relating to ML and TF.

4.4.2. All employees must be aware of who the current MLRO and DMLRO is.

4.4.3. Relevant employees (as defined in section 6.3.1) must undergo annual AML/CTF training. This includes, but is not limited to Commercial Directors, Sales Managers, the Board of Directors, VIP Customer Managers, Personal Management Licence Holders, Compliance, Finance and HR.

4.4.4. AML/CTF training will be conducted face-to-face or online as appropriate and as part of broader compliance training.

4.4.5. Personnel must demonstrate that they have understood the requirements of this Policy. This will be assessed by a short online competency test. The test must be passed with 80% competency, failing which it must be retaken.

4.4.6. Playtech must maintain a written record of all training provided and awareness measures taken.

4.5. Money Laundering Reporting Officers

4.5.1. Playtech must appoint a nominated officer, known as the MLRO, for each entity in the Group which is subject to the Regulations. Playtech's MLRO is appointed at Group level and holds the role of MLRO for each Group entity, subject to certain exceptions, which must be expressly agreed by the Group MLRO. Selection of the MLRO is dependent on the individual:

4.5.1.1. having sufficient level of seniority within Playtech;

4.5.1.2. being free to act on his or her own authority; and

4.5.1.3. having sufficient resources to carry out the function.

4.5.1.4. Details of the appointed MLRO are provided.

4.5.2. The MLRO has responsibility for, among other things:

- receiving reports of suspicious activity from any employee or other person to whom this Policy applies;
- considering all reports and evaluating whether there is any knowledge, suspicion or grounds to suspect ML or TF;
- reporting any suspicious activity or transaction to the National Crime Agency ('NCA') by completing and submitting a Suspicious Activity Report;
- asking the NCA for consent to proceed, where appropriate, in relation to reported transactions and making sure that no transactions are continued illegally;
- promptly responding to any reasonable requests for information made by the NCA;
- implementing this policy, monitoring its use and effectiveness and dealing with any queries about it; and
- auditing internal control systems and procedures to ensure they are effective.

4.5.3. The MLRO has appointed a DMLRO to support the implementation of the Policy and serve as a delegate in the event the event that the MLRO is absent.

4.5.4. The MLRO may engage the assistance of other suitably qualified individuals within Playtech regulated group companies in complying with his/her responsibilities, but ultimate responsibility and accountability remains, at all times, with the MLRO.

5. Personnel Obligations

5.1. Primary Obligations

5.1.1. Personnel must be aware of and understand ML and TF, the offences related to ML and TF, and their responsibilities and obligations that arise from the ML and TF legislation.

5.1.2. Personnel must not commit, or assist others in committing, any ML or TF offences.

5.2. Reporting Obligations

5.2.1. Personnel who know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in an offence of ML or TF, must disclose this to the MLRO immediately. All initial reporting should be in person or by telephone where possible. Personnel may also fill out an Internal Report Form, which is available on the company intranet.

5.2.2. Personnel must follow the instruction of Playtech's MLRO on what, if any, further action to take following a report. They must not attempt to carry out an investigation. However, as a minimum:

- if the transaction or matter you are concerned about is not complete, you must not proceed with it unless advised to do so by the MLRO; and
- if the transaction or matter you are concerned about has been completed, you must still report it to the MLRO immediately.

5.2.3. Personnel must not 'tip off' the customer or other party concerned or any third party that:

- a report has been made to the MLRO;
- the MLRO has made a SAR (see below) to the authorities;
- an investigation is in contemplation or is underway; or
- a transaction is being delayed, whilst consent to proceed is being sought from the authorities.

5.2.4. Personnel who believe that they have suffered detrimental treatment (including dismissal, disciplinary action, threats or other unfavourable treatment) as a result of reporting suspected ML or TF should disclose this to the Chief Compliance Officer, General Counsel or an HR focal point, or raise it confidentially via the 'Speak Up' Line (see Playtech's Speak Up Policy).

5.3. Reporting by the MLRO/DMLRO

5.3.1. Playtech's MLRO must consider the matter disclosed to them, along with any other relevant information available to them, to decide whether or not a disclosure needs to be made to the relevant authorities (known as a 'Suspicious Activity Report' or 'SAR').

5.3.2. If Playtech's MLRO decides that it is appropriate to report the matter, it must be reported to the relevant authority as soon as practicable.

5.3.3. Playtech's MLRO must record their decision to report or not to report and the reasons for their decision in writing, attaching any supporting documentation.

5.3.4. If a report is made, Playtech's MLRO must act in accordance with the relevant authority's instructions.

5.3.5. In evaluating and determining whether to submit a SAR, the MLRO will consider, among other things:

- details of the grounds for knowledge or suspicion of ML/TF;
- any information in Playtech's possession that could be relevant, including customer due diligence information, knowledge of other parties involved and, where possible, whether the transactions concerned are in line with the relevant account's past activity, its purpose, profile, or normal course of business;
- any information in the public domain that could be relevant, including negative news, political exposure, exposure to sanctions or the existence of prior investigations, etc.; and
- further information obtained from the customer, if necessary. Any approach to the customer should be made sensitively and probably by someone already known to the customer, to minimise the risk of alerting the customer, or an intermediary, that a disclosure to the relevant authority is being considered.

6. Internal Controls

6.1. Customer Due Diligence Obligations

6.1.1. Customer due diligence obligations

6.1.1.1. Playtech has implemented customer due diligence ('CDD') processes which are appropriate, proportionate to the nature and size of its business and tailored to its various business activities. Appendix C references the current procedures in place.

6.1.1.2. Playtech carries out CDD on all customers (B2C and B2B) to mitigate the risks of ML and TF. CDD is the process of obtaining information to know your customer. It can include simplified due diligence ('SDD') measures or enhanced due diligence measures ('EDD').

6.1.1.3. Playtech must assess whether to apply SDD or EDD on a risk-sensitive basis, taking into account a non-exhaustive list of factors, including the purpose of an account or relationship, the level of assets to be deposited by a customer or the size of transactions undertaken, the regularity or duration of the business relationship and geography. The type of CDD completed will differ between our B2C and B2B customers.

6.1.1.4. Playtech's full SDD and EDD procedures are set out in its Due Diligence Procedures (see Appendix C).

6.1.2. Requirement to carry out CDD

6.1.2.1. SDD must be carried out:

- prior to establishing a business relationship, which is:
  - for a B2B relationship, when a customer agrees Heads of terms with Playtech;
  - for a B2C relationship between a casino operator and a customer ('Player'), when a Player opens an account with a Playtech-operated online casino;
- when there is any suspicion of ML or TF;
- in relation to B2B customers, prior to carrying out an occasional transaction that either:
  - amounts to €15,000 or more when the transaction is carried out in a single operation or in several operations that appear to be linked, or
  - constitutes a transfer of funds exceeding €1,000;
- in relation to B2C customers, prior to carrying out any transaction (i.e. the wagering of a stake or collection of winnings) that amounts to EUR2,000 or more whether the transaction is executed in a single operation or in several operations which appear to be linked (e.g. if carried out through a single period of being logged in to Playtech gambling facilities);
- when there are doubts about the veracity or adequacy of previously obtained customer identification data; and/or
- for existing customers on a risk-sensitive basis, including when a customer's relevant circumstances change.

6.1.3. EDD includes both standard due diligence measures and additional due diligence measures (both of which are set out in section 6.1.4 below). It must be applied:

- in any case where Playtech considers there is a high risk of ML or TF. Factors to be considered when assessing whether there is a high risk of ML or TF are set out in Appendix D. For example, where the business relationship involves a non-face-to-face consumer (as in the case of remote casinos) and there are no additional safeguards in place, such as electronic signatures, the relationship must be considered to present a high risk of ML and TF;
- in any business relationship or transaction involving a high-risk third country (see Appendix C);
- if a customer or potential customer is a Politically Exposed Person ('PEP') (see further below), or a family member or known close associate of a PEP;
- in any case where a customer is suspected to have provided false or stolen identification documentation or information and Playtech proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose; and/or
- in any other case which, by its nature, can present a higher risk of ML or TF.

6.1.4. Simplified due diligence

6.1.4.1. SDD measures include:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source e.g. original, certified or notarized documentation and documents issued by an official body (see section 6.1.7 for further detail);
- identifying the beneficial owner of a corporate customer and taking reasonable measures to verify their identity so that Playtech is satisfied that it knows who the beneficial owner is (see section 6.1.6 for further detail);
- verifying that any person purporting to act on behalf of the customer (such as an agent) is authorised to do so, and identifying and verifying the identity of that person;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- assessing and, as appropriate, obtaining information on the customer's source of funds and source of wealth; and
- conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with Playtech's knowledge of the customer, the customer's business and risk profile (including where necessary the source of funds) and ensuring that the documents, data or information held are kept up-to-date.

6.1.5. Enhanced due diligence

6.1.5.1. EDD measures include SDD (as above) and:

- specific controls for business relationships or transactions involving high-risk third countries;

- seeking additional independent, reliable sources to verify information provided or made available to us;
- gathering further information about the customer to better understand the nature of the customer's business or their financial situation, and to determine the customer's reputation from publicly available information;
- examining the background and purpose of the transaction, as far as reasonably possible, and taking steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;
- taking adequate measures to establish the source of wealth and source of funds that are involved in the business relationships or transactions with the customer;
- assessing a corporate customer's AML/CTF controls;
- increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious; and
- obtaining approval from MLRO before establishing or continuing a business relationship.

6.1.6. Beneficial ownership

6.1.6.1. A 'beneficial owner' is defined for the purposes of this policy as any individual who: (i) exercises ultimate control over the management of the body corporate; (ii) who ultimately owns or controls (in each case whether directly or indirectly), more than 10% of the shares or voting rights in the body corporate; (iii) who holds the right, directly or indirectly to appoint or remove a majority of the board of directors; or (iv) has the right to exercise, or actually exercises, significant influence or control over the body corporate.

6.1.6.2. Where it is not possible to identify the beneficial owner of a body corporate after taking all necessary reasonable measures, Playtech will verify the identity of the senior managing official.

6.1.6.3. The 10% threshold stated here applies without prejudice to the right of Playtech to decide that a lower percentage may be indicative of ownership and control in relation to any particular customer.

6.1.7. Identification and verification

6.1.7.1. Identification of a customer means being told or coming to know of the customer's identifying details, such as their name and address.

6.1.7.2. Verification means proving a customer is who they claim to be, by obtaining and validating documents or information which supports this claim of identity. Identification and verification differ for B2B and B2C relationships.

6.1.7.3. Playtech's identification and verificiation procedures are set out in its Due Diligence Procedures (see Appendix C).

6.1.8. Timing of verification

6.1.8.1. Playtech requires CDD to be satisfactorily complete before a business relationship can be established or a financial transaction carried out. There is one exception: provided that the verification is completed 'as soon as practicable' after contact is first

established, verification of identity of a customer may be completed during the establishment of the business relationship where:

- this is necessary to avoid interrupting the normal conduct of business; and
- and there is little risk of ML and TF occurring.

6.1.8.2. The MLRO must give approval for this exception to be relied on.

6.1.9. Requirements to cease transactions or terminate relationship

6.1.9.1. Where CDD cannot be completed as required under this Policy, Playtech:

- must not carry out any transaction through a bank account with the customer or on behalf of the customer;
- must not establish a business relationship or carry out a transaction with the customer otherwise than through a bank account;
- must terminate any existing business relationship with the customer; and
- must consider whether a ML or TF report should be made to the relevant authorities.

6.1.9.2. Where the circumstances are suspicious, the procedure for reporting of suspicion in section 5.2 should be followed.

6.1.9.3. See Playtech's Due Diligence Procedures for its procedures for terminating a business relationship (see Appendix C).

6.1.9.4. To avoid potentially committing one of the principal ML offences, Playtech also needs to consider ending the business relationship with a customer in the following circumstances:

- where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spend;
- where the risks of ML or TF are considered to be too high;
- where the Player's gambling activity leads to an increasing level of suspicion, or actual knowledge of ML; or
- where the customer is proven to a reasonable degree of confidence to not be the identity they claim to be.

6.1.10. Ongoing monitoring

6.1.10.1. Playtech must, on a risk-sensitive, ongoing, basis, scrutinise transactions undertaken throughout the course of the relationship with the customer (including, where necessary, the source of funds) to ensure that the transactions are consistent with its knowledge of the customer, the customer's activities and risk profile.

6.1.10.2. Playtech must also undertake reviews of existing records and keep the documents or information obtained for the purposes of applying CDD up to date.

6.1.10.3. Particular regard should be had to transactions that are complex, large and unusual or part of an unusual pattern, or concern customers identified as 'high risk'. Further triggers are set out in Playtech's Due Diligence Procedures (see Appendix C).

6.1.11. Record keeping

6.1.11.1. Playtech must keep records of the actions taken to complete CDD, as well as any difficulties encountered during the verification process. All CDD records must be kept

confidential. Playtech must keep all documentation, data and information held for the purpose of identifying the customer up to date. This means that CDD must be reviewed annually, or at any such other time that there is a change in a customer's circumstances. See also section 6.1.10.

6.2. Politically Exposed Persons

6.2.1. Playtech must have in place appropriate controls, including risk-based procedures, to determine whether a customer or beneficial owner of a customer is a politically exposed person ('PEP', as defined below) and to manage the enhanced risks arising from the relevant person's business relationship or transactions with such a customer.

6.2.2. Playtech's controls and procedures include:

- checking the identity of customers against politically exposed person PEP, sanctions and enforcement lists. For players, this function is provided electronically by an external third-party provider;
- where a potential or existing player is identified by electronic identification verification as a PEP, or as being on a sanctions list, the player details are sent to Playtech's Compliance Team to confirm the match;
- EDD must be undertaken for any customer identified as a PEP, or potential PEP. In particular the source of any funds or wealth of the customer must be established; and
- if a match is confirmed the account is placed under constant monitoring and sent to the MLRO for account registration approval or, in the case of existing customers, the continuance of the relationship.

6.2.3. A PEP is an individual (domestic or international) who has been entrusted within the last year with one of the following prominent functions by a state or an international body. Excluding middle-ranking or more junior officials, it includes:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament, or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts, or of other judicial bodies whose decisions are not subject to further appeal except in exceptional circumstances;
- members of Courts of Auditors, or of the boards of central banks;
- ambassadors and charges d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises;
- directors, deputy directors and members of the board, or other equivalent function of, an international organisation; and
- where an executive director, senior officer, trustee, partner, guardian, or other individual who has executive or effective control of the customer, is a PEP (this does not include non-executive directors or other persons in non-executive positions and only applies to corporate customers).

6.2.4. It also includes:

- family members of a PEP - spouse, civil partner, children and their spouses or civil partners, and parents; and
- known close associates of a PEP - persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of a PEP.

6.3. Personnel Measures

6.3.1. Personnel can pose an ML or TF risk. Playtech must carry out background screening on relevant Personnel prior to the commencement of their employment, or contract, including address and reference checks. Personnel screening means the assessment of:

- the skills, knowledge and expertise of the individual to carry out their functions effectively; and
- the conduct and integrity of the individual.

6.3.2. Relevant employees who will be subject to screening are those in positions where their work is:

- relevant to Playtech's compliance with any of its ML and TF obligations; or
- otherwise capable of contributing to the identification or mitigation of the risks of ML or TF, or the prevention or detection of ML or TF.

6.3.3. Playtech must carry out enhanced background screening on senior management and employees in positions deemed to be at greater risk of being exposed to ML or TF, including VIP customer managers and Personal Management Licence Holders.

6.3.4. Personnel must not hold accounts with any Playtech white-label sites unless approved by senior management and only for testing or business purposes. Screening is conducted prior to commencement of employment to ensure that no unauthorised accounts are held, and any accounts found are closed.

6.4. Internal Audit

6.4.1. Playtech has an independent audit function with the responsibility:

- to examine and evaluate the adequacy and effectiveness of the AML/CTF policies, controls and procedures adopted;
- to make recommendations in relation to those policies, controls and procedures; and
- to monitor Playtech's compliance with those recommendations.

6.5. Contractual Language

6.5.1. Playtech will include in its contracts with its business partners an obligation on the parties to the contract that they will comply with the relevant AML/CTF laws and regulations.

6.6. Record-keeping

6.6.1. Playtech must retain a copy of the documents and information necessary in order to comply with its CDD obligations, and any supporting evidence or records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after either:

- the end of the business relationship with the customer; or
- the date of an occasional transaction.

6.6.2. In accordance with data protection legislation, on expiry of the five-year retention period, personal data must be deleted, unless otherwise provided for by law, which determines the circumstances under which data can further be retained.

6.6.3. The records maintained must be sufficient to allow a competent third party to assess the effectiveness of Playtech's AML/CTF policies and procedures, including transaction records, due diligence information, suspicious transaction reports, and AML/CTF training records.

APPENDIX A - UK LEGISLATION, REGULATIONS AND GUIDANCE

Playtech abides by all laws and regulations relating to AML/CTF in the jurisdictions in which it operates. For the purpose of this Policy, UK laws are used for reference:

- The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (SI 2019 No. 1511)
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017 No. 692)
- The Proceeds of Crime Act 2002 (as amended by the Crime and Courts Act 2013 and the Serious Crime Act 2015)
- The Terrorism Act 2000 (as amended by the Anti-Terrorist, Crime and Security Act 2001, the Terrorist Act 2006 and the Terrorist Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007).
- European Union Fourth Anti-Money Laundering Directive
- European Union Fifth Anti-Money Laundering Directive
- Financial Action Task Force ('FATF') Forty Recommendations
- UK Gambling Commission, 'The prevention of money laundering and combating the financing of terrorism Guidance for remote and non-remote casinos' Fifth edition, January 2020
- Criminal Finances Act 2017

APPENDIX B - RELATED DOCUMENTS

- Playtech Risk Assessment
- Playtech Business-to-Business Due Diligence Procedure
- Business-to-Consumer Customer Risk Process
- Playtech High-risk Countries
- Tradetech Alpha Anti-money Laundering and Counter-terrorist Financing Policy
- CFH Clearning Anti-money Laundering and Counter-terrorist Financing Policy
- Safecap and Magnasale Anti-money Laundering and Counter-terrorist Financing Policy
- Playtech Speak Up Policy
- Playtech Business Ethics Policy

APPENDIX C - DETERMINING A HIGH RISK OF MONEY LAUNDERING

Factors to be considered when assessing whether there is high risk of ML or TF include whether:

- the business relationship is conducted in unusual circumstances;
- a business relationship or transaction involves a high-risk third country;
- the customer is resident in a geographical area of high risk;
- the product or transaction might favour anonymity;
- the situation involves non-face-to-face business relationships or transactions (as in the case of remote casinos), without certain safeguards, such as electronic signatures;
- payments will be received from unknown or unassociated third parties of the customer;
- new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new product;
- the business relationship or transaction involves countries:
    - identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
    - identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs, or subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations;
    - providing funding or support for terrorism;
    - that have organisations operating within their territory which have been designated, by the government of the UK, as proscribed organisations under the Terrorist Act or, by other countries, international organisations or the European Union as terrorist organisations; or
    - identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organisation for Economic Cooperation and Development or other international bodies or non-governmental organisations) as not implementing requirements to counter money laundering and terrorist financing that are consistent with the FATF recommendations.
- the customer transacts with significant amounts of cash;
- the customer provides false, forged or stolen identification documentation upon establishing a business relationship;
- the customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas;
- the product, service or transaction involves peer-to-peer gaming;
- the product is electronic roulette; and

- the product, service or transaction involves Ticket In/Ticket Out (TITO) or similar technology.