



UK Licencing

Anti-Money Laundering/ Prevention of Terrorist Financing Manual

BetIndex Limited
Charter Place
23-27 Seaton Place
St Helier
Jersey
JE1 1JY
Telephone 0162 682218

1 Contents

1	CONTENTS	2
2	INTRODUCTION	4
2.1	Background and Approach	4
2.1.1	Objective	4
2.2	Policy	4
2.2.1	Procedures will be maintained to ensure the following:	5
2.2.2	Responsibilities	5
2.2.3	Provision of Education and Training	6
2.3	Regime and Culture	6
2.3.1	Importance of compliance culture	6
2.3.2	Review of effectiveness	7
3	RISK ASSESSMENT	8
3.1	Risk Assessment	8
3.1.1	Nature of Participants	8
3.1.2	Status of Participants	8
3.1.3	Location of Participants	9
3.1.4	Amount of funds being transacted	9
3.1.5	Nature and frequency of transactions	9
3.2	Summary of factors and considered associated risk:	10
3.2.1	Review of Risk Assessment	10
4	POLICY AND PROCEDURES	11
4.1	Identification	11
4.1.1	General:	11
4.1.2	Anonymous Accounts	12
4.1.3	Evidence of identity for participants	12
4.1.4	Evidence of identity for business participants	13
4.1.5	Enhanced Participant due diligence	14
4.1.6	On-going Monitoring of transactions	15
4.2	Record keeping and retrieval of records	17
4.2.1	Record of Transactions	17
4.2.2	Retention of Records	17
4.2.3	Nominated Officer	18
4.2.4	Register of Money Laundering enquiries and reports	18
4.3	Internal procedures including the reporting of suspicious transactions, both internal and external	20
4.3.1	Internal suspicious activity reporting	20
4.3.2	Reporting and “active” business	20

4.3.3	External suspicious activity reporting	21
4.3.4	Whistleblowing Policy	21
4.4	Staff education, training and development	22
4.4.1	Importance for AML/PTF risks	22
4.4.2	The importance of staff in ML prevention	22
4.4.3	Human Resources risk factors in ML prevention	22
4.4.4	Integrity	22
4.4.5	Staff Recruitment	22
4.4.6	Staff Knowledge, Training and Awareness	23
4.4.7	Continuing Personal Development (“CPD”)	23
4.4.8	Staff promotion and transfer	24
4.5	Technological Developments	24
5	PROCEEDINGS	25
5.1	Offences	25
6	APPENDICES	26
6.1	Appendix A – Suspicious Transaction Report	26

All rights reserved. The information contained in this Manual is confidential and the intellectual property of BetIndex Limited (“the Company”) and for use during the course of employment with the Company or other companies within the same group. It may not be relied upon by, or in closed or circulated to, any other person or for any other purpose without the prior written consent of the Company.

©

2 Introduction

2.1 Background and Approach

2.1.1 Objective

The objective of this manual is:

A high level assessment of the operations and services provided by BetIndex Limited and the risks that they may facilitate money laundering or the financing of terrorism

To set out the policies, procedures, systems and controls necessary for BetIndex Limited to meet its obligations

BetIndex Limited's approach is based upon:

- Gambling Act 2005
- Proceeds of Crime Act 2002
- Terrorism Act 2006
- Gambling (Licensing and Advertising) Act 2014
- Gambling Commission's guidance on the prevention of money laundering and combating the financing of terrorism

Together referred to as "the codes" in relation to the detection and prevention of money laundering and terrorist financing.

The procedures that are appropriate for the purpose of forestalling and preventing money laundering include:

- Identification
- Record keeping
- Internal procedures including the reporting of suspicious transactions, both internal and external
- Staff education, training and development

BetIndex Limited is required to assess its Anti-Money Laundering (AML) / Prevention of Terrorist Financing (PTF) risks and implement appropriate measures in respect of the above based on its assessment. This manual sets out how management achieve this.

2.2 Policy

It is BetIndex Limited's policy that UK statutory and regulatory obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

Positive management action will be exercised in order to minimise the risk of the company's services and gaming activities being abused for the purposes of laundering funds associated with criminal activity, as defined by the relevant UK legislation.

BetIndex Limited will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Joint Financial Crimes Unit (JFCU) of the Jersey Constabulary and thereafter shall be undertaken in conjunction with the relevant Jersey authorities and in accordance with Jersey custom and practice to avoid any risk of BetIndex Limited committing a tipping-off offence.

The company's vigilance, policy and procedures will be based upon the regulations referred to above and associated guidance issued by the UK Gambling Commission.

2.2.1 Procedures will be maintained to ensure the following:

- All persons conducting business with the company are properly identified, that their identity is verified where appropriate and sufficient information is gathered and recorded to permit the company to "know its client" and predict the expected pattern of business.
- Potential new participants that do not appear to be legitimate are declined and where there is suspicion relating to criminal conduct on the part of a declined participant such suspicion is reported to the Nominated Officer. Established participants activities are regularly monitored to ensure that they fit the customer's profile, especially in respect of large or abnormal transactions.
- Records are retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- All suspicions are reported promptly to the Nominated Officer.
- Full co-operation is provided to the law enforcement authorities to the extent required by statute/regulation
- That the company's vigilance systems are implemented and regularly monitored.

2.2.2 Responsibilities

BetIndex Limited's Senior Management is responsible for:

- The day to day compliance with anti-money laundering obligations within the areas of the company for which they are responsible.
- Ensuring that the Nominated Officer is provided with prompt advice of unusual/suspicious transactions and other matters of significance.
- Providing the Nominated Officer with the appropriate resources to fulfil the function effectively.
- Ensuring that the Nominated Officer has complete autonomy in the suspicious activity report evaluation process and unfettered access to information necessary to carry out that process.

- The Directors and Nominated Officer will ensure that he/she is provided with or has access to the necessary resources to keep up to date with new money laundering requirements and developments.

The Nominated Officer is responsible for:

- Developing necessary policies, procedures, training and education of staff.
- Developing and maintaining policy in line with evolving statutory and regulatory obligations and experience/advice from enforcement agencies.
- Representing the company to all external agencies and any other third party making enquiries in relation to money laundering prevention or compliance.
- Ensuring that all parts of the company are complying with the stated policy and therefore monitoring operations and development of the policy to this end.
- Receiving internal disclosures under part 7 of POCA and part III of the Terrorism Act.
- Deciding whether these should be reported to the Jersey JFCU in line with the provisions of the Egmont Group.
- If appropriate, making such external reports.
- Ensuring that appropriate consent is applied as necessary.

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering.
- Reporting to the Nominated Officer all knowledge or suspicions of money laundering.
- Complying fully with all money laundering procedures in respect of client identification, client monitoring, record keeping, vigilance and reporting.

2.2.3 Provision of Education and Training

All members of management and staff will receive initial training and on-going training as and when required.

2.3 Regime and Culture

2.3.1 Importance of compliance culture

Detailed and comprehensive policy and procedures are not sufficient to forestall the facilitation of money laundering. If the culture of an organisation is to circumvent or ignore the rules then they will be ineffective.

It is the policy of the company's directors and senior management to encourage a compliance culture by:

- Demonstrating support for compliance with these procedures and with sound corporate ethics
- Providing support for staff in their AML/PTF efforts
- Demonstrating support for the Nominated Officer
- Demonstrating no tolerance of clients and other external parties who are not transparent or are not cooperative in AML/PTF efforts
- Encouraging risk awareness in staff

- Encouraging a spirit of compliance
- Fostering awareness through training
- Setting remuneration and reward packages appropriately
- Taking appropriate action in respect of breaches
- Encouraging the raising of concerns by staff at all levels
- Providing the necessary resources for proper application of procedures and to address concerns

2.3.2 Review of effectiveness

Management will review and assess the culture within the company and the effect of human factors on the effectiveness of procedures as part of its risk review.

3 Risk Assessment

3.1 Risk Assessment

BetIndex Limited has to consider the AML/PTF risks associated with its service offering and adopt a risk based approach when considering the requirements for:

- Identity of participants
- Evidence of identity
- Enhanced participant due diligence

The business undertaken by the company and management's assessment of its inherent money laundering/terrorist financing risk has been considered as follows:

The major factors that may highlight increased or decreased potential risk are considered to be:

3.1.1 Nature of Participants

Business Participants are considered by the company to represent a greater risk to the company from an AML/PTF risk, than an individual participant.

It is management's considered view that a Business Participant transacting with the company in what may be considered a normal manner represents only a minimal enhanced risk of money laundering or terrorist financing.

Nevertheless, the risk is enhanced and as such, satisfactory evidence of the nature and identity of the Business Participant is considered by Management to be essential prior to the business relationship being entered into. This is considered in Section 4.1.5 later.

3.1.2 Status of Participants

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting. However, it is management's considered view that a PEP transacting with the company in what may be considered a normal manner represents only a minimal enhanced risk of money laundering or terrorist financing.

3.1.3 Location of Participants

A participant located in a jurisdiction which is not Financial Action Task Force (FATF) compliant, may generally be considered to represent a potential risk of money laundering or terrorist financing activity. However, it is management's considered opinion that an individual transacting with the company in what may be considered a normal manner, but from such a territory, represents only a minimal enhanced risk of money laundering or terrorist financing.

Whilst the above factors are considered when determining the identification requirements at registration, Management considers that other factors, when combined with the above, create heightened risk of on-going money laundering or terrorist financing activity. These contributory factors include but are not limited to:

- Amount of funds being transacted
- Nature and frequency of transactions

In order to determine the participant risk, these factors will be considered on a case by case basis.

3.1.4 Amount of funds being transacted

If funds paid or staked by the participant are over Euros 2,000 or aggregate in excess of Euros 2,000 (or currency equivalent) in any 24 hour period (Threshold), there is an enhanced risk of money laundering or terrorist financing activities and additional identity checks are undertaken (see 4.1.3).

On its own, the risk associated with large deposits may not be overly significant. However, when combined with irregular or unusual account activity or with the PEP status or location of the participant, the risk may be significantly enhanced.

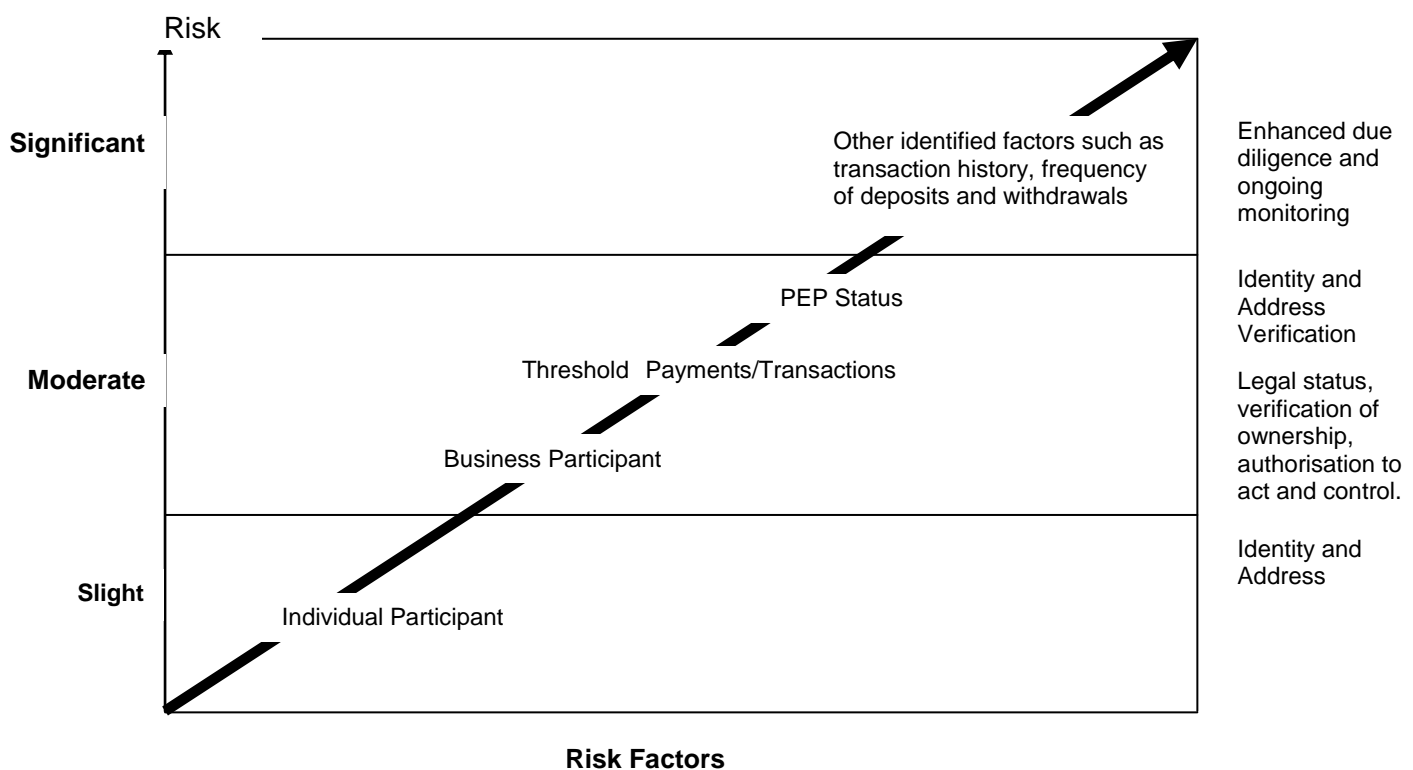
3.1.5 Nature and frequency of transactions

Where an individual is making regular deposits and betting transactions there is considered only minimal potential risk of money laundering or terrorist financing. Irregular patterns of activity or regular deposits and withdrawals with limited betting transactions may highlight enhanced risk. Participants managing their payments and withdrawals so as to remain non-qualifying may also represent enhanced potential risk.

The procedures detailed in the following pages address both the requirement to identify participants and to gather evidence verifying their identity but also to monitor on-going activity to determine a change in the risk profile of the participant.

3.2 Summary of factors and considered associated risk:

- value of funds deposited or staked with the licence holder;
- jurisdiction of participant or business participant;
- source of funds deposited;
- any other relevant matter brought to the attention of the licence holder during the account opening process for the participant or the Business Participant;
- any relevant supervisory or regulatory guidance given by the Gambling Commission;
- the legal nature of the business participant.



3.2.1 Review of Risk Assessment

The company will undertake a review of the relevance of its risk assessment as soon as it is reasonably practical to do so or as and when significant changes in business operations dictate.

4 Policy and procedures

Procedures adopted by BetIndex Ltd to mitigate the above risks and to comply with the Codes:

4.1 Identification

4.1.1 General:

BetIndex Limited does not allow online gaming or the depositing of funds for the purpose of online gaming unless the intended participant has:

- registered with the company through the registration page at the respective domain operated under the gaming licence and
- has created an account with the company and
- has confirmed their acceptance of the terms and conditions.

To register, a player must provide the company with details of their:

- First Name
- Last name
- Username (chosen)
- Gender
- Date of Birth
- Email Address
- Telephone Number (optional)
- Address
- Post Code
- Country

Participants registering on the site are required to input a password of their choosing.

No player under the age of 18 is able to register with the company. If their age is below 18 they are unable to register.

Known problem gamblers will be excluded from registration as will gamblers who have previously been excluded from the site. Gamers wishing to re-register with the site will be required to send an email to customer services requesting that their account be reactivated.

Records will be maintained by BetIndex Limited's administration of all current, attempted and past registrations.

Upon completion of all required fields and confirmation of agreement to the terms and conditions, an email will be sent to the registered user at the email address provided. Registration will not take place if all fields are not completed.

To activate the player will be required to re-log on to respective domain using the link provided, upon successful input of their password their account will be activated.

No monies can be deposited with the company and no free units allocated to the account until the account has been activated.

4.1.2 Anonymous Accounts

Gamers will not be able to register with fictitious names or anonymous accounts.

When registering with a website owned by the Licence Holder, the account will not be opened unless the requested identity details (shown above) are completed in full. Duplicate accounts will not be allowed and checks will be made at the time of registration.

Fictitious names will not be allowed. Fictitious names will be identified at the time funds are deposited to the account and the account terminated.

A participant whose account is terminated will be advised by email.

4.1.3 Evidence of identity for participants

Payments received from participants that exceed Euro 2000 (or currency equivalent) or payments/stakes which are received cumulatively within a 24 hour period exceed Euro 2000 (or currency equivalent) are classified in the Codes as threshold payments and as such trigger the requirement for evidence to be gathered confirming the registered participants' identity.

When a participant makes a threshold payment to the company or when a participant stakes an amount which will be deemed a threshold payment, the funds will be locked and no withdrawals made until such time as the identity of the participant has been verified. Locking of the account will not prevent the participant from continuing to bet.

Once verification is completed the account can be unlocked and business continues as normal.

If verification cannot be completed, then the operator must proceed in line with the regulations and terminate the business relationship with the customer.

An email will be sent automatically to the participant explaining why activity has ceased and the account suspended and will request the following information:

a) Verification of identity:

The following are acceptable identity documents:

- A passport
- A national ID card
- An armed forces ID card
- A full driving licence

To be acceptable identity documents must be:

- A good clear copy, plainly legible,
- Unexpired at the date of receipt,

- Bear a photo of the holder, and
- Signed by the holder.

b) Verification of address:

- A recent account statement (i.e. no more than 6 months old) from a recognised bank, building society or credit card company or the most recent mortgage statement from a recognised lender.
- An unexpired photographic driving licence or national identity card containing current residential address if the document has not been used to verify identity.
- A recent rates, council tax or utility bill (recent in respect of utility bills is considered to be for the last quarter i.e. no more than 6 months old). Mobile telephone bills are **not** acceptable as evidence of address under any circumstances.
- Correspondence from an official independent source such as a central or local government department or agency.
- Documents provided to verify an address should **not** refer to P O Boxes or 'care of' addresses.

The email will automatically be copied to the Administration Team. The Administration Team will log the email and await receipt of the required documents.

Only upon receipt of the documents to a satisfactory standard will management authorise the re-activation of the account and process the threshold payment.

The account will be marked as having received due diligence.

The Administration team will also consider whether a suspicious transaction report should be made to the Nominated Officer. The factors that may influence that decision are:

- If the required documents are not received and the monies and account remain suspended.
- The transaction history. If none or very few bets have been placed and a withdrawal of deposited funds is being requested, this may lead the Administration team to consider the transaction suspicious
- If bets are being placed regularly and monies won this should not normally raise suspicions
- If a single bet is placed and large monies are won, suspicions may be raised as to the integrity of the system

If suspicious activity is considered a possibility a suspicious transaction report will be lodged in accordance with the procedures in section 4.3.1.

4.1.4 Evidence of identity for business participants

Before a Business Participant is able to register and activate an account the following information is required.

- copy of the identity and address of the shareholders (representing in excess of 20% of the total shares issued) and all directors and controllers of the business participant
- a copy of the company's certificate of incorporation and memorandum and articles of association
- copy of a board resolution authorising certain individuals to act on behalf of the company
- confirmation of geographical sphere of the company's operations
- nature of its activities
- name of regulator (if appropriate)

4.1.5 Enhanced Participant due diligence

In certain cases, highlighted by the risk assessment (see section 3), management may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the company. Participants who pose an additional risk will be marked within the administrative system and a report of their transactions made available to the Nominated Officer.

A participant who poses higher risk may be:

- a head of state, head of government, minister or deputy or assistant minister;
- a senior government official;
- a member of parliament;
- a senior politician;
- an important political party official;
- a senior judicial official;
- a member of a court of auditors or the board of a central bank;
- an ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- a high-ranking officer in an armed force;
- a senior member of an administrative, management or supervisory body of a State-owned enterprise;
- a senior official of an international entity or organisation; and
- an honorary consul

Any family members of a person mentioned above, including a spouse or equivalent, child or the spouse or partner of a child, brother or sister (including a half-brother or half-sister), parent, parent-in-law, grandparent or a grandchild.

- Any close associate of a person mentioned above including:
- Any natural person who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with such a person;
- Any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of such a person;
- Any natural person who is known to be the beneficiary of a legal arrangement of which such a person is a beneficial owner or beneficiary;
- Any natural person who is in a position to conduct substantial financial transactions on behalf of such a person.

Or a person resident in a country which the company has reason to believe does not apply or insufficiently applies, the FATF recommendations.

In addition any persons that are the subject of any warnings or notices issued by the Gambling Commission will be considered a higher risk.

If the risk of a Business Participant is considered high enhanced due diligence will be obtained. This will include:

- Verification of the identity and address of the shareholders (representing in excess of 20% of the total shares issued) and all directors and controllers of the business participant
- A copy of the company's certificate of incorporation and memorandum and articles of association
- Copy of a board resolution authorising certain individuals to act on behalf of the company
- Confirmation of the geographical sphere of the company's operations
- Nature of its activities
- Name of Regulator (if appropriate)

Based on the risk assessment, and on each individual case, management will decide whether a company search is required and in what form additional due diligence is required. Additional due diligence may include:

- World-Check is an independent online database containing names and details of individuals that may be considered a heightened risk to the company. Examples of individuals featured on the World-Check database include Politically Exposed Persons (PEPs), prominent public figures or persons known or suspected to be involved in financial crime
- Consideration by the company as to whether additional aspects of the participants identity should be verified – perhaps through the certification/notarisation of identity and address verification, securing of bank references etc.
- Consideration by the company as to whether information is required on the source of funds and the source of wealth/background of the participant

4.1.6 On-going Monitoring of transactions

All transactions by all participants are recorded and can be reported on a daily, weekly, monthly or annual basis.

It is recognised that a significant change to the normal operation of an account could be a sign of suspicious activity. A change may be:

- Unusually large deposits based on past deposit history
- Large deposits followed by large withdrawals combined with minimal betting transactions
- Multiple changes to address details
- Deposits and stakes reaching the threshold requirements



In addition changes made to the participants identity and personal information will be reported on to the company's management. The evidence of identity previously provided by the participant will be reviewed and steps taken to renew and update that information in light of the reported changes to the participant's identity. In certain cases, this may mean that the account is suspended pending receipt of new identity and address verification.

In the event that satisfactory confirmation of the information as to the identity of the participant or satisfactory verification of evidence of identity is not provided, then the account will be suspended, no further betting activity allowed and consideration be given to the lodging of a suspicious transaction report.

4.2 Record keeping and retrieval of records

4.2.1 Record of Transactions

BetIndex Limited will maintain appropriate records of all participants and their associated transactions. The Island based directors and Nominated Officer have unfettered access to all records (other than those which are stored in an encrypted or hashed form) and reporting through the back office computer system. All records and audit trails can be accessed by them and reported in hard copy format without delay and within 7 days of any request being made.

- Identification and verification of identify

The directors and Nominated Officer will at all times retain access to the back office computer system which holds the registration details of all participants. Such records can be accessed without delay via bespoke reports accessed/generated by the back office system.

The Nominated Officer has the ability to retrieve all identity verification that has been collated on those considered to pose a higher risk or those who have been subject to qualifying payments. Hard copies can be retrieved on request.

- Deposits, Withdrawals, Bets, Prize Payments

All financial transactions are recorded against the participant within the back office system and are reconciled against banking records provided by the Payment Service Providers, and bank. This includes the name of the participant or unique identity number, the amount and nature of the transaction, the date of the transaction, the source or recipient of the funds and the nature of the financial transaction – credit/debit card, e-wallet etc.

All financial transactions are maintained in a system audit log which is available to the Nominated Officer and directors upon request.

Each transaction is recorded in the database of the website with a specific reference. Transactions are sorted in the back-office using the same reference pattern and can be scrutinised by the directors and Nominated Officer by date, participant or nature of the transaction

4.2.2 Retention of Records

Records will be maintained in a secure and accessible form: Secure backups of all data are made on a daily basis.

Records include:

- all registration details
- identification verification
- enhanced due diligence

- suspended accounts and reason for suspension
- closed accounts
- suspicious transaction reports
- financial transactions – deposits, bets made, withdrawals, prize payments
- self-exclusions
- self-imposed limits
- excluded players
- bets placed
- complaints and responses
- audit trails
- accounting and bookkeeping records including VAT returns, duties payable etc.
- bank reconciliations
- Customer Service electronic correspondence records

Records associated with a participant (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the participant's account or the date of the last transaction.

The Nominated Officer logs any Participants who have been the subject of a suspicious transaction report on the computer system. Records associated with such participants will be maintained until such time as the Nominated Officer agrees to them being destroyed. In cases where an on-going investigation is being conducted, the Nominated Officer will retain the records until such time (but in any case for at least 5 years) as the investigating JFCU officer confirms that the records are no longer required.

4.2.3 Nominated Officer

Nominated Officer

xxxxxx

Deputy Nominated Officer

xxxxxx

4.2.4 Register of Money Laundering enquiries and reports

The Nominated Officer maintains a register separately from other records associated with the company which details:

- a) Enquiries made to BetIndex Limited by law enforcement or other officials acting under powers provided by the Money Laundering and Terrorist Financing Requirements

This register contains:

- The nature and date of the enquiry
- The name of the enquiring officer and enforcement agency
- The powers being exercised
- Details of the participant
- Details of the transaction

- Outcome of enquiry (if known)

b) All reports made to a constable within the JFCU in relation to suspicious transactions

This register contains:

- The nature and date of the report including details of the participant and the transaction
- The name of the person making the report
- The name and agency of the constable to whom the report is made
- Information about the transaction which is sufficient to identify the relevant papers
- Details of the acknowledgement of receipt of report provided by the JFCU
- Outcome of enquiry (if known)

c) All reports made to the Nominated Officer by BetIndex Limited employees

This register contains:

- The nature and date of the report including details of the participant and the transaction
- The name of the person making the report
- Information about the transaction which is sufficient to identify the relevant papers
- Details of the acknowledgement of receipt of report provided by the Nominated Officer
- Outcome of the report

4.3 Internal procedures including the reporting of suspicious transactions, both internal and external

BetIndex Limited shall at all times have an appointed Nominated Officer.

The appointed Nominated Officer will be sufficiently senior within the company and will have the right of direct access to the Directors of the company.

The Nominated Officer will have unfettered access to all reports, transaction histories, complaints and audit trails.

4.3.1 Internal suspicious activity reporting

Suspicious activity must be reported to the Nominated Officer or Deputy Nominated Officer as soon as reasonably practical using the attached form, as per Appendix 6.1. The form is also available on request from the Nominated Officer. The case may be discussed initially with the Nominated Officer, but a telephone discussion is not a substitute for formal notification using the appropriate form.

It is important that the form is used as this properly documents the report itself and ensures that all relevant information is included. For this reason it is important that all parts of the form are completed.

Receipt of the report will be acknowledged by the Nominated Officer.

It is not necessary for the person making the report to include their name on it. However if an acknowledgement is required the person making the report will need to identify themselves to the Nominated Officer in some other way, such as by providing a covering memo.

Once an initial report has been submitted the person should continue to submit reports where further suspicious activity takes place, or if there are developments in respect of the matter originally reported.

4.3.2 Reporting and “active” business

Where a suspicion is reported in respect of a transaction that has not taken place or an activity that has not commenced this fact should be made clear to the Nominated Officer. If the person submitting the report is involved with the transaction or activity they should not do anything further until advised that they can do so by the Nominated Officer.

The Nominated Officer in conjunction with the Directors will manage the process of ensuring that the transaction may proceed, including obtaining JFCU clearance if appropriate.

4.3.3 External suspicious activity reporting

The Nominated Officer has full access to information and records of the company that the Directors consider necessary to evaluate internal reports received. They will document the evaluation process and the reasons for conclusions reached.

If after completing the evaluation process the Nominated Officer considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the Nominated Officer are responsible for:

- Submitting the necessary information to the JFCU
- Recording the disclosure in the register of disclosures
- Dealing with subsequent production or account monitoring orders, if there are any.
- Inform the Gambling Commission of the unique reference number within five days of receipt from the JFCU.

4.3.4 Whistleblowing Policy

If, in the course of employment, an employee becomes aware of information which they reasonably believe tends to show one or more of the following, they must use BetIndex Limited disclosure procedure set out in the Whistleblowing Policy:

- That a criminal offence has been committed is being committed or is likely to be committed.
- That a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject.
- That a miscarriage of justice that has occurred, is occurring, or is likely to occur.
- That the health or safety of any individual has been, is being, or is likely to be endangered.
- That the environment, has been, is being, or is likely to be damaged.
- That information tending to show any of the above, is being, or is likely to be deliberately concealed.
- That the business or any associated person has been, is being, or is likely to be receiving or offering bribes.
- That any foreign official has been, is being, or is likely to be bribed or offered facilitation payment by the company or any associated person.

4.4 Staff education, training and development

4.4.1 Importance for AML/PTF risks

The way the company is organised can increase or mitigate the exposure of the company to money laundering and terrorist financing risks. In particular procedures and controls operated by the company, many of which are required by law, can be applied in order to manage AML/PTF risk.

4.4.2 The importance of staff in ML prevention

Success in preventing money laundering and terrorist financing cannot be achieved by having appropriate policies alone. Even the best policies are useless if staff ignore or circumvent them, whether through ignorance, carelessness or deliberately. Staff are a business's strongest defence or their weakest link. It is therefore essential that the principles outlined in section 2.3.1 are adhered to.

4.4.3 Human Resources risk factors in ML prevention

The main human resources risk factors are considered to be:

- Staff lack integrity
- Staff lack knowledge, training or awareness
- Staff have conflicts of interest
- Direct criminal or terrorist exploitation of HR weaknesses.

4.4.4 Integrity

The integrity of the directors and employees of the company are the foundation of its AML/PTF measures. If staff lack integrity there is a danger that they may become involved in or become willing accomplices to laundering activity.

Direct involvement in laundering operations is the possible extreme. More likely is that staff without the right attitude are unlikely to:

- Maintain awareness and detect money laundering
- Report money laundering if they become aware of it
- Take seriously their own training or that of their subordinates
- Encourage reporting and foster a culture that supports money laundering prevention.

4.4.5 Staff Recruitment

It is important that we take appropriate steps to ensure the integrity of new staff. Such steps should be risk based, with the extent of the effort proportional to the role of the employee and the money laundering threat inherent in the role they are being recruited for.

The following staff screening procedures are operated by BetIndex Limited:

- For all new staff at least one reference will be taken up. References will be obtained by obtaining the permission of the prospective employee to write direct to the referee. References supplied by the prospective employee and references addressed “to whom it may concern” will not be accepted unless they can be confirmed direct with the referee.
- Copies of relevant qualifications will be confirmed by requesting sight of certificates, copies of which will be retained on the employees file.
- Curriculum vitae will be obtained from all prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer.

For staff recruited for Manager, Nominated Officer or Director positions, the following additional checks will be performed:

- The identity of the prospective employee will be verified by requesting sight of identity verification documents.
- Worldcheck
- A police vetting form submitted to the Commission.

4.4.6 Staff Knowledge, Training and Awareness

Recruiting staff of integrity is not sufficient in itself. Staff must have sufficient awareness and training to detect money laundering and terrorist financing and to understand what is expected of them.

It is key to effective AML/PTF arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering
- Staff are aware of their personal legal obligations

The steps adopted by the group to ensure staff have appropriate awareness and training are as follows:

- All new staff will receive AML/PTF induction training, to include:
 - The provisions of the AML/PTF code and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - Their personal obligations under the AML/PTF Code and associated personal liabilities for non-compliance
 - The internal reporting procedures detailed in the AML/PTF Manual
- AML/PTF refresher training will be delivered at least annually for all staff.
- The Nominated Officer will provide other ad hoc information about news and developments. This will be targeted as appropriate.
- The Nominated Officer will send periodic reminders of the need to report certain matters.

4.4.7 Continuing Personal Development (“CPD”)

While certain formal structured training will be provided, staff are also required as a condition of their employment to maintain their own personal CPD.

4.4.8 Staff promotion and transfer

When an employee is promoted or transferred to a new role the Nominated Officer will be informed in advance, either electronically or in writing. The Nominated Officer will confirm whether any further training or vetting is required, and whether the training or vetting is required before the appointment can take place.

4.5 Technological Developments

BetIndex Limited recognises the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism. As a consequence:

- The Directors retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the company has engaged with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- BetIndex Limited is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

5 Proceedings

5.1 Offences

POCA and the Terrorism Act create offences of failing to report suspicious activity. Where a person fails to comply with the obligations to make disclosures to a nominated officer, or the nominated officer to the Jersey JFCU, as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee, they are open to criminal prosecution. In certain circumstances, a person also commits an offence under POCA or the Terrorism Act if he discloses information that a SAR has been submitted that is likely to prejudice any investigation, or discloses information that an investigation into allegations that an offence under POCA or the Terrorism Act has been committed, that is likely to prejudice the investigation.

A person in the regulated sector also commits an offence if he knows or suspects that an appropriate officer or, in Scotland, a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted, and falsifies, conceals, destroys or disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation,

The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

Version 3. Dated: 24th March 2015

6 Appendices

6.1 Appendix A – Suspicious Transaction Report

Report Prepared by:	
Participant/Gamers Name	
Username	
Address	
Email Address	
Telephone Number	
Is identification and address verification held?	
Is enhanced due diligence held?	

Reason for suspicion	
To include: Identification verification Criminal conduct known or suspected	

Date of report	
-----------------------	--

To be copied, and one copy completed below returned to the staff member as acknowledgement. Remember you are required to do nothing that might prejudice inquiries i.e. tipping off the client or any other third party.

Receipt of report acknowledged:	
Signed, Nominated Officer	
Date	