



AML MANUAL

OCTOBER 2020



Contents

Purpose	2
The Offence of Money Laundering	2
Proceeds of Crime	3
Republic of Marshall Islands Anti-Money Laundering Regulations Act 2002	4
Reporting Entities and their obligations	4
Internal Controls, Policies and Procedures	7
Identification Requirements	10
Enhanced Identification Requirements	12
Branches and subsidiaries:	14
Liability of employers and principals	14
Liability of Directors	15



Purpose

The purpose of this Manual is to provide guidance on the Anti-Money Laundering and Know your Client Policy which is followed by BAXIA MARKETS LIMITED (hereafter the “Company”) in order to achieve full compliance with the Anti-Money Laundering Regulations Act 2002, under the Supervision of the Banking Commission and the FIU in Republic of Marshall Islands.

The Manual should be read in conjunction with the Operations Manual included in the Internal Procedures Manual and the procedures which are followed for account opening.

The aim of the Anti-Money Laundering Regulations Act 2002 is to address the deficiencies that existed in the previous legislation and ensure that Republic of Marshall Islands is in line with international standards and best practice. It will better equip the regulators and law enforcement agencies in the fight against money laundering and terrorism financing.

According to the Anti-Money Laundering Regulations Act 2002, reporting entities have an obligation to verify a customer’s identity, maintain records, and monitor transactions. In addition, reporting entities are required to ensure that accounts are in the true names of clients, to ensure that money transmissions include originator information. Also, the reporting entities have an obligation to report suspicious transactions or certain information and appoint a compliance officer.

These guidelines do not purport to be a comprehensive summary of the Anti-Money Laundering and the Prevention of Terrorism Procedures or a substitute thereof and should be read in conjunction with both Acts which are the source of the law.

The Offence of Money Laundering

The Anti-Money Laundering Regulations Act 2002 extensively define the offence of money laundering



1. A person who is guilty of money laundering if, knowing or believing that property is or represents the benefit of criminal conduct or being reckless as to whether the property is or represented such benefit, the person, without lawful authority or excuse (the proof of which shall lie on the person)-
 - a. Converts, transfers or handles the property, or removes it from the Republic;
 - b. conceals or disguises the true nature, origin, location, disposition, movement of the property or any rights with respect to it; or
 - c. acquires, possesses or uses property

Any person who participate in such conduct as described above, including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing or procuring the commission of such conduct commits the offence of money laundering as a principal offender and shall be liable to be tried and punished accordingly and is liable on conviction to a fine not exceeding SCR5,000,000 or to imprisonment for a term not exceeding 15 years or to both.

2. Every person who -
 - a. organizes or directs others to commit;
 - b. attempts to commit;
 - c. conspires to commit;
 - d. participates as an accomplice to a person committing, or attempting to commit, an offence under subsection 1 commits the offence of money laundering.
3. Knowledge, intent or purpose required as an element of any act referred to in subsection 1 may be inferred from surrounding facts.
4. Where it is necessary in the case of an offence of money laundering alleged to have been committed by a body corporate to establish the state of mind of the body corporate, it shall be sufficient to show that a director, officer, employee or agent of the body corporate, acting in the course of employment or agency as the case may be, had that state of mind.



Proceeds of Crime

The crime of money laundering is not restricted to operations connected with money obtained from drug trafficking but include many types of criminal activity that can yield proceeds. This includes among others terrorism, fraud, robbery or theft, forgery, smuggling, counterfeiting, and extortion. Criminal conduct is defined as per below:

- a. constitutes any act or omission against any law of the Republic including the financing of terrorism as referred to in the Prevention of Terrorism Act, and for the avoidance of doubt includes the offence of money laundering established by this Act and whether committed in the Republic or elsewhere;
- b. where the conduct occurs outside the Republic, would constitute such an offence if it occurred within the Republic and also constitutes an offence under the law of the country or territorial unit in which it occurs;
- c. includes any act or omission against any law of another country or territory whether committed in that other country or territory or elsewhere, unless the Attorney General certifies in writing that it would not be in the public interest to take action in the Republic in relation to an act or omission as defined in this sub-section; and;
- d. includes participation in such conduct, including but not limited to, aiding, abetting, assisting, attempting, counselling, conspiring, concealing or procuring the commission of such conduct;

Knowledge under the Republic of Marshall Islands' Anti-Money Laundering Regulations Act 2002

The definition of money laundering covers those operations where a person knows, or should have reason to believe, that the money with which they are concerned is derived, obtained or realized, directly or indirectly, from an unlawful activity as described above.



It is only necessary that the person should have knowledge or reasonable grounds for knowledge of the unlawful source of the funds to be guilty of the offence. Positive knowledge is not the test; knowledge may be inferred from objective factual circumstances.

What knowledge entails in the case of corporate bodies is clearly stated in the law. It is sufficient that a director, officer, employee or agent of the body corporate acting in the course of his employment or agency had that state of mind. Guilty knowledge of any employee can result in an offence being committed by the employer (as well as by the employee). Crimes committed outside Republic of Marshall Islands

The unlawful activity from which the "dirty money" is derived is any act or omission which was committed or done in Republic of Marshall Islands. Also, acts or omissions committed or done outside Republic of Marshall Islands constitute an offence in Republic of Marshall Islands if they are punishable in Republic of Marshall Islands.

Reporting Entities and their obligations

The Anti-Money Laundering Regulations Act 2002 defines a reporting entity as those persons that carry out certain businesses and activities which can be either financial or non-financial in nature. Reporting entities include banks (including offshore banks), credit unions, bureaux de change (including hotels), insurance companies, money transfer companies, securities companies, trust and company service providers, dealers in precious metals and precious stones, casinos, real estate agents. The Act has been extended to cover Designated Non-Financial Businesses and Professions (DNFBP) which includes lawyers, accountants, notaries and other independent legal professions.

The obligations of the reporting entities include the following:

- Identify and assess money laundering and terrorist financing risks
- Establish and maintain internal control systems and procedures
- Appoint compliance officer
- Apply customer due diligence measures
- Apply enhance customer due diligence measures and enhanced ongoing monitoring for Politically Exposed Persons



- Carry out customer due diligence measures before or during the course of establishing a business relationship or carrying out a one-off transaction. One-off transaction is transaction carried out other than as part of a business relationship that exceeds USD 5,000 in cash or through wire transfers, whether the transaction is carried out in a single operation or several operations which appear to be linked.
- May apply simplified customer due diligence where the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing
- Shall apply on a risk-sensitive basis enhances customer due diligence and enhanced ongoing monitoring in any situation which by nature presents a higher risk of money laundering, terrorist financing activities or other criminal conduct on the basis of the national risk assessment
- May rely on regulated person or foreign regulated person to apply customer due diligence measures of a customer provided:
 - There is no suspicion of money laundering or terrorist financing activities
 - The following information is provided immediately on opening of the account or commencement of the business relationship:
 - Identity of each customer and beneficial owner
 - Purpose and intended nature of the business
 - Satisfied that the regulated person shall immediately provide it with the relevant information within 3 working days of request
 - Regulated person is subject to requirements equivalent to our Anti-Money Laundering Regulations Act 2002 and in line with international standards
 - Regulated person not prevented by professional privileges or any other restrictions to promptly share the information required
- To cease transaction where it is unable to apply customer due diligence measures
- Maintain accounts in true name
- To record and retain identification details in wire transfers
- Monitor customer activities and transactions
- Scrutinising transactions undertaken throughout the relationship to ensure that the transactions are consistent with the knowledge of the customer, the business and risk profile and the source of funds of the customer
- Keeping the customer due diligence up to date
- Maintain records for a minimum of 7 years



- Report suspicious activities within two business days of forming the suspicion or receiving the information
- The need to identify and verify the identity of a customer when establishing a business relationship; If the customer is a politically exposed person (“PEP”), a reporting entity shall adequately identify the person and verify his or her identity. In addition, to have appropriate risk management systems to determine whether the customer is a PEP.
- Take reasonable measures to ascertain the purpose of any transaction in excess of USD 10,000 or of USD 5,000 in the case of cash transactions and the origin and ultimate destination of the funds involved in the transaction;
- In relation to its cross-border banking and other similar relationships adequately identify the identity of the person, gather sufficient information about the nature of the business, assess the AML/CFT controls and obtain senior management’s permission before entering into a new relationship;
- To not proceed with a transaction if there is no satisfactory evidence of a customer’s identity;
- To maintain records on a customer’s identity for a minimum period of 7 years from the date of any transaction or correspondence or on which the business relationship ceases; A reporting entity that fails to maintain records is guilty of an offence.
- Maintain accounts in the clients’ true name;
- Ensure that money transmission includes accurate originator information on electronic funds transfers and that the information shall remain with the transfer;
- To monitor complex, unusual or large transactions with no apparent economic or lawful purpose as well as ongoing monitoring of business relationships /transactions undertaken throughout the course of the relationship;
- To report any transaction or attempted transaction that may be related to the commission of an offence of ML/FT to the FIU.
- Following the Anti-Money Laundering Regulations Act 2002 every reporting entity shall report each transaction that is carried out by or through it involving cash transactions of USD 5,000 or more or the equivalent money in the currency of other countries.
- The Company is required to register with the FIU within 60 days of commencement of the Anti-Money Laundering Regulations Act 2002 or of the commencement of business operations. In this respect, please note that the registration will be done electronically through a secured portal which will be set up by the FIU & there will be a fine not exceeding USD 10,000 for failure to register within the specified time period. In the event that there are any changes made to the



registered particulars, the FIU will have to be notified in writing of the changes within 30 days of such change. If the Company does not comply there will be a fine not exceeding USD 10,000 for failure to report any changes made. The following information will be required by the Company for the respective registration:

- a. Legal name of the natural person, legal person or legal arrangement
- b. Registration number, license number, or National Identity Number
- c. Full contact details of the reporting entity
- d. Full name and contact details of the compliance officer and the alternative compliance officer

Further to the abovementioned obligations, reporting entities should therefore ensure that their staff are fully aware of their obligations found in the law and abide by them so as to ensure compliance. Therefore, a reporting entity shall appoint compliance and reporting officer who shall be responsible for ensuring the reporting entity's compliance with the provisions of this Act.

Internal Controls, Policies and Procedures

Every Reporting Entity must take appropriate measures to make sure that its employees engaged in dealing with customers or processing business transactions maintain the identification and record-keeping procedures laid down in the Anti-Money Laundering Regulations Act 2002.

The Company shall maintain records of the following:

- a. customer due diligence measures, including account files, business correspondence and copies of all documents evidencing the identities of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with the provisions of this Act;
- b. all transactions carried out both domestically and internationally by it and correspondence relating to the transactions as is necessary to enable any transaction to be readily reconstructed at any time by the FIU or the Attorney-General, and the records shall contain particulars sufficient to identify —
 - the nature and date of the transaction;



- the type and amount of currency involved;
 - the type and identifying number of any account with the reporting entity involved in the transaction;
 - if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee (if any), the amount and date of the instrument, the number (if any) of the instrument and details of any endorsement appearing on the instrument;
 - the name and address of the reporting entity, and of the officer, employee or agent of the reporting entity who prepared the record;
- c. enquiries relating to money laundering and terrorist financing activities, made to it by the FIU.

However, the Company has an obligation to report suspicious transactions when it has reasonable grounds to suspect the following:

- reasonable grounds to suspect that any service, or transaction may be related to the commission of criminal conduct including an offence of money laundering or of terrorist financing activities or to money or property that is or represents the benefit of criminal conduct;
- information that may be relevant to an act preparatory to an offence or to money or property, information relevant to an investigation or prosecution of a person for an offence or of assistance in the enforcement of this Act or the Proceeds of Crime (Civil Confiscation) Act,
- the reporting entity shall submit a suspicious transaction report to the FIU within two business days of ascertaining the reasonable grounds, forming the
- suspicion of receiving the information.
- The FIU shall acknowledge receipt of the suspicious transaction report within 24 hours of its receipt

The Anti-Money Laundering Regulations Act 2002 requires the appointment of a senior officer with the necessary qualifications and experience as the Compliance and Reporting Officer (CRO)

The CRO shall be responsible for the following:

- a. identify, assess, advise on, monitor and report on the reporting entity's compliance with regulatory requirements and the suitability of its internal procedures on an on-going basis to the



Board or senior managers and to the respective supervisory authority upon request and if the compliance officer is the sole senior manager, the report shall be submitted to the respective supervisory authority;

- b. ensure that the reporting entity maintains a manual of compliance of the policies, procedures, and systems, — with a compliance framework, which shall be submitted to the supervisory authority for review, upon request;
- c. with all relevant anti-money laundering and countering the financing of terrorism legal and regulatory obligations of the reporting entity and the processes to allow the staff to report violations confidentially to the compliance officer; and
- d. to identify the procedures to be followed when there have been breaches or suspected breaches of regulatory requirements or internal policies;
- e. compliance officer shall ensure the compliance by staff of the reporting entity with the provisions of the manual of compliance maintained under paragraph (b) and the noncompliance of the provisions of the manual shall be recorded, showing the nature, form and period of non-compliance and such non-compliances shall be made available to the onsite examiners of the respective supervisory authority, for examination.
- f. to develop a compliance culture – to ensure that all directors and relevant staff are familiar with the laws and regulations of the Republic of Marshall Islands to combat money laundering and terrorist financing activities, which includes an understanding of the relevant compliance policies, procedures and systems of the reporting entity as well and the compliance officer imparts awareness of the need for compliance, thereby developing within the reporting entity a robust compliance culture;
- g. to monitor the developments and changes in the legislations, policies, standards and other guidelines issued by the international bodies in order to keep the reporting entity updated with the regulatory developments and changes in international requirements;
- h. to implement the training programme –
 - for directors and relevant staff which includes the training programme on general anti-money laundering and countering the financing of terrorism awareness, client acceptance procedures, know your customer (KYC) procedures, remediation and suspicious activity reporting relevant to the reporting entity's activities;
 - at least once in every year and whenever there are changes in the laws, regulations or international requirements to ensure that the directors and related staff are aware of the latest developments in the anti-money laundering and countering the financing of terrorism



- activities; (iii) to undergo additional training, in order to enhance his or her professional skills, at least once in every year;
- the Company with no more than five employees will not be required to develop a separate training program or conduct training as long as they ensure that all relevant staff members participate in anti-money laundering and countering the financing of terrorism trainings offered, or recommended by or on behalf of their respective supervisory authority at least once in every two years.
- i. to perform review of the compliance framework and make regular assessment reports to the senior management, identify the deficiencies and making recommendations for any updates or revisions;
 - j. reporting entities who have not more than five staff members shall conduct self-assessment of their compliance framework and institute any necessary updates or revisions and make available the self-assessment report to the respective supervisory authority, upon request;
 - k. to ensure the preparation and submission of an annual compliance report to the supervisory authority for information within 90 days after each calendar year and the reporting entities who have not more than five staff members may request authorisation from their respective supervisory authority to submit a compliance report, as may be determined by the supervisory authority, for information.

Identification Requirements

Reporting Entities must identify prospective customers at the time of opening of an account or entering into a business relationship. The duty to identify a customer and to keep informed of the customer's business continues after the relationship is established.

Unless satisfactory evidence of identity is obtained "*as soon as is reasonably practicable*" the reporting entity must not proceed any further with the transaction unless directed to do so by the Financial Intelligence Unit ("FIU"). The reporting entity is also required to report the attempted transaction to the FIU.

What constitutes an acceptable time to identify the customer must be determined in the light of all the circumstances including the nature of the business, the geographical location of the parties and whether



it is practical to obtain the evidence before commitments are entered into or money changes hands. Thus, the Reporting Entity can open an account or begin the business relationship provided that it promptly takes appropriate steps to verify the customer's identity.

When must the Identity be verified?

Whenever an account is to be opened or a continuing business relationship is entered into, the identity of the prospective customer must be verified. Reporting entities are required to obtain information on the purpose and nature of the business relationship. Thereafter as long as records are maintained, no further evidence of identity is needed unless the reporting entity has any reason for suspicions, for instance if there is a marked change in the nature or volume of business passing through the account.

Reporting entities are advised to develop a customer profile based on the information obtained. A customer profile will assist the reporting entity in identifying suspicious transactions and facilitate the monitoring of accounts and transactions.

Also, when a transaction is undertaken when there is no business relationship, or an electronic funds transfer is carried out, the reporting entity is required to take the identity of the customer. Furthermore, identity must be verified in all cases where money laundering or the financing of terrorism is suspected, or where there are doubts as to the veracity or adequacy of the identification information obtained.

If a natural person conducts a transaction through a reporting entity and the latter has reasonable grounds to believe that the person is undertaking the transaction on behalf of another person, the reporting entity shall identify and verify the identity of the ultimate beneficial owner for whom the transaction is being conducted.

The obligation to obtain evidence of identity is general. Identification is not required when it concerns an occasional cash transaction under USD 5,000, unless there is a suspicion that the transaction is unlawful. However, following Anti-Money Laundering Regulations Act 2002, when the Company is executing a cash transaction/wire transfer shall retain the details and report the particular concerning such transactions to the FIU. However, the Company shall report each transaction carried out by or through it involving cash transactions of USD 5,000 or more or the equivalent money in the currency of other countries.



Enhanced Identification Requirements

A reporting entity is under the obligation to take reasonable measures to ascertain the purpose of a transaction in excess of USD 10,000. In these cases the origin and ultimate destination of the funds should be established.

A reporting entity should have a risk management system to determine if a person is a PEP. If the customer is a PEP, a reporting entity must adequately identify the person and verify his or her identity, take reasonable measures to establish the source of wealth and the source of property, and regularly monitor the account. Approval of senior management should be obtained before establishing a business relationship with the customer. PEP are only persons holding prominent public positions in a foreign country.

A Reporting Entity shall in its cross-border correspondent banking and other similar relationships undertake enhanced measures when identifying and verifying the identity of the person with whom it conducts such a business relationship. These measures include gathering sufficient information about the nature of the business, use publicly available information to determine the reputation of the correspondent and the quality of supervision to which it is subject, assess the correspondent's AML/CFT controls. Approval of senior management should be obtained before establishing a new correspondent relationship.

Where the relationship is a payable-through account, a reporting entity shall ensure that the person with whom it has established the relationship has verified the identity of and performed on-going due diligence on the person's customers and have direct access to the accounts. The reporting entity shall also ensure that the person is able to provide the relevant customer identification data upon request and that it has a physical presence in the Republic under the law which it was established unless it is part of a group that is subject to supervision as a whole.

A reporting entity shall apply customer due diligence measures when:

- a. establishing business relationship;



- b. carrying out every one-off transaction; one-off transaction means a transaction carried out other than as part of a business relationship that exceeds USD 5,000 in cash or through wire transfers, whether the transaction is carried out in a single operation or several operations which appear to be linked.
- c. the reporting entity has doubts on the veracity or adequacy of documents, data or information obtained for the purpose of identification or verification of a customer; or
- d. there is reasonable suspicion of money laundering, terrorist financing activities or other criminal conduct.
- e. shall keep records relating to customer due diligence, ongoing monitoring, the safeguards exercised before relying on regulated persons and the business or services carried out by or with a customer or on his behalf;
- f. shall be made available on request to the respective supervisory authority and the FIU or the Attorney General or a prosecutor on behalf of Anti-Corruption Commission of Republic of Marshall Islands in the performance of their functions;
- g. shall be undertaken against every customer of the gambling sector, if the money involved in the gambling

The Company shall apply customer due diligence measures to existing customers at appropriate times on risk-sensitive basis. In order to determine the extent of customer due diligence measures on risk-sensitive basis or on the basis of national risk assessment, the Company shall identify the type of customer, business relationship, product or transaction; and the guidelines issued by the FIU or Supervisory Authority. In addition, the Company shall ensure to be able to demonstrate to its supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering, terrorist financing activities or other criminal conduct.

When there is suspicious of money laundering, financing of terrorism or other criminal conduct, the reporting entity shall apply the customer due diligence measures found in regulation.

Where a reporting entity knows or has reasonable grounds to believe that a customer, or a beneficial owner of a customer, residing in or outside Republic of Marshall Islands is or becomes a politically exposed person, the reporting entity shall apply, on a risk-sensitive basis, enhanced customer due diligence measures and enhanced ongoing monitoring. In addition, the reporting entity shall obtain the approval of the senior management before a business relationship is established with the customer, and



take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or one- off transaction.

Where a reporting entity relies on an intermediary or third party, it shall immediately obtain the identification data and ensure that copies are made available upon request without delay. Where the reporting entity is a financial institution, it shall satisfy itself that the third party or intermediary is regulated and supervised for and has measures to comply with the requirements of the Anti-Money Laundering Regulations Act 2002.

A reporting entity shall comply the requirements of this Act notwithstanding any obligations as to confidentiality or other restriction on the disclosure of information imposed any written law or otherwise.

Cessation of Operations

In the event that the Company plans to cease its operations, it shall notify the FIU, 14 days prior to such cessation, by electronic communication providing the justification and effective date. If the Company ceases to operate in the Republic of Marshall Islands shall, within 30 days from the date of ceasing its operations, handover all the records required to be maintained under the Act to their supervisory authority in electronic format.

Branches and subsidiaries:

A reporting entity shall require its branches and subsidiaries outside Republic of Marshall Islands to apply, to the extent permitted by the laws of the country where they are located, measures at least equivalent to those set out in the Regulations with regard to customer due diligence, ongoing monitoring and record- keeping.

Where no such equivalent customers due diligence measures are required under the laws of the country where the branches and subsidiaries are located, the reporting entity shall

- a. Inform its supervisory authority accordingly



- b. Apply the customer due diligence measures provided in the Regulations, as applicable to the risk of money laundering, financing of terrorism or other criminal conduct and
- c. Produce to the FIU, without delay on request, all information data and documents in the possession or control of such branch or subsidiary undertaking in accordance with the obligations of the reporting entity under the Regulations.

Liability of employers and principals

Further to the Anti-Money Laundering Regulations Act 2002, any act done or omission made by a person as an employee or agent shall be treated as done or made by that person's employer or principal if it was done or made with the knowledge or approval of the employer or principal or without such knowledge or approval if it was the result of lack of supervision, provided, in the case of an agent, that he or she acted within the terms of his or her agency or contract.

Liability of Directors

Where anybody corporate is convicted of an offence under the Anti-Money Laundering Regulations Act 2002 or any Regulations made under the Act, every person being the director, controller or officer concerned in the management of the body corporate shall be guilty of the offence where it is proved that the act or omission that constituted the offence took place with that person's knowledge, authority, permission or consent.



Trust Company Complex,
Ajeltake Road
Ajeltake Island, Majuro,
Republic of the Marshall
Islands, MH 96960

Local Call 22 222033
Phone +(357) 22 222033

www.baxiamarkets.com
support@baxiamarkets.com