2008-01-18 13:06:00

G014_ANTI-MONEY_LAUNDERING

Anti-money laundering & prevention of financing of terrorism

Guidelines

G 014

1 Administration

1.1 Authority

This document is issued by the Financial Services Regulatory Commission (the Commission) pursuant to r 119 of the Antigua & Barbuda Interactive Gaming and Interactive Wagering Regulations.

> **119.** The Commission may establish standards, specifications and guidelines in relation to gaming equipment and systems.

1.2 Confidentiality

This document, all related documents, and methodologies embodied in this document and related documents ("*the documents*") are the property of the Financial Services Regulatory Commission. Unauthorised copying and distribution of *the documents*, by any means, on any media is prohibited.

This document, its themes, and ideas are strictly confidential and may not be used in any manner other than its expressed purpose, without the written permission of the author. The documents are authorised for use by licence holders.

The documents are copyright.

1.3 Disclaimer

The rules and procedures provided in these documents are current at the time of writing. The Commission may in its absolute discretion amend these rules and procedures, or any definitions or interpretations pursuant to these documents at anytime.

Each licence holder should ensure it has the current version of each document.

1.4 Queries

All queries relating to this document should be made, in writing, to:

Director of Gaming
Financial Services Regulatory Commission
First Caribbean Financial Centre
Old Parham Road
St John's
Antigua and Barbuda

e-mail : director@antiguagaming.gov.ag

1.5 References & related documents

The Financial Services Regulatory Commission utilised many documents and international standards when compiling the suite of guidelines.

The current list of related guidelines is available from the Commission's website at http://www.antiguagaming.gov.ag.

Licence holders and other interested parties should acquaint themselves with the contemporary documents before relying on them.

1.6 Table of contents

2 Preliminary

2.1 Purpose

The purpose of this document is to provide guidance as to control systems which might be applied to meet the requirements of r 105(n):

> **105.** A control system submission must be in a form approved by the Commission and describe and explain the licence holder's proposed control system and in particular must include:
>
> (n) anti-money laundering policies and procedures;

2.2 Introduction

The guidance provided here suggests controls, which a licence holder might include in its Anti-money laundering / prevention of terrorism policies and procedures, which the Commission consider appropriate for the purpose of managing compliance and risk associated with money laundering matters.

These guidelines do not circumvent any legislation, regulation or statutory direction which the licence holder is bound to comply.

3 Control guidance

Policy objective

Licence holders shall ensure their businesses, gambling, and related transactions are free from criminal involvement, money laundering and the funding of terrorism.

3.1 Internal organisation

3.1.1 Designated functions

1. The organisation should map its business areas, services, and relationships to the designated services in the First Schedule to the Money Laundering (Prevention) Act 1996 (as amended).

2. The organisation should document the functions, and roles and responsibilities relating to all business areas, services and relationships captured by the First Schedule to the Money Laundering (Prevention) Act.

3. The organisation should determine the relative size (in terms of personnel, revenue, systems) of the portions of the business which are impacted by anti-money laundering and counter-financing of terrorism.

3.1.2 Compliance officer details

1. The organisation should ensure the Compliance Officer is identified, full name and contact details are provided to the Supervisory Authority and the Commission.

3.1.3 Internationally dispersed businesses

1. The organisation should document all internal and external financial transaction types including instructions relating to financial transactions. Particular attention should be paid to transactions and instructions which span national boundaries.

2. The organisation shall undertake a formal risk assessment of all internal and external transactions and financial instructions which span national boundaries.

3. The anti-money laundering and counter-financing of terrorism detection and reporting policies and procedures should be documented for each jurisdiction in which the organisation has a presence, whether physical, virtual or through an associate.

4. The organisation should have mechanisms implemented to ensure it keeps abreast of all relevant laws in all jurisdictions in which it has a presence, whether physical, virtual or through an associate.

3.1.4 Regulatory attention

1. The organisation shall implement appropriate remedial action in relation to any matter bought to its attention by any regulatory authority in any jurisdiction in which it has a presence, whether physical, virtual or through an associate.

3.1.5 Anti-money laundering / counter terrorism financing compliance structure

1. The Compliance Officer should work independently from all other functions within the organisation.

2. The organisation should ensure there is an appropriate number of trained staff across all appropriate business functions to effectively undertake its anti-money laundering and counter terrorism financing responsibilities.

3. The roles and responsibilities of the Compliance Officer should be formally documented.

4. The anti-money laundering and counter terrorism financing roles and responsibilities of all staff should be formally documented and disseminated.

3.1.6 Anti-money laundering / counter terrorism financing policies & procedures

1. The organisation shall have formal anti-money laundering and counter terrorism financing policies.

2. The formal anti-money laundering and counter terrorism financing policies and procedures shall be customised to meet the specific and unique business undertaken by the organisation, within the context of its operating environment, and within the context of all associates with whom the organisation transacts.

3. The organisation shall have formal anti-money laundering and counter terrorism financing procedures for all staff.

4. The effectiveness of the policies and procedures should be reviewed at least annually, to ensure continued appropriateness in the dynamic threat and risk environments in which the organisation exists.

3.1.7 Compliance officer

1. The Compliance Officer should be a manager.

2. The Compliance Officer is a Key Person for purposes of the Interactive Gaming and Interactive Wagering regulations.

3. The Compliance Officer should have authority to act independently to fulfil his or her anti-money laundering and counter terrorism financing roles and responsibilities.

4. The Compliance Officer should have full support of executive management and the Board.

5. The organisation should submit a report detailing the reasons for the termination of the Compliance Officer to the Commission.

6. The Compliance Officer should submit a written report to the Commission detailing the reasons for termination of Compliance Officer responsibilities.

7. The organisation shall consider the potential for conflict of interest in any other duties or responsibilities undertaken by the Compliance Officer. The organisation should ensure potential or perceived conflict of interest scenarios do not occur.

8. The organisation shall ensure all incidents or suspicions of all staff members are bought to the attention of the Compliance Officer. The organisation shall ensure there is a clear and unambiguous reporting method from all staff to the Compliance Officer.

9. Organisations shall ensure all staff know who the Compliance Officer is.

3.1.8 Board & senior management oversight

1. The anti-money laundering and counter terrorism financing policies shall be approved by the most senior level of management (Board, Chief Executive Officer, etc).

2. The anti-money laundering and counter terrorism financing programme should be approved by the most senior level of management (Board, Chief Executive Officer, etc).

3. The most senior level of management should provide continuous oversight of the effectiveness of the organisation's anti-money laundering and counter terrorism financing programme. The method of undertaking this oversight should be documented.

3.2 Money laundering / terrorism financing risk identification

3.2.1 Risk assessment

1. Organisations should have a formal and documented risk management methodology (i.e. AS/NZS4360, etc).

2. The organisation should undertake a risk assessment specifically relating to money laundering and terrorism financing.

3. The organisation should ensure risk rating categories should provide sufficient granular to provide objective classification of relative risk ratings, allowing objective prioritisation of risk treatments.

4. The organisation should ensure the nature, size and complexity of its business, the environment in which it operates and the nature, size, complexity and environment of persons with which it transacts are consider in performing risk assessments.

5. The anti-money laundering and counter terrorism financing risk management activities should be formal and documented, such that an independent auditor may be able to determine the appropriateness of the risk management programme.

6. As a result of the risk management programme the organisation should have documented controls and treatment plans, and evidence of such.

7. The organisation should have mechanisms in place to re-visit the risk management programme every time there's a material change in its operating context and environment. The risk management programme should be repeated at least annually.

8. The organisation should undertake a money laundering and terrorism financing risk assessment before engaging any new Client Service Provider or business associate.

9. The organisation should undertake a money laundering and terrorism financing risk assessment before engaging any new technology.

3.2.2 Services & channels

1. The organisation shall consider the nature of the services it, its Client Service Providers, and business associates provide when performing the money laundering and terrorism financing risk assessment.

3.2.3 Channels

1. The organisation shall consider the nature of the channels it, its Client Service Providers, and business associates utilise when performing the money laundering and terrorism financing risk assessment.

3.2.4 Jurisdictions

1. The organisation shall consider the nature of the jurisdictions it, its Client Service Providers, and business associates utilise when performing the money laundering and terrorism financing risk assessment.

2. The organisation should pay special attention to potential business associates, where the other person is located in or has dealings within jurisdictions that have not adopted a comprehensive anti-money laundering programme.

3.2.5 Customers

1. The organisation shall consider the nature of its, its Client Service Providers, and business associates customers when performing the money laundering and terrorism financing risk assessment.

3.2.6 Evidence

1. The organisation should ensure the risk criteria used and risk assessment relating to all Client Service Providers, business partners, and customers are documented.

3.2.7 Politically exposed persons (PEPs)

1. The organisation shall have a formal and documented process to determine if it, its Client Service Providers, and business partners to ensure politically exposed persons (PEPs) are identified.

2. There should be a formal, documented procedure in the action to be undertaken when a PEP is identified.

3.3 Anti-money laundering / counter terrorism financing programme

3.3.1 Programme - general

1. The organisation should have an anti-money laundering and counter terrorism financial programme the primary purpose of which is to minimise, identify, mitigate, and manage the risk the organisation may reasonably face that the provision by the organisation of its interactive gaming, interactive wagering or related business activities might involve or facilitate (a) money laundering, or (b) the financing or terrorism.

2. The organisation's anti-money laundering and counter terrorism financing programme should, where necessary, be integrated with the anti-money laundering and counter terrorism financing programme of its Client Service Providers and business associates.

3. The organisation should have the flexibility and procedures necessary to amend the anti-money laundering and counter terrorism financing programme in accordance with iterations of the risk management programme.

4. The organisation should have quality or performance metrics to ascertain the effectiveness of its anti-money laundering and counter terrorism financing programme.

3.3.2 Programme - customer & associate identification

1. Organisations should have within its anti-money laundering and counter terrorism financing programme a part, the primary purpose of which is to set out the applicable customer and associate identification procedures for the purpose of statutory compliance.

2. The organisation's customer and associate identification methods, where necessary, be integrated with the anti-money laundering and counter terrorism financing programme of its Client Service Providers and business associates.

3. The organisation may utilise risk management techniques with regard to its customer and associate identification methods up to criteria defined by various statutes.

4. The organisation should incorporate the changing threat, vulnerability and controls relating to customer and associate identification within its risk management programme.

5. The organisation should have quality or performance metrics to ascertain the effectiveness of its anti-money laundering and counter terrorism financing programme as it pertains to customer identification.

3.4 Customer & associate identification & verification

3.4.1 Identification

1. The organisation should have effective controls to ensure it does not provide interactive gaming or interactive wagering services until the documented identification procedures have been satisfactorily undertaken.

2. The organisation shall ensure the necessary minimum identification is collected and maintained with regard to customers, Client Service Providers, Key Persons, and associates.

3. The organisation should perform enhanced identification checks where it could be reasonably believed there is a heightened risk of money laundering or terrorism financing.

4. The organisation should have quality or performance metrics to ascertain the effectiveness of its enhanced identification processes per guideline 3.4.1 3 above.

5. The organisation should use risk management methods to determine whether it will rely on verification from documentation, electronic data, or a combination of both – subject to statutory requirements.

6. The organisation should have quality or performance metrics to ascertain the effectiveness of its verification methods per guideline 3.4.1 5 above.

7. The organisation should use risk management methods to determine what it accepts as reliable and independent verification for both documentation and electronic data – subject to statutory requirements.

8. The organisation should have quality or performance metrics to determine the effectiveness of its standard of evidence depending on its nature per guideline 3.4.1 7 above.

9. The organisation should use risk management methods to establish pre-defined tolerance levels for matches and errors in electronic data.

10. The organisation should have quality or performance metrics to determine the effectiveness of pre-defined tolerance levels for electronic data per guideline 3.4.1 9 above.

11. The organisation should have risk based procedures in place to determine whether, and in what circumstances, the organisation is prepared to rely upon a copy of a reliable and independent document in verifying *Know Your Customer* (KYC) information collected from a customer.

12. The organisation should have quality or performance metrics to determine whether, and in what circumstances, the organisation is prepared to rely

upon a copy of a reliable and independent document in verifying KYC information collected from a customer per guideline 3.4.1 11 above.

13. The organisation should have risk based procedures in place to identify and respond to discrepancies in the course of verifying KYC information.

14. The organisation should have quality or performance metrics in relation to any procedures it has to identify and respond to discrepancies in the course of verifying KYC information per guideline 3.4.1 13 above.

3.4.2 Authentication

1. The organisation should have risk based procedures in place to determine in what circumstances it will take steps to determine whether a document produced by a customer may have been forged, tampered with, cancelled or stolen and, if so, what steps it will take to establish whether or not the document has been forged, tampered with, cancelled or stolen.

2. The organisation should have quality or performance metrics in relation to any procedures it has to determine whether a document produced by a customer may have been forged, tampered with, cancelled or stolen and the steps taken to establish whether or not the document has been forged, tampered with, cancelled or stolen per guideline 3.4.2 1 above.

3. The organisation should have risk based procedures in place to determine whether it will use any authentication service that may be available in respect of a document or electronic data.

4. The organisation should have quality or performance metrics in relation to any procedures it has to determine whether it will use any authentication service that may be available in respect of a document or electronic data per guideline 3.4.2 3 above.

5. The organisation should have risk based procedures in place to determine whether, and how, to confirm KYC information collected from a customer by independently initiating contact with the customer or person that the customer claims to be.

6. The organisation should have quality or performance metrics in relation to any procedures it has to determine whether and how, it will confirm KYC information collected from a customer by independently initiating contact with the customer or person that the customer claims to be per guideline 3.4.2 5 above.

3.4.3 Agents of customers

NOTE: for the purposes of this section Agents include Client Service Providers and business associates such as aggregators and business associates of the aggregators.

1. The organisation should have procedures in place to collect the minimum information required, in accordance with the statutes, for an agent of a customer who is authorised to act for or on behalf of the customer in relation to a designated service.

2. The organisation should have quality or performance metrics in relation to any procedures it has to collect the minimum information required, in accordance with the statutes, for an agent of a customer who is authorised to act for or on behalf of the customer in relation to a designated service per 3.4.3 1 above.

3. The organisation should have risk based procedures in place to determine whether, and to what extent, it should verify the minimum information collected for an agent of a customer.

4. The organisation should have quality or performance metrics in relation to any procedures it has to determine whether, and to what extent, it should verify the minimum information collected for an agent of a customer per guideline 3.4.4 3 above.

5. The organisation should have procedures in place to provide for an agent of a non-natural customer to be identified by a verifying officer.

6. The organisation should have quality or performance metrics in relation to any procedures it has to provide for an agent of a non-natural customer to be identified by a verifying officer per guideline 3.4.4 5 above.

7. If the organisation has provided for an agent of a non-natural customer to be identified by a verifying officer, the organisation should have procedures in place to meet any minimum requirements of identification by a verifying officer.

8. The organisation should have quality or performance metrics in relation to any procedures it has to meet the minimum requirements of identification by a verifying officer if the organisation has provided for an agent of a non-natural customer to be identified by a verifying officer per guideline 3.4.4 7 above.

3.4.4 Agents of licence holders

1. If the organisation has authorised another person to be its agent, or otherwise uses the service of another person, for the purpose of carrying out applicable customer identification procedures then the organisation should have a formal, documented agreement with the other person in relation to customer identification procedures carried out by the other person on its behalf.

2. The organisation should have procedures in place to determine whether it is appropriate to rely upon the applicable customer identification procedures carried out by an authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator having regard to the money laundering / terrorism financing risk faced by the organisation relevant to the provision of interactive gaming, interactive wagering or related service to the customer.

3. The organisation should have quality or performance metrics in relation to any procedures it has to determine whether it is appropriate to rely upon the applicable customer identification procedures carried out by an authorised agent, other person, Client Service Provider, business associate,

aggregator, or business associate of an aggregator having regard to the money laundering / terrorism financing risk faced by the organisation relevant to the provision of the designated service to the customer per guideline 3.4.4 2 above.

4. The organisation should have procedures in place to determine the money laundering / terrorism financing risks associated with the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator.

5. The organisation should have quality or performance metrics in relation to any procedures it has to determine the money laundering / terrorism financing risks associated with the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator per guideline 3.4.4 4 above.

6. The organisation should have procedures in place to satisfy itself that appropriate records are kept and maintained by the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator.

7. The organisation should have quality or performance metrics in relation to any procedures it has to satisfy itself that appropriate records are kept and maintained by the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator per guideline 3.4.4 6 above.

8. The organisation should have procedures in place so that the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator can relay any money laundering / terrorism financing suspicions they may have to the organisation.

9. The organisation should have quality or performance metrics in relation to any procedures in place so that the authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator can relay any money laundering / terrorism financing suspicions they may have to the organisation per guideline 3.4.4 8 above.

10. The organisation should have policies and procedures in relation to due diligence carried out on authorised agent, other person, Client Service Provider, business associate, aggregator, or business associate of an aggregator that are authorised to identify a customer or person who may conduct interactive gaming or interactive wagering with a customer of the organisation.

3.5 Monitoring & reporting

3.5.1 Ongoing customer due diligence

1. The organisation should have procedures in place to monitor its customers receiving interactive gaming, interactive wagering or related services at, through or in association with the organisation's licence, on an ongoing basis with a view to minimising, identifying, mitigating and managing money laundering / terrorism financing risk.

2. The organisation should have risk based procedures in place to determine whether and in what circumstances KYC information should be updated or verified for ongoing customer due diligence purposes.

3. The organisation should have risk based systems and controls in place to determine whether, as a result of a change in customer circumstances, additional KYC information needs to be obtained from that customer for ongoing customer due diligence purposes.

4. The organisation should have risk based procedures in place to determine the source of wealth of customers, as an integral part of the KYC information.

5. If the organisation is associated with Client Service Providers or aggregators and if its ongoing due diligence obligations will be discharged by another entity then the name of the responsible entity shall be recorded in logs.

6. The organisation shall have procedures in place to ensure that it monitors all customers against official lists of prescribed persons/entities on an ongoing basis.

3.5.2 Transaction monitoring

1. The organisation should have a risk based transaction monitoring program in place to monitor transactions of customers, Client Service Providers and business associates.

2. The organisation shall have risk based procedures in place to identify suspicious transactions, including regard to complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or visible lawful purpose.

3.5.3 Suspicious matter reports

1. The organisation's suspicious matters monitoring and reporting systems should cover all interactive gaming, interactive wagering and related business and financial transaction areas and potentially relevant business units.

2. The organisation's monitoring and reporting systems and procedures should have regard to whether the customer is who they claim to be.

3. The organisation's monitoring and reporting systems and procedures should have regard to whether a customer, transaction or matter may be connected to tax evasion.

4. The organisation's monitoring and reporting systems and procedures should have regard to whether a customer, transaction or matter may be connected to what would be an offence if it occurred in Antigua & Barbuda.

5. The organisation's monitoring and reporting systems and procedures should have regard to whether a customer, transaction or matter may be connected to an offence under any laws within the CARICOM – if the

activity occurred within the CARICOM. The exception to this guideline relates to the legality of the licenced interactive gaming or interactive wagering and associated business itself. It is the customers responsibility with regard to such matters.

6. The organisation's monitoring and reporting systems and procedures should have regard to whether a customer or associate, transaction or matter may be connected to the financing of terrorism.

7. The organisation's monitoring and reporting systems and procedures should have regard to whether a customer or associate, transaction or matter may be connected to money laundering.

8. The organisation shall have procedures in place to report suspicious matters to the ONDCP and the Financial Services Regulatory Commission.

9. The organisation shall have procedures in place to ensure a suspicious matter report contains all relevant details of the customer and matter that has triggered the suspicion.

10. The organisation shall have procedures in place to allow it to evaluate and report suspicious matters to ONDCP and FSRC within the specified timeframe.

11. The organisation shall have policies, procedures, and controls in place to prevent 'tipping off'.

12. The organisation shall ensure all personnel are aware of the "safe harbour" provisions under the Money Laundering (Prevention) Act 1996 (as amended).

3.5.4 Threshold transaction reports

1. The organisation shall have systems and processes in place in relation to detecting and reporting threshold transactions.

2. The organisation's detection and reporting system shall cover all areas concerning threshold transactions.

3. The organisation shall have procedures in place to report threshold transactions to ONDCP and the FSRC.

4. The organisation shall have procedures in place to ensure a threshold transaction report contains all relevant details of the customer and transaction in accordance with statutory requirements.

5. The organisation shall have procedures in place to allow it to report threshold transactions to ONDCP and the FSRC within the specified timeframe.

3.5.5 Information in electronic funds transfer instructions

1. The organisation should have systems and processes in place to ensure that complete payer information is obtained for all relevant domestic and international electronic funds transfer instructions (EFTIs) before it passes

on, dispatches or takes any other action to carry out the transfer instruction in accordance.

2. The organisation shall have systems and processes in place to flag all relevant domestic and international incoming EFTIs which do not have complete payer information.

3. The organisation should have systems and processes in place to request complete payer information from the ordering institution in international EFTIs where that information is incomplete and is requested by ONDCP.

4. Where the organisation is the beneficiary institution, then systems and procedures shall be in place to comply with ONDCP and FSRC requests in a timely manner to report instances of the ordering institution's non-compliance with requests for the required transfer information.

5. The organisation should have policies and procedures to refuse to pay on an international EFTI which does not contain the required transfer information where the organisation is the beneficiary institution and the ordering institution is overseas.

3.6 Employee due diligence

3.6.1 Employee due diligence programme

1. The organisation should have an employee due diligence programme.

2. The organisation shall identify which employees are in a position to facilitate the commission of a money laundering or terrorism funding transaction.

3. The organisation should perform an assessment of its employees' money laundering / terrorism funding risk.

4. The organisation should have risk based procedures in place to screen all prospective and new employees who may be in a position to facilitate the commission of a money laundering / terrorism funding transaction.

5. The organisation should have risk based procedures in place to re-screen employees where there is a change in their responsibilities to a position to facilitate the commission of a money laundering / terrorism funding transaction.

6. The organisation should have a risk based procedure in place to re-screen employees in positions able to facilitate the commission of a money laundering / terrorism funding transaction on a periodic basis.

3.6.2 Disciplinary measures

1. The organisation should have a system in place for managing and disciplining any employee who fails, without reasonable excuse, to comply with any anti-money laundering / counter terrorism funding system, control or procedure established in accordance with Anti-money laundering / Counter terrorism funding programme.

3.7 Training & awareness

3.7.1 Anti-money laundering / counter terrorism funding risk awareness training programmes

1. The organisation shall have an anti-money laundering / counter terrorism financing risk awareness training program in place.

2. Having regard to its money laundering / terrorism financing risk the training programme should be designed and developed to reflect the needs of different levels and roles of employees in relation to the following: content (e.g. awareness and depth), delivery (e.g. learning, face-to-face), duration (e.g. 1 hour, 1 day), and frequency (e.g. annually, periodic).

3. The organisation should ensure anti-money laundering / counter terrorism training is provided to all new employees.

4. The organisation should ensure the training programme includes the following areas: obligations of the organisation under the legislation; consequences of non-compliance with the legislation; examples of money laundering / terrorism financing typologies for organisation's industry; money laundering / terrorism financing risk assessment of the organisation; controls in place (through anti-money laundering / counter terrorism financing programme) to address money laundering / terrorism financing risk; customer identification procedures for staff; summary management report (SMR[1]) procedures and "risk triggers"; threshold transaction reporting procedures; EFTI originator information procedures; and IFTI reporting procedures.

3.7.2 Evidence of training

1. The organisation should keep adequate records of training related to anti-money laundering / counter terrorism financing.

2. The organisation should assign responsibility for anti-money laundering / counter terrorism financing training.

3.8 Compliance & audit

3.8.1 Anti-money laundering / counter terrorism financing compliance programme

1. The organisation should have a compliance program in place to monitor its compliance and identify and remedy any non-compliance with all legislation, regulations and directions from competent authorities.

2. The organisation should have procedures in place to ensure that any changes to anti-money laundering / counter terrorism funding obligations are promptly recognised and adhered to.

3. The organisation should record all instances of non-compliance with the anti-money laundering / counter terrorism funding obligations.

[1] SMR (Summary management report) is a system to extract financial transaction reports information in a summarised or aggregated form.

3.8.2 Compliance report

1. The organisation should have procedures in place to lodge anti-money laundering / counter terrorism funding compliance reports to the Board or most senior management.

2. The organisation should have procedures in place to lodge anti-money laundering / counter terrorism funding compliance reports to the ONDCP – per Directives from the ONDCP.

3.8.3 Independent review

1. The organisation shall have a policy in place to carry out an independent and regular review (by either an internal or external party) of all components of its anti-money laundering / counter terrorism funding programme.

2. The organisation should have procedures in place to implement findings of independent reviews.

3. The organisation shall ensure the results of independent reviews are provided to senior management of the organisation.

3.8.4 FSRC feedback

1. The organisation should have procedures in place to ensure senior management is notified of any FSRC feedback or communication with regard to the anti-money laundering / counter terrorism funding programme or its elements.

3.9 Record keeping

3.9.1 Policies & procedures

1. The organisation shall keep all anti-money laundering / counter terrorism funding related records for the minimum statutory period.

2. The organisation should have the ability to retrieve records without undue delay upon request by a competent regulator or law enforcement.

3. The organisation shall maintain interactive gaming, interactive wagering, and related records for the minimum statutory period – rr 175-178 of the Interactive Gaming and Interactive Wagering Regulations 2007 (as amended).

4. The organisation should maintain hard copy records in an adequate environment and manner as to ensure the integrity, confidentiality and availability of all information.

5. The organisation should maintain a soft copy records in an adequate environment and manner as to ensure the integrity, confidentiality and availability of all information.

3.9.2 Anti-money laundering / counter terrorism financing programme

1. The organisation should keep a record of its anti-money laundering / counter terrorism funding programme and of any amendments to this program.

2. The organisation should maintain evidence that it has put an appropriate anti-money laundering / counter terrorism financing programme in place.

3. The organisation should retain evidence of key decision-making processes in relation to anti-money laundering / counter terrorism funding.

4. The organisation should make records of all steps taken to remedy any non-compliance detected during self assessments and/or by the regulator.

5. The organisation should retain records of any internal and external anti-money laundering / counter terrorism funding audits, including findings relating to those audits.

3.9.3 Customer identification & verification

1. The organisation shall keep appropriate records of customer identification procedures.

2. The organisation should have processes in place to receive and retain customer information if that information has been obtained by a third party within the course of offering interactive gaming, interactive wagering or a related activity.

3.9.4 Corresponding associate due diligence

3. The organisation should create records of due diligence assessments, with regard to anti-money laundering / counter terrorism funding, of business associates including Client Service Providers.

4. The organisation should keep records of due diligence assessments, with regard to anti-money laundering / counter terrorism funding, of business associates including Client Service Providers.

5. The organisation should keep records in relation to documented responsibilities, with regard to anti-money laundering / counter terrorism funding, of business associates including Client Service Providers.

3.9.5 Transactions & suspicious matters

1. The organisation should keep appropriate records about electronic funds transfer instructions.

2. The organisation should keep appropriate records of international fund transfer instruction reports.

3. The organisation should keep appropriate records of transactions.

4. The organisation should keep appropriate records of threshold transaction reports.

5. The organisation should keep appropriate records of suspicious matter reports.

6. The organisation should keep appropriate records of decisions not to report suspicious matters.

7. The organisation should keep appropriate records supplied by the customer in relation to the provision of designated services.

8. The organisation should maintain adequate customer-provided transaction records.

3.10 Correspondent associate

3.10.1 Due diligence assessments

1. The organisation should conduct a preliminary due diligence assessment before entering into a business associate; (including Client Service Provider, payment gateway, aggregator, aggregator business associate, etc); relationship.

2. The organisation should perform regular and ongoing due diligence assessments of the business associate; (including Client Service Provider, payment gateway, aggregator, aggregator business associate, etc); relationship.

3. The organisation should ensure the due diligence assessment examine the matters which will minimise the money laundering / terrorism funding risk.

3.10.2 Senior management approval

1. The organisation should ensure a senior officer approves each new correspondent business associate; (including Client Service Provider, payment gateway, aggregator, aggregator business associate, etc); relationship after having regard to the due diligence assessment.

2. The organisation should clearly document the responsibilities of each party to the business associate; (including Client Service Provider, payment gateway, aggregator, aggregator business associate, etc); relationship.

3.10.3 Shell banks

1. The organisation should have a policy prohibiting relationships with shell banks.

2. The organisation should have a policy prohibiting correspondent business associate; (including Client Service Provider, payment gateway, aggregator, aggregator business associate, etc); relationships with persons that deal with shell banks.

End of document