

Volume: 55 Issue: 172 Date: 16 Jumaadhal Aakhira 1448 – 25 November 2026 Wednesday

Regulation No: 2026/R-95

REGULATION ON SIMPLIFIED AND ELECTRONIC CUSTOMER DUE DILIGENCE

The President's Office
Boduthakurufaanu Magu
Male, Maldives'

Phone: 3336211
Mobile: 7242885

Website: www·gazette·gov·mv

- For publication of regulations and guidelines in the Gazette, send to legalaffairs@po·gov·mv

بسم الله الرحمن الرحيم

Maldives Monetary Authority

Republic of Maldives

REGULATION ON SIMPLIFIED AND ELECTRONIC CUSTOMER DUE DILIGENCE

Table of Contents

CHAPTER ONE: PRELIMINARY 1
1. Introduction 1
2. Short Title 1
3. Applicability 1

CHAPTER TWO: RISK-BASED APPROACH AND RISK ASSESSMENT 2
4. Responsibility for Compliance 2
5. Risk Assessment 3
6. Internal Control Requirements 4

CHAPTER THREE: DUE DILIGENCE REQUIREMENTS AND VERIFICATION STANDARDS 5
7. Application of Simplified Due Diligence 5
8. Enhanced Customer Due Diligence for High Risk 6
9. Verification of Beneficial Owners 6

CHAPTER FOUR: ELECTRONIC CUSTOMER DUE DILIGENCE AND THIRD-PARTY RELIANCE 6
10. Electronic Customer Due Diligence Methods 6
11. Electronic Identification and Verification Methods 7
12. Identification and Verification Through Video Call 7
13. Reliance on Third Parties 9

CHAPTER FIVE: CUSTOMER PROTECTION 10
14. Customer Protection 10

CHAPTER SIX: RECORD KEEPING AND DATA PROTECTION 11
15. Record Keeping Requirements 11
16. Transitional Arrangements 12
17. Definitions 13
18. Commencement 15

بسم الله الرحمن الرحيم

Maldives Monetary Authority

Republic of Maldives

REGULATION ON SIMPLIFIED AND ELECTRONIC CUSTOMER DUE DILIGENCE

CHAPTER ONE: PRELIMINARY

1. Introduction

(a) This Regulation is issued pursuant to paragraph (a), subparagraph (3) of section 75 of Law No.: 10/2014 (Prevention of Money Laundering and Financing of Terrorism Act).

(b) This Regulation sets out the minimum requirements and standards that Reporting Entities must follow during the identification and verification of Customers through Simplified Due Diligence measures and Electronic Customer Due Diligence methods.

2. Short Title

This Regulation shall be cited as the "Regulation on Simplified and Electronic Customer Due Diligence".

3. Applicability

(a) This Regulation applies to the following persons:

i. Banks;

ii. Financing Companies;

iii. Payment Services Providers that provide any of the following services;

1. Account Information Service;

2. Electronic Money Issuance Service;

3. Payment Initiation Service;

4. Payment Transactions Acquisition Service; and

5. Remittance Service.

iv. Insurance Companies and intermediaries, when they engage in life insurance and family takaful businesses;

v. Any of the following persons licensed and regulated by the Capital Market Development Authority under the Law No.: 2/2006 (Maldives Securities Act):

1. dealing company;

2. investment advisers;

3. fund managers;

4. underwriters;

5. stock exchange companies; and

6. any other person designated by the Authority in consultation with the Capital Market Development Authority.

vi. Money Changing Businesses;

vii. Designated Non-Financial Businesses and Professions as defined in the Act; and

viii. Any other Reporting Entity determined by the Authority.

(b) Reporting Entities shall follow the requirements and standards set forth in the Act and other applicable regulations and guidelines for matters not covered by this Regulation.

CHAPTER TWO: RISK-BASED APPROACH AND RISK ASSESSMENT

4. Responsibility for Compliance

(a) Each Reporting Entity shall take a risk-based approach in complying with this Regulation.

(b) For Reporting Entities that are companies, the board of directors shall ensure the effective implementation of appropriate policies and procedures to address any risks associated with the identification and verification of Customers through Simplified Due Diligence measures or Electronic Customer Due Diligence methods. These include operational, customer information-related, information technology, and money laundering and terrorism financing risks.

(c) For Reporting Entities operating as Sole Proprietorships, the individual proprietor shall be responsible for developing and ensuring the effective implementation of appropriate policies and procedures to address any risks associated with the identification and verification of Customers through Simplified Due Diligence measures or Electronic Customer Due Diligence methods.

(d) In the case of Reporting Entities operating as Partnerships, the managing partner or controlling partner(s) shall be responsible for developing and ensuring the effective implementation of such policies and procedures.

(e) The policies and procedures specified under paragraphs (b), (c) and (d) must address, at a minimum, operational, customer information-related, information technology, and money laundering and terrorism financing risks associated with the identification and verification of Customers through Simplified Due Diligence measures and Electronic Customer Due Diligence methods.

(f) The responsible persons specified in paragraphs (b), (c) and (d) shall ensure that the employees, agents, and any third parties to whom they have outsourced functions of their respective Reporting Entity, and where applicable, their subsidiaries and branches, comply with this Regulation.

5. Risk Assessment

(a) Reporting Entities shall assess money laundering and terrorism financing risks prior to using Simplified Customer Due Diligence measures or Electronic Customer Due Diligence methods set out in this Regulation for the identification and verification of Customers. Such risk assessments shall be;

i. conducted in accordance with the Reporting Entity's documented risk assessment methodology and risk appetite, having regard to the Customer's status, and the risks associated with the product, service, delivery channel, geographical location and transactions; and

ii. take into account the national and sectoral risks, the global risk context, and other relevant regulatory or supervisory information.

(b) Prior to implementing Electronic Customer Due Diligence methods, Reporting Entities shall assess technology, data protection, cybersecurity, and third-party service provider risks. In particular, Reporting Entities shall specifically assess risks related to:

i. the risk of identity fraud or impersonation including the use of deep-fake technology, generative artificial intelligence, or other synthetic media to defeat verification processes;

ii. the risk of data interception or breach, including the compromise of biometric data or verification credentials;

iii. the reliability and independence of the data sources used, including the vulnerability of such sources to AI-generated or manipulated inputs;

iv. the potential for exploitation of the technology or method by criminals, including presentation attacks, injection attacks, and the use of compromised or stolen biometric templates; and

v. the adequacy of the Reporting Entity's liveness detection and anti-spoofing measures to detect and prevent the use of deepfakes, synthetic media, and other AI-powered impersonation techniques.

(c) Reporting Entities shall develop and implement appropriate policies, procedures, and control measures to effectively manage and mitigate the risks identified under paragraph (a) and (b).

(d) Reporting Entities shall document the risk assessment method and basis under paragraph (a) and (b).

(e) The risk assessment shall be reviewed and updated whenever the technology or method is materially changed, or at least annually, whichever is sooner. For the purposes of this section, a "material change" means any modification to the technology, methodology, process, model, system, data source, control, or operating environment used in the customer due diligence process that could reasonably affect the integrity, reliability, effectiveness, accuracy, security, or outcomes of customer due diligence conducted by the institution.

(f) For the purposes of this Regulation, the outcome of a risk assessment conducted under this section shall determine whether the customer relationship or transaction qualifies as lower risk, or high risk, or is otherwise subject to the standard customer due diligence measures prescribed under the Act and any applicable regulations issued for Reporting Entities.

6. Internal Control Requirements

(a) Prior to the implementation of Simplified Due Diligence measures or Electronic Customer Due Diligence methods, all Reporting Entities shall update their internal programs for the prevention of money laundering and financing of terrorism, as required under section 21 of the Act.

(b) A Reporting Entity that provides Payment Transaction Execution Service as part of its licensed or permitted activities and uses Simplified Due Diligence measures or Electronic Customer Due Diligence methods for the identification and verification of Customers during onboarding shall implement automated systems to monitor transactions initiated thereafter.

(c) Reporting Entities shall ensure that their employees are properly trained in the identification and verification of Customers through Simplified Due Diligence measures and Electronic Customer Due Diligence methods. For Reporting Entities that are Sole Proprietorships or Partnerships without employees, compliance with this requirement may be satisfied by maintaining documented evidence that the individual practitioner or partners have familiarised themselves with this Regulation and any relevant guidance issued by the Authority or their respective supervisory body.

(d) Reporting Entities that are part of a financial group shall implement group-wide policies and procedures for Simplified Due Diligence measures and Electronic Customer Due Diligence methods, ensuring consistent application of risk-based measures and methods across all branches and subsidiaries.

CHAPTER THREE: DUE DILIGENCE REQUIREMENTS AND VERIFICATION STANDARDS

7. Application of Simplified Due Diligence

(a) Reporting Entities may apply Simplified Due Diligence measures under this Regulation only to Customers who are natural persons and where a risk assessment under section 5 has identified a lower risk.

(b) The scope and extent of Simplified Due Diligence applied shall be commensurate with the identified level of risk. Reporting Entities shall not apply simplified measures that are disproportionate to the level of risk identified.

(c) Reporting Entities shall document the basis for determining that Simplified Due Diligence is appropriate in each case or category of Customers, including reference to the specific lower risk factors identified.

(d) Simplified Due Diligence measures shall not be applied where:

i. the Customer acts on behalf of, conducts a transaction for the benefit of, or is represented by another person, whether directly or indirectly;

ii. there is any suspicion of money laundering or financing of terrorism, regardless of the risk level determined under the risk assessment;

iii. specific high-risk scenarios are identified that cannot be appropriately mitigated;

iv. the Reporting Entity is unable to comply with the minimum Simplified Due Diligence measures set out in this section;

v. a Customer initially onboarded under Simplified Due Diligence measures is subsequently identified as presenting a risk level other than lower risk, in which case the Reporting Entity shall immediately cease to apply Simplified Due Diligence measures and shall conduct the appropriate level of customer due diligence necessary to manage the risk identified;

vi. the Customer is a business registered under Law No. 18/2014 (Business Registration Act); and

vii. the Authority determines any other circumstances or persons to whom or circumstances in which Simplified Customer Due Diligence shall not apply.

(e) Where a lower risk has been established under section 5 for a Customer, at a minimum, a Reporting Entity shall apply the following as the Simplified Due Diligence measures:

i. identify and verify the identity of the Customer, by collecting their full name, including any aliases, identification number (e.g. identity card number, passport number, Visa number, or work permit number, date and place of birth, current residential and permanent address, contact address, contact information, nationality, and any other documentation that identifies the Customer; and

ii. any other Simplified Customer Due Diligence measures prescribed by the Authority.

(f) For the purpose of identification and verification under paragraphs (e)(i) and e(ii), the Reporting Entities may use any one of the Electronic Customer Due Diligence methods specified in paragraph 11 (b).

(g) Verification may be completed after the establishment of the business relationship, provided that the relationship is subject to monitoring and that verification is completed within a reasonable timeframe not exceeding thirty (30) days.

(h) Where a lower risk has been established under section 5 for a Customer, a Reporting Entity shall review, update, and verify the Customer's due diligence information at least once every five (5) years from the date of the last review, and shall do so earlier where it becomes aware of a change in the Customer's risk profile or any other circumstance that may affect the level of money laundering or terrorist financing risk associated with the Customer.

8. Enhanced Customer Due Diligence for High Risk

(a) Where a risk assessment under section 5 identifies a high risk, the Reporting Entity shall apply enhanced due diligence measures as required under the regulations applicable to Reporting Entities and the Act.

(b) Nothing in this Regulation shall be construed to limit or reduce the enhanced due diligence obligations imposed on Reporting Entities under the Act, including any applicable regulations or guidelines issued by the Authority or the relevant supervisor.

(c) Reporting Entities shall ensure that customer due diligence information, records, and verification documentation are reviewed and updated in accordance with the requirements set out in the Act, and the regulations issued by the Authority or the relevant supervisor.

9. Verification of Beneficial Owners

(a) Regardless of whether the Customer is a natural or legal person, Reporting Entities shall identify and take reasonable measures to verify the identity of the Beneficial Owner(s).

(b) Reporting Entities may use the Electronic Customer Due Diligence methods provided in this Regulation for the verification of Beneficial Owners at any risk level, provided that the specific verification standards applicable to the relevant risk level are satisfied.

(c) Where the Beneficial Owner presents a higher money laundering or terrorist financing risk than the Customer, or where the Reporting Entity has doubts about the veracity or adequacy of Beneficial Ownership information, the Reporting Entity shall apply verification measures commensurate with that higher risk level.

CHAPTER FOUR: ELECTRONIC CUSTOMER DUE DILIGENCE AND THIRD-PARTY RELIANCE

10. Electronic Customer Due Diligence Methods

(a) Electronic Customer Due Diligence methods under this Regulation may be applied at any risk level, subject to the following:

i. For lower risk, Electronic Customer Due Diligence methods may be used as a standalone verification method; and

ii. For high risk, Electronic Customer Due Diligence methods must be combined with enhanced customer due diligence measures prescribed in the applicable regulations issued for Reporting Entities.

(b) This Regulation does not limit or reduce any enhanced due diligence obligations imposed by the Act or under the regulations issued by the Authority or by a supervisor for high-risk Customers.

11. Electronic Identification and Verification Methods

(a) This section applies whenever a Reporting Entity chooses to identify and verify the identity of Customers, Beneficial Owners, and any third parties who act on behalf of the Customer using Electronic Customer Due Diligence methods.

(b) Permitted Electronic Customer Due Diligence methods include:

i. identification and verification of the persons specified in paragraph (a), or other relevant documentation or information by obtaining a soft copy of the relevant document(s), combined with a live video call in accordance with section 12 of this Regulation;

ii. identification and verification of the persons specified in paragraph (a), or other relevant documentation or information through a Government System;

iii. identification and verification of the persons specified in paragraph (a) or other relevant documentation or information through a Bank or any other entity authorized by the Authority subject to section 13;

iv. identification and verification of the persons specified in paragraph (a) or other relevant documentation or information through a biometric authentication linked to a Government System; or

v. any other Electronic Customer Due Diligence methods prescribed by the Authority.

(c) The paragraph (b) does not prohibit supplementary verification of mobile numbers, email, or authenticator applications. Where mobile number or email verification is conducted, it must be executed via a One-Time Password (OTP) and shall not substitute for primary identity proofing.

12. Identification and Verification Through Video Call

(a) All Reporting Entities subject to this Regulation may use video call as a method of Electronic Customer Due Diligence.

(b) Video calls shall be treated as a method of identification and verification, and shall not be used as a determinant of risk level. It may be used for the identification and verification of Customers, Beneficial Owners, and third parties who act on behalf of the Customers at any risk level, subject to the following conditions:

i. For lower risk, video call may be used as a standalone method of identification and verification, including under Simplified Due Diligence where permitted in this Regulation.

ii. For high risk, video call identification and verification must be combined with enhanced customer due diligence measures prescribed in the Act and applicable regulations issued for Reporting Entities.

(c) Reporting Entities shall not use video call for identification and verification purposes where:

i. the Reporting Entity has doubts about the authenticity of the identification document provided and presented during a video call;

ii. the quality of the video connection prevents clear verification of the identity of the persons specified in paragraph (b) and the document details;

iii. the Customer, Beneficial Owner, or the Customer's authorised representative refuses to comply with the requirements of this section;

iv. the Reporting Entity suspects money laundering or terrorist financing; or

v. any other circumstances prescribed by the Authority.

(d) Identification and verification through video call shall include the following stages:

i. checking the veracity of the identification documents obtained;

ii. obtaining a colour photo of the Customer, Beneficial Owner, or the authorised representative of the Customer and the identification document of the Customer, Beneficial Owner or the Customer's authorised representative, where applicable, during the video call conducted for identification and verification purposes, by taking a screenshot that meets the following requirements:

1. the quality of the photo must be sufficient to compare it with the photo on the identification document;

2. the Customer, Beneficial Owner, or the Customer's authorised representative's face and the identification documents must be clearly visible;

3. the Customer, Beneficial Owner, or the Customer's authorised representative's face must not be covered by foreign objects such as masks or scarves, provided that nothing in this subparagraph shall be construed to prohibit religious head coverings where the full face (eyes, nose, and mouth) remains clearly visible for comparison with the identification document;

4. no person other than the Customer, Beneficial Owner, or Customer’s authorised representative, as applicable, shall appear in the photo. Where the Customer is a legal person or arrangement, the photo shall include only the individual undergoing the electronic identification and verification process on behalf of that entity.; and

5. any other requirements prescribed by the Authority.

iii. verifying the identification document by comparing the photo in the identification document and the photo obtained during the video call.

(e) Video call identification and verification may be performed manually, automatically, or by a combination of both.

(f) If video call identification and verification are performed manually, Reporting Entities shall ensure that employees who participate in the process are appropriately trained.

(g) Reporting Entities shall ensure that automated face recognition software, if used, employs active liveness detection technology capable of detecting and rejecting deepfakes, presentation attacks, and injection attacks. The information system used must not allow the use of static images, pre-recorded videos, or digitally manipulated or AI-generated media.

(h) The liveness detection technology employed under paragraph (g) shall, at a minimum, meet the following standards:

i. it must be capable of verifying that the individual is physically present in real-time during the identification and verification process;

ii. it must be capable of detecting and rejecting presentation attacks, including the use of printed photographs, digital screens, pre-recorded videos, and three-dimensional masks (including silicone, latex, or resin face coverings designed to impersonate a Customer), and other similar devices or materials;

iii. it shall be capable of detecting and rejecting injection attacks, including digitally injected or synthetic video streams;

iv. it shall be tested and configured to achieve a false acceptance rate no higher than such threshold as may be specified by the Authority;

v. the Reporting Entity shall retain evidence of conformance testing or vendor certification demonstrating that the liveness detection technology meets the standards set out in this paragraph; and

vi. any other standards prescribed by the Authority.

(i) Reporting Entities shall be responsible for the customer due diligence procedures, irrespective of the function being outsourced or the usage of outsourced information systems or technologies.

13. Reliance on Third Parties

(a) Reporting Entities may rely on a third party or a third party-operated information system for the identification and verification of Customers.

(b) Unless specified otherwise in this Regulation, a third party or a third party-operated information system shall be a Bank or any other entity authorised by the Authority.

(c) The third party shall obtain the written consent of the Customers before sharing their information or a document containing their information with a Reporting Entity for the purposes of identification or verification.

(d) Reporting Entities shall enter into a written contract if they rely on a third party for the identification and verification of Customers.

(e) Reporting Entities shall ensure that the contracts with third parties contain provisions that require the third parties to make available to the Reporting Entity, upon request and without delay, identification information and relevant documentation related to the identification and verification of Customers.

(f) The Banks and entities authorised by the Authority may develop framework contracts to act as third parties for the purpose of this Regulation. Such contracts shall not be discriminatory.

(g) Third parties shall comply with the Authority's requirements to include certain terms and conditions in the contracts to ensure that the terms of such contracts are not discriminatory and do not impose excessive obligations on the parties.

(h) Reporting Entities shall bear the ultimate responsibility for Customer due diligence where they rely on a third party.

CHAPTER FIVE: CUSTOMER PROTECTION

14. Customer Protection

(a) Reporting Entities shall act in good faith and provide Customers with clear, accessible, and timely information regarding the procedures used for identification and verification, including whether such procedures are conducted through electronic means, and, where applicable, the risk-based application of Simplified Due Diligence measures.

(b) Reporting Entities shall use encryption when exchanging information through electronic means to ensure that Customer data is properly protected. In the absence of specific standards set for such encryption by the Authority, the Reporting Entity shall use encryption in accordance with international best practices.

(c) Where a Reporting Entity processes Customer personal data for purposes ancillary to the mandatory customer due diligence obligation, including, but not limited to, the use of facial recognition technology, biometric liveness detection, or the storage of video call recordings, the Reporting Entity shall obtain the Customer's explicit consent prior to commencing such processing.

i. Consent obtained for such ancillary processing shall be separate and distinct for each purpose and shall be in explicit form; the date, time, and other relevant information evidencing the consent, and a record shall be retained in accordance with section 15.

(d) Nothing in this section shall be construed to require Customer consent for the identification and verification measures that are mandated under the Act, or this regulation where Simplified Customer Due Diligence measures or Electronic Customer Due Dilligence methods are used by a Reporting Entity, or by any other applicable regulations or guidelines issued by the Authority or the relevant supervisory authority. Customer's refusal to provide

the requisite identification information or comply with customer due diligence requirements shall result in the Reporting Entity declining to establish or maintain the business relationship, in accordance with the Act, or any other applicable regulations or guidelines issued by the Authority or the relevant supervisory authority.

(e) Where Electronic Customer Due Diligence methods involve the collection or processing of biometric data, the Reporting Entity shall:

i. obtain separate and explicit consent specifically referencing the collection of biometric data;

ii. inform the Customer of the purpose, duration of storage, and deletion policy for such biometric data; and

iii. ensure that biometric data is stored separately from general identification records where technically feasible either through logical or physical separation. Any means of separation adopted by the Reporting Entity is acceptable where the Reporting Entity can demonstrate that biometric data is adequately protected through strong encryption, restricted access controls, segregation of duties, audit trails, monitoring, and other appropriate safeguards proportionate to the sensitivity and risk of the data.

(f) Consent obtained for the processing of personal data for customer due diligence purposes shall be separate and distinct from any consent obtained for other purposes.

(g) A Customer's refusal to provide consent for ancillary processing shall not prevent the Customer from accessing financial services, provided that alternative, compliant means of customer due diligence are available.

(h) For the purpose of this section, Customer consent may be obtained in either electronic form or physical written form.

CHAPTER SIX: RECORD KEEPING AND DATA PROTECTION

15. Record Keeping Requirements

(a) Reporting Entities shall keep all information related to electronic identification and verification for a minimum period of five (5) years, in line with section 20 of the Act. Where a Reporting Entity has a reason to believe that any such information might be required for an investigation or legal proceeding, the Reporting Entity must keep such information for such period until such information is no longer required for an investigation or legal proceeding.

(b) The records required to be retained under paragraph (a) shall include, at a minimum, the following:

i. Customer identification data collected during the verification process, including name, date of birth, identification number, and contact details;

ii. One-Time Password (OTP) logs, including the mobile number to which the OTP was sent, the date and time of transmission, and confirmation of receipt;

iii. Biometric session outputs, including facial geometry templates, liveness detection results, and biometric match or non-match records;

iv. Full video recordings of any video call conducted for identification purposes, or at minimum, a clipped segment that includes the verification of the identification document and the liveness check. The retained recording must clearly show the individual's face and the identification document presented;

v. Colour screenshots captured during the video call identification and verification process in accordance with section 12;

vi. Consent records, including the date, time, and method by which consent was obtained and biometric data collected as specified in this Regulation;

vii. Metadata associated with the verification session, including the date and time of verification, the method or methods used, the IP address or device identifier, the geographic location (if captured), and the identity of the verifying officer (if applicable);

viii. Government System query confirmations and responses; and

ix. Third-party verification records and contracts, where reliance is placed on a third party under section 13.

(c) Reporting Entities shall maintain records in a manner that allows them to be retrieved and provided without delay upon receipt of a lawful request from the Authority, the Financial Intelligence Unit, or the relevant supervisory body.

(d) Where a Reporting Entity maintains an electronic information system for Customer management, all products and services provided to Customers who were onboarded using Electronic Customer Due Diligence methods shall be classified accordingly within that system.

(e) This Regulation does not impose a general obligation on Reporting Entities to retrospectively remediate, or re-record video identification sessions conducted prior to the commencement of this Regulation, provided that such sessions complied with the legal and regulatory requirements in force at the time of recording.

(f) Where a Reporting Entity has reason to believe that a video recording, taken and maintained before commencement of this Regulation, may be relevant to an ongoing or anticipated investigation, inquiry, or legal proceeding, the Reporting Entity shall retain such recording and disclose its existence to the requesting authority, regardless of whether the recording meets the technical standards set out in this Regulation.

16. Transitional Arrangements

(a) All Reporting Entities shall ensure full compliance with this Regulation within six (6) months from the date on which this Regulation comes into force.

(b) Notwithstanding paragraph (a), a Reporting Entity that, at the date this Regulation comes into force, already has in place procedures for Electronic Customer Due Diligence methods shall review and update such procedures to align with the specific requirements of this Regulation, including, but not limited to, video call standards, liveness detection, and video

recording retention requirements. Such updates shall be completed within three (3) months from the date on which this Regulation comes into force.

(c) A Reporting Entity that does not have Electronic Customer Due Diligence methods in place at the date this Regulation comes into force but wishes to implement such methods after the commencement date must ensure that any new Electronic Customer Due Diligence system or process complies fully with this Regulation prior to its deployment or use with Customers.

(d) Nothing in this Regulation prevents a Reporting Entity from voluntarily applying the standards set out in this Regulation to its existing customer base as part of a risk-based remediation or data-cleansing exercise

17. Definitions

In this Regulation, unless the context otherwise requires:

(a) “Account Information Service” has the same meaning as provided in Regulation No.: 2022/R-42 (Regulation on Payment Services), issued by the Authority;

(b) "Act" means Law No.: 10/2014 (Prevention of Money Laundering and Financing of Terrorism Act);

(c) “Authority” means the Maldives Monetary Authority established under Law No.: 6/81 (Maldives Monetary Authority Act 1981);

(d) "Automated Systems" means any system-based transaction monitoring tools capable of identifying or flagging unusual, suspicious, or higher-risk transactions. It does not mandate a specific technology solution, provided the system used is appropriate to the Reporting Entity's size, nature, complexity, and money laundering and terrorism financing risk exposure;

(e) “Bank” has the same meaning as provided in Law No.: 24/2010 (Maldives Banking Act);

(f) “Beneficial owner” has the same meaning as provided in Law No.: 10/2014 (Prevention of Money Laundering and Financing of Terrorism Act);

(g) “Capital Market Development Authority” means the authority established under Law No.: 2/2006 (Maldives Securities Act);

(h) “Customer” includes natural or legal persons;

(i) “Electronic Money” has the same meaning as provided in Law No.: 8/2021 (National Payment System Act);

(j) “Electronic Money Issuance Service” has the same meaning as provided in Regulation No.: 2022/R-42 (Regulation on Payment Services), issued by the Authority;

(k) “Financing Business” has the same meaning as provided in Regulation No.: 2021/R-132 (Regulation on Financing Business), issued by the Authority;

(l) “Financing Company” means a company licensed by the Authority to conduct Financing Business in the Maldives;

(m) "Government System" means an identity verification system that is operated, maintained, authorised, or recognised by the government and used for the purpose of verifying the identity of individuals and entities, and includes any such system operated and maintained or recognised by the Authority;

(n) “Insurance Company” means a company licensed by the Authority to conduct insurance business in the Maldives;

(o) “Money Changing Businesses” means entities licensed by the Authority to carry on the business of buying and selling foreign currencies;

(p) “Payment Initiation Service” has the same meaning as provided in Regulation No.: 2022/R-42 (Regulation on Payment Services), issued by the Authority;

(q) “Payment Service” has the same meaning as provided in Law No.: 8/2021 (National Payment System Act);

(r) “Payment Services Provider” has the same meaning as provided in Law No.: 8/2021 (National Payment System Act);

(s) “Payment Transaction” means the placing, transferring or withdrawing of money; where money includes Electronic Money;

(t) “Payment Transactions Acquisition Service” has the same meaning as provided in Regulation No.: 2022/R-42 (Regulation on Payment Services), issued by the Authority;

(u) “Payment Transaction Execution Service” has the same meaning as provided in Regulation No.: 2022/R-42 (Regulation on Payment Services);

(v) “Regulator” or “Supervisor” means:

i. the Authority, in the case of Reporting Entities licensed or regulated by the Maldives Monetary Authority;

ii. the Capital Market Development Authority, in the case of Reporting Entities licensed by the Capital Market Development Authority; and

iii. in the case of Designated Non-Financial Businesses and Professions (DNFBPs), the respective supervisory body or self-regulatory organization designated under the Act or any other law to oversee compliance with anti-money laundering or countering financing of terrorism obligations for that profession or sector.

(w) “Remittance Service” has the same meaning as provided in Law No.: 8/2021 (National Payment System Act);

(x) “Reporting Entities” has the same meaning as provided in Law No.: 10/2014 (Prevention of Money Laundering and Financing of Terrorism Act);

(y) "Electronic Customer Due Diligence methods" means the process of identifying and verifying a Customer using electronic methods, where the Customer is not physically present for identification purposes;

(z) "Simplified Due Diligence measures" means the application of reduced or less stringent measures for the identification and verification of a Customer, commensurate with a demonstrably lower risk;

(aa) “Partnership” shall have the meaning given in Law No. 13/2011 (the Partnerships Act);

(bb) “Company” shall have the meaning given in Law No. 7/2023 (Companies Act); and

(cc) “Sole Proprietorship” shall have the meaning given in Law No. 19/2014 (Sole Proprietorships Act).

18. <u>Commencement</u>

This Regulation shall come into force on the date on which it is published in the Government Gazette.