Anti-Money Laundering Regulations, 2002

BANKING ACT

Arrangement of Sections

Anti-Money Laundering Regulations, 2002

BANKING ACT

The Banking Commissioner pursuant to Section 181 of the Banking Act, 17 MIRC, Chapter 1, as amended, hereby makes Regulations in respect to matters related to Anti-Money Laundering and Countering the Financing of Terrorism.

(a) *Definitions*. For the purposes of these Regulations, the terms defined in §102 of the Act have the meanings set forth therein. In addition, for purposes of these Regulations, unless the context otherwise requires:

(1) "Act" – means the Banking Act 1987, 17 MIRC, Chapter 1;

(2) "acting in concert" – means knowing participation in a joint activity or parallel action towards a common goal of acquiring control of a bank or FSP, whether or not pursuant to an express agreement;

(3) "AML/CFT Program" – means documented internal policies, procedures and controls designed to ensure that the entity complies with the Banking Act, these Regulations and any guidance provided by the Banking Commission on AML/CTF.

(4) "Attorney General" – means the Attorney General appointed pursuant to the Constitution of the Republic of the Marshall Islands;

(5) "Banking Commissioner" – means the Commissioner of Banking appointed under the Act;

(6) "batch transfer" – means a transfer comprised of a number of individual transfers of funds or value, whether by wire transfer or otherwise, that are being sent by, or to, the same financial institution, but may/may not be ultimately intended for different persons;

(7) "Beneficial Owner" – means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to ultimate ownership or control and ultimate effective control refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control;

(8) "control" of a bank or FSP for purposes of Section 1(c) to (f) – means:

(i) the power, directly or indirectly, to direct the management or policies of a bank or FSP; or

(ii) to vote 10% or more of any class of voting shares of a bank or FSP;

(9) "cross-border transfer" – means any transfer of funds or value, whether by wire transfer or otherwise, where the originator and beneficiary institutions or customers

(Rev. 05/13/2010)
(Rev. 01/30/2014)
(Rev. 05/16/2019)
(Rev. 05/27/2021)

are located in different jurisdictions. This also refers to any chain of transfers that has at least one cross-border element;

(10) "domestic transfer" – means any transfer of funds or value, whether by wire transfer or otherwise, where the originator and beneficiary institutions or customers are located in the same jurisdiction. This refers to any chain of transfers that takes place entirely within the borders of a single jurisdiction, even though the system used to effect the transfer may be located in another jurisdiction;

(11) "financial group" – means a group that consists of a parent company (or any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles), together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level;

(12) "FSPs" – means "financial services providers" as defined in the Act;

(13) "identify" – in relation to natural persons, means to ascertain the genuine full name, date of birth, address, nationality, and occupation/business or principal activity through reliable, verified means;

"identify" – in relation to legal persons and arrangements, means to ascertain the registered name, address, business or principal activity through reliable, verified means as well as identifying the natural persons who are the director(s), secretary, beneficiaries, settlors, trustees, beneficial owners and signatories/operators of the account(s);

"institution affiliated party" – means any director, officer, employee or person who:

(i) owns or controls a bank or FSP, or

(ii) participates in the conduct of the affairs of a bank or FSP;

(14) "legal arrangement" – means express trusts, long-term irrevocable bank trusts, trusteeships, and other similar arrangements;

(15) "legal person" – means any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This includes bodies corporate, foundations, partnerships, associations and similar bodies.;

(16) "money or value transfer services" or "MVTS" – means a financial service that accepts cash, cheques, other monetary instruments or other stores-of-value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer or through a clearing network to which the MVT service belongs. Transactions performed by such services can involve one or more intermediaries and a third party final payment.;

(17) "Politically exposed person" – means any person who is or has been entrusted with a prominent public function in a foreign country including, but not limited to Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned companies, and important political party officials. Family members and close associates who have business relationships with such persons are also included herein;

(18) "senior management" – means an officer or employee of the bank, FSP, or DNFBP with sufficient knowledge of its money laundering and terrorist financing risk exposure, and sufficient authority, to make decisions affecting its risk exposure;

(19) "settlor" – means the settlor as defined in the Trust Act of 1994, 50 MIRC, Chapter 1;

(20) "shell bank" – means a bank that has no physical presence (i.e. no meaningful mind and management) in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision;

(21) "third party" – means a person relied on by a bank or FSP to perform some of the elements of the customer due diligence process or to introduce business to the bank or FSP;

(22) "trustee" – means a person performing functions under Part II of the Trust Act of 1994, 50 MIRC, Chapter 1;

(23) "VASP" – means "virtual asset service provider" as defined in the Act;

(24) "virtual asset transfer" – means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another;

(25) "wire transfer" – means any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and beneficiary may be the same person.

Subject to this subsection (b), any term that is defined in the FATF Recommendations (including its General Glossary) but not in §102 of the Act or in these Regulations has the same meaning in these Regulations as in the FATF Recommendations.

Section 1. Persons Associated With or Who Control Banks and Financial Services Providers.

(a) Each bank and Financial Services Provider ('FSP') shall identify, obtain the requisite information, retain records and file with the Banking Commissioner reports regarding persons affiliated with or who own or control the bank or FSP to the extent and in the manner required by this Section 1.

(b) *Recordkeeping*

Each bank and FSP shall:

(1) adopt a methodology by which it will identify all persons who, acting alone or in concert with one or more persons, owned or controlled the bank or FSP at any time during the immediately preceding calendar year;

(2) adopt a methodology by which it will ascertain whether any institution affiliated party has been convicted of any offense involving dishonesty, breach of trust or money laundering; and

(3) record the information gathered pursuant to this subsection (c)(1) and (2) in a report no later than thirty (30) days following the end of the year.

(c) The Compliance Officer, as designated by each bank or FSP pursuant to Section 2A (Internal Policies, Procedures, Policies, and Training), shall certify that the information collected and retained by the bank or FSP pursuant to subsection (c)(3) is true and accurate.

(d) *Reporting – Ownership/Control Reports*.

(1) Information regarding ownership and control of banks and FSPs shall be reported by completing an Ownership/Control Report form (OCR) pursuant to the OCR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 1.

(2) The OCR shall be filed with the Banking Commissioner, as indicated in the instructions to the OCR. The identification details of any institution affiliated party who has been convicted of any offense involving dishonesty, breach of trust or money laundering must be included with the OCR, including details of the offence, conviction and penalty.

(3) The OCR shall be filed annually, no later than by February 1. In addition, a revised OCR shall be filed within thirty (30) days of any change in ownership or control of a bank or FSP, or upon the charging or conviction of any institution affiliated party who has been convicted of any offense involving dishonesty, breach of trust or money laundering.

(e) *Retention of Reports*. Each bank or FSP shall retain a copy of all reports together with any supporting documentation required by this Section 1 for a period of six (6) years from the date the report is filed with the Banking Commissioner.

Section 2. Internal Policies, Procedures, Controls and Training.

Section 2A: Internal Policies, Procedures, Controls, and Training

2A.1 Banks and FSPs must adopt and implement internal policies, procedures, and controls against ML/TF ('the AML/CTF Program'). The AML/CTF Program must be informed by

the ML/TF Risk Assessment and have regard to matters such as the size of the business, the products and services it offers and the jurisdictions in which it operates or provides services.

The AML/CTF Program must result in compliance with these Regulations, the Banking Act and any guidance issued by the Banking Commission. The Program must ensure that the risks identified by the Risk Assessment conducted pursuant to Section 2C are mitigated effectively. The AML/CTF Program must be approved by senior management, be regularly monitored, updated regularly, and enhanced to mitigate risks as and when they are identified.

2A.2 Banks and FSPs must designate a Compliance Officer at the management level. The compliance officer and other appropriate staff should have timely access to customer identification data and customer due diligence (CDD) information, transaction records, and any other relevant information. The Compliance Officer should have the authority to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors or equivalent body.

2A.3 The Compliance Officer must acquaint themselves with relevant information on the detection and prevention of money laundering, terrorist financing and proliferation financing. At a minimum this includes knowledge of the Banking Act (1987); The AML/CTF Regulations; the National Risk Assessment, thematic and sectoral risk assessments, and any guidance or information on AML/CTF/CPF provided by the Banking Commission. The Compliance Officer must know and understand the powers of the Banking Commission and the penalties for non-compliance with the Banking Act and AML Regulations.

2A.4 Banks and FSPs must maintain an adequately resourced and independent audit function to test compliance (including sample testing) with Part XIII of the Act and these Regulations.

2A.5 Banks and FSPs must establish ongoing employee training to ensure that employees are trained on current money laundering, terrorist financing and proliferation financing, techniques, methods, trends and indicators, Training must include a clear explanation of all aspects of money laundering/ terrorist financing/proliferation financing laws and obligations in the Marshall Islands, and in particular, the money laundering offence and penalties as they pertains to bank staff; CDD, and Suspicious Activity Reporting and the penalties that may apply to individual staff and officers for offences under the Banking Act.

2A.6 Banks and FSPs must establish adequate screening procedures to ensure high standards when hiring employees. This must include identification of past convictions for offences involving dishonesty, financially-motivated crime or money laundering.

2A.7 Banks and FSPs must have a centralized system for maintaining records of the information on the identity of customers, principal beneficiaries, authorized agents, Beneficial Owners, suspicious transactions and transactions exceeding $10,000 or its equivalent in a foreign currency.

2A.8 An MVTS provider that uses agents to provide MVTS on its behalf must include them in its AML/CFT Program and monitor them for compliance with these programs.

Section 2B: Supervision and Monitoring

2B.1 *Supervision of Banks and FSPs*. The Banking Commissioner is responsible for supervising banks and FSPs for compliance with Part XIII of the Act and these Regulations. The Banking Commissioner shall have all necessary powers to carry out the functions under this Section 2B.1, including (a) the power to examine records and inquire into the business and affairs of any bank or FSP, and (b) the power to compel production of any information relevant to monitoring compliance with Part XIII of the Act and these Regulations.

2B.2 *Examination of Banks and FSPs*. The Banking Commissioner may assess and evaluate banks and FSPs, and their staff, for compliance with Part XIII of the Act and these Regulations.

The process of inspection may include a wide range of activities such as: examining and assessing documents; quizzing and testing of staff on their knowledge, ability and willingness to fulfill obligations under the Act; sampling (either targeted or randomly) customer files, accounts and other filings; obtaining statements and acknowledgements from staff and customers; conducting 'process testing' (such as conducting anonymous transactions to test reporting processes).

Documents, information and evidence collected during the process of examination may be used in the process of enforcing the Act.

The frequency and intensity of examinations will be 'risk-based'- meaning that they are determined on the basis of the ML/TF/PF risk presented to the Marshall Islands and other jurisdictions by each entity.

In determining the risk presented by each entity the Banking Commissioner will take into account:

(a) Intelligence, data, information and evidence on financially-motivated offending, money laundering, terrorist or proliferation financing committed by the entity, its customers, clients, staff, officers, and/or owners;
(b) indications of activities being conducted within, or by, the entity that may be intended to prevent or interfere with the enforcement of the Banking Act or the AML Regulations by the Banking Commission;
(c) the level of cooperation afforded by each entity with respect to requests for information and guidance and recommendations made by the Banking Commission;
(d) the level of pro-active risk-mitigation undertaken by the entity;
(e) the quality of the AML/CTF Program and evidence of the adoption, adherence and compliance with the AML/CTF Program;.

2B.3 *Annual Submission of Independent Audit*. Banks and FSPs shall ensure an annual independent audit is performed to verify the adequacy of, and compliance with, the

AML/CTF Program. This audit shall be carried out in accordance with any guidance provided by the Banking Commission. Banks and FSPs shall submit to the Banking Commissioner the report resulting from the annual independent audit.

Section 2C: Risk Assessment

2C.1 Every bank and FSP must undertake and maintain a Risk Assessment to identify, assess and understand the money laundering, terrorist financing and proliferation financing risks that they face.

2C.2 In performing the Risk Assessments, a bank or FSP must incorporate information from the Marshall Islands National Risk Assessment as well as any Sectoral or Thematic Risk Assessments provided by Marshall Islands authorities and any information or guidance provided by the Banking Commission. The Risk Assessment must consider all relevant risks, including those associated with:

a. the customers and countries or geographic areas it serves, the products and services it provides, the transactions it undertakes, the industries in which its customers operate, the use those customers make of the products and services, and the delivery channels it uses;

b. its reliance on third parties under Section 3F of these Regulations; and

c. new products, practices, and technologies.

2C.3 The nature and extent of the Risk Assessment performed a bank or FSP must be appropriate to the nature, size, and complexity of its business. An entity's Risk Assessment must consider the risk presented to other jurisdictions by the products and services it offers and must include the collection and examination of open-source intelligence on money laundering, terrorist financing and proliferation financing using the types of products and services offered by the entity.

2C.4 Risk assessments performed under this Section 2C must be documented in writing in a manner that demonstrates their basis, kept up to date, and provided to the Banking Commissioner upon request.

2C.5 A Risk Assessment must be performed and documented as soon as reasonably practicable, but in no case more than three (3) months after commencing business as a bank or FSP. Banks and FSPs existing on the effective date of this Section 2C must perform and document a risk assessment within 12 months of Section 2C entering into effect.

Section 3. Risk-Based Customer Due Diligence (CDD).

Section 3A: Definition of Risk-Based Customer Due Diligence

3A.1 CDD includes:

a. identification of customers, including Beneficial Owners of the formal customer;

b. gathering of information on customers to create a customer profile;

c. application of acceptance policies to new customers;

d. maintenance of customer information on an ongoing basis;

e. monitoring of customer transactions; and

f. rules on transfers (including wire transfers) and correspondent banking.

3A.2 CDD must be applied on a risk basis, which must include enhanced CDD for higher-risk customers and politically exposed persons and may include simplified CDD for lower-risk customers.

3A.3 CDD must be applied to existing customers on the basis of materiality and risk, and CDD must be conducted on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

3A.4 Where a bank or FSP is unable to apply CDD measures as required by these Regulations in relation to a customer, or where CDD identifies that the customer presents a level of risk that can not be effectively mitigated (such as unexplained sources of wealth or funds) , the bank or FSP:

a. must not open any account, commence business relations, or perform any transaction for or on behalf of the customer;

b. must terminate any existing business relationship with the customer; and

c. must consider making a report under Section 5 of these Regulations.

3A.5 Where a bank or FSP forms a suspicion of money laundering, terrorist financing or proliferation financing, and reasonably believes that the CDD process will tip-off the customer, it may choose not to apply CDD and instead file a report under Section 5. In these circumstances, the entity must however, not open any account, commence business relations, or perform any transaction or service for or on behalf of the customer.

In making the decision to not conduct CDD the entity may need to balance the value to law enforcement of the information gathered versus the potential harm of tipping off the customer. The entity may seek assistance from the Banking Commission on this decision.

Section 3B: Identification of Customers

3B.1 Banks and FSPs must not keep anonymous accounts or accounts in obviously fictitious names.

3B.2 Banks and FSPs must identify their customers and verify their customers' identities. Customers include persons who are (or who seek to be):

a. in a business relationship ("business relationship");

b. engaged in one or more occasional transactions when the total value of the transactions exceeds $10,000 (“threshold occasional transaction”);

c. carrying out transfers of funds and value as provided in Section 3M ; and

d. engaged in any business or transaction in any instance where there is a suspicion that the person is involved in money laundering, terrorist financing or proliferation (“suspicious activity”) with the banks or FSP.

3B.3 In order to ensure proper customer identification, the bank or FSP must identify and verify the identity of the customer at any time that:

a. the person applies for a business relationship;

b. the person seeks to engage in a threshold occasional transaction including deposits into a third party account, or transactions on behalf of, a third party;

c. the person seeks to carry out a transfer of funds or value;

d. the person engages in a suspicious activity; or

e. where doubts have arisen as to the veracity or adequacy of previously obtained identification data on the person.

3B.4 For customers who are natural persons, the bank or FSP must verify the customer’s identity required using reliable, independent source documents, data, or information as provided for in Schedule 1 of these Regulations.

3B.5 For customers who are legal persons or legal arrangements, the bank or FSP must obtain and verify:

a. the customer’s name and legal form, including by obtaining proof of incorporation or similar evidence of establishment or existence (such as a trust instrument);

b. the identification of members of the customer’s controlling body (such as directors or trustees) as per the identification process for natural persons;

c. legal provisions that set out the power to bind the customer;

d. legal provisions that authorize persons to act on behalf of the customer;

e. the identity of the natural person purporting to act on behalf of the customer, using source documents as provided in Section 3B.4;

f. the address of the registered office and, if different, a principal place of business; and

g. such other reliable, independent source documents, data, or information as provided for in Schedule 1 of these Regulations.

3B.6 Banks and FSPs must verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person using reliable, independent source documents, data, or information as provided for in Schedule 1 of these Regulations.

3B.7 Banks and FSPs must understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

3B.8 Legible file copies must be made and retained of the relevant identification data, account files, and business correspondence, and results of any analysis undertaken, for at least six (6) years following the termination of an account or business relationship (or longer if requested by the Banking Commissioner).

3B.9 Banks and FSPs must ensure that all customer and transaction records are available on a timely basis (and in no event later than five (5) working days) to the Banking Commissioner or other domestic competent authority upon appropriate authority.

Section 3C: Determination of Beneficial Owner of the Customer

3C.1 Banks and FSPs must identify and take reasonable measures to verify the identity of the Beneficial Owner by using relevant information or data obtained from a reliable source such that the bank or FSP is satisfied that it knows the identity of the Beneficial Owner.

3C.2 For life and other investment-linked insurance, in addition to the CDD measures required for the customer and the Beneficial Owner, the beneficiary under the policy must be identified and verified. As soon as the beneficiary is identified or designated, the bank or FSP must:

a. take the name of any beneficiary identified as a specifically named natural or legal person or arrangement; and

b. obtain sufficient information concerning any beneficiary designated by characteristics, class, or other means to satisfy itself that it will be able to establish the beneficiary's identity at the time of the payout.

In both cases, verification of the beneficiary's identity must occur at the time of the payout. Verification must be performed using reliable, independent source documents, data, or information as provided for in Schedule 1 of these Regulations. Where a bank or FSP is unable to comply with this Section 3C.2, it should consider making a report under Section 5.

3C.3 For public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission, and certain non-resident public companies subject to adequate regulatory disclosure requirements and quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision in a jurisdiction that is implementing effectively the FATF Recommendations, no further identification is necessary. In determining if there has been effective implementation in the jurisdiction, banks and FSPs should take into account the information available on whether these countries adequately apply the FATF Recommendations, including by examining the

reports and reviews prepared by the Financial Action Task Force, International Monetary Fund, and World Bank publications.

3C.4 For other customers that are legal persons or legal arrangements, the bank or FSP must understand the nature of the customer's business and the ownership and control structure of the customer, including the ultimate natural person(s) who owns or controls a legal person, including natural persons with a controlling interest as described in this Section.

3C.5 With respect to legal persons, identification must be made of:

a. each natural person (if any) who owns directly or indirectly 25 percent or more of the vote or value of an equity interest in the legal person; and

b. to the extent there is doubt as to whether the person(s) identified under a. is(are) the Beneficial Owner(s) or where no natural person exerts control through ownership interests, the natural person(s) (if any) exercising control through other means; and

c. where no natural person is identified under a. or b. above, the relevant natural person who holds the position of senior managing official.

3C.6 With respect to a trust, identification must be made of the settlor(s), trustee(s), protector (if any), all of the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust. With respect to other types of legal arrangements, identification must be made of persons in equivalent or similar positions.

3C.7 For purposes of determining the Beneficial Owner of a customer, indirect control may extend beyond formal (direct) ownership or could be through a chain of corporate vehicles and through formal or informal nominee arrangements.

3C.8 Legible file copies must be made and retained of the relevant identification data, account files and business correspondence, and results of any analysis undertaken, for at least six (6) years following the termination of an account or business relationship (or longer if requested by the Banking Commissioner).

3C.9 Banks and FSPs must ensure that all customer and transaction records are available on a timely basis (and in no event later than five (5) working days) to the Banking Commissioner or other domestic competent authority upon appropriate authority.

Section 3D: Delayed Verification

3D.1 Banks and FSPs must verify the identity of the customer and Beneficial Owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Banks and FSPs may apply to the Banking Commission for authorization to delay completion of the customer verification process in Section 3B.3 a. and 3B.3 b. and Section 3C until after the establishment of the business relationship. Permission may be granted by the Banking Commission only if the bank or FSP presents a procedure that complies with Section 3D.2 and 3D.3 and then permission is at the discretion of the Banking Commissioner.

3D.2 Banks and FSPs may delay verification only if: verification occurs as soon afterwards as reasonably practical, the delay is essential to not interrupt the normal course of business, and the money laundering and terrorist financing risks are effectively managed.

Examples of situations where it may be essential not to interrupt the course of the normal conduct of business can be found in Appendix 1 Part A of these Regulations.

3D.3 Banks and FSPs seeking to delay verification must adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification. Procedures to manage risk concerning delayed customer identification should include a set of measures such as a limitation of the number, types and/or amount of transactions that can be performed, and enhanced monitoring of large and complex transactions being carried out outside of the expected pattern for that relationship.

Entities that seek to delay verification must accept that doing so may expose the entity and its staff to a heightened (and potentially unacceptable) risk of prosecution, or civil penalties, for a range of offences if it is later determined that the risks had not been effectively managed.

Whether the risks have been 'effectively managed' may be determined by objective factual circumstances.

Section 3E: Establishment of Customer Profile

3E.1 Every bank and FSP must create a profile for each customer of sufficient detail to enable it to implement the CDD requirements of these Regulations. The customer profile should be based upon sufficient knowledge of the customer, including the customer's business with the bank or FSP and the source of the customer's funds, wealth and/or assets.

Section 3F: Reliance on Third Parties

3F.1 Banks and FSPs may apply to the Banking Commission for authorization to rely on third parties such as trust and company service providers to perform the duties in Section 3B and 3C of these Regulations. Permission may be granted by the Banking Commission only if the bank or FSP presents a plan of internal policies and practices that comply with this Section.

3F.2 Banks and FSPs may rely upon third parties that are also banks and FSPs (other entities that are subject to supervision by the Banking Commission under these Regulations).

3F.3 Banks and FSPs may rely upon non-resident third parties if the bank or FSP is satisfied that the third party is adequately regulated and supervised and has measures in place to comply with the CDD and recordkeeping requirements in these Regulations.

Banks and FSPs must be satisfied that a non-resident third party is subject to money laundering and terrorist financing policies comparable with the FATF Recommendations. They must be satisfied that the non-resident third party is subject to licensing and supervision to enforce those policies and has not been subject to any material disciplinary action that calls into question its execution of those policies. Banks and FSPs must ensure

that non-resident third parties are located in a jurisdiction that is implementing effectively the FATF Recommendations. In making this determination, banks and FSPs should take into account the information available on application and adequacy of implementation of the FATF Recommendations to entities in individual countries. Banks and FSPs may not rely on a non-resident third party established in a country identified by the Banking Commissioner as a higher risk country.

3F.4 In each instance of reliance on third parties, the bank or FSP must immediately obtain from the third party the information required in Section 3B and 3C. While it is not necessary to obtain copies of the CDD documentation from the third party, banks and FSPs must take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to CDD requirements will be made available without delay, if requested.

3F.5 Banks and FSPs may not rely upon third parties identified by the Banking Commission as non-complying with the FATF Recommendations, or third parties for whom the bank or FSP has independent credible reason to believe are not complying with the FATF Recommendations.

3F.6 The ultimate responsibility for implementation of the CDD requirements of these Regulations remains with the bank or FSP, and the bank or FSP remains liable for any failure to apply such measures.

3F.7 The requirements of this Section do not apply to outsourcing or agency relationships, i.e. where the agent is acting under a contractual arrangement with the bank or FSP to carry out its CDD functions.

3F.8 The requirements of this Section do not apply to business relationships, accounts, or transactions between banks and FSPs for their clients.

Section 3G: Acceptance of New Customers

3G.1 As set forth in Section 3A.4 of these Regulations, banks and FSPs must not accept as customers those persons whose identity and Beneficial Owner as required in Section 3B, 3C, and 3D cannot be verified or for whom sufficient information to form a customer profile cannot be gathered.

3G.2 It is important that the policy on acceptance of new customers is not so restrictive that it results in a denial of access by the general public to financial services, especially for people who are financially or socially disadvantaged.

Section 3H: The Maintenance of Customer Information on an Ongoing Basis

3H.1 Banks and FSPs must gather and maintain customer information on an ongoing basis. Documents, data, or information collected under the CDD process should be kept up to date and relevant by undertaking reviews of existing records at appropriate times, particularly for higher risk categories of customers or business relationships.

Section 3I: Ongoing Monitoring of Customer Transactions

3I.1 Banks and FSPs must monitor ongoing customer transactions. Monitoring must include the scrutiny of customer transactions to ensure that they are being conducted according to the bank's or FSP's knowledge of the customer and the customer's business and risk profile, the source of funds, and may include predetermined limits on amount of transactions and type of transactions.

3I.2 Banks and FSPs must pay special attention to all complex, unusual large transactions, or unusual pattern of transactions that have no visible economic or lawful purpose. Banks and FSPs must examine as far as possible the background and purpose of such transactions and set forth their findings in writing. Banks and FSPs must keep such findings available for examination by the Banking Commission, auditors, and any other competent authorities, for a minimum of six (6) years. In such cases, banks and FSPs should determine if they should file a suspicious activity report.

3I.3 Banks and FSPs must pay special attention to all business relationships and transactions with legal persons, natural persons, and financial institutions from countries that are not sufficiently applying the FATF standards and recommendations. Enhanced due diligence should be proportionate to the level of risk involved, and follow the procedures presented in Section 3K below.

Section 3J: Termination of Customer Relationship

3J.1 If the bank or FSP has already commenced a business relationship and is unable to comply with the CDD required for a customer, or where CDD identifies an unlawful, or unexplained, source for the customer's funds and wealth it must terminate the customer relationship and file a suspicious activity report under Section 5.

Section 3K: Enhanced CDD for Higher Risk Customers and Politically Exposed Persons

3K.1 Banks and FSPs must apply enhanced CDD for customers that pose a higher risk of money laundering, terrorist financing or proliferation financing ("enhanced CDD"). Enhanced CDD should include measures to establish the source of wealth and source of funds of customers and Beneficial Owners identified as higher-risk customers including Politically Exposed Persons ('PEPs').

Banks and FSPs must develop and maintain a list of PEPs and Higher-Risk Customers.

Enhanced CDD should be applied to customers and Beneficial Owners identified as higher risk customers and PEPs at each stage of the CDD process.

Examples of higher risk factors that banks and FSPs must consider are set forth in Appendix 1 Part B of these Regulations.

3K.2 No customer or Beneficial Owner identified as a higher-risk customer or PEP should be accepted as a customer unless a senior member of the bank's or FSP's management has approved.

3K.3 Where a customer or Beneficial Owner has been accepted and the customer or Beneficial Owner is subsequently found to be, or subsequently becomes a higher risk customer or a PEP, banks and FSPs must obtain senior management approval to continue the business relationship.

3K.4 Where banks and FSPs are in a business relationship with a higher-risk customer or a PEP, they must conduct enhanced ongoing monitoring of that relationship. This includes periodically obtaining independent, verified information on the source of funds, wealth and assets. If, at any time this can not be achieved the entity must terminate the relationship and submit a Suspicious Activity Report.

Ongoing monitoring of the relationship also includes periodic examination of the transactions of the PEPs and higher-risk customers and identifying a legitimate source and application for the transactions.

Ongoing monitoring of the relationship also includes examination of any Suspicious Activity Reports submitted on the customer. If, after further examination, analysis and inquiry the original suspicion cannot be allayed or refuted the entity must terminate the relationship.

3K.5 Banks and FSPs must put in place appropriate risk management systems to determine whether a potential customer or the Beneficial Owner is a higher-risk customer or a PEP. This must include periodically cross-checking the PEP and Higher-Risk Customer List with the full list of the entity's customers.

3K.6 Banks and FSPs must take reasonable measures to determine whether a customer or Beneficial Owner is a domestic politically exposed person or an international organization politically exposed person. In cases of a higher risk business relationship with such persons, the measures for higher risk customers in Sections 3K.1 to 3K.4 must be applied.

3K.7 For life insurance policies, if the bank or FSP determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, enhanced CDD must include reasonable measures to identify and verify the identity of the beneficiary's Beneficial Owner, at the time of payout. Where the bank or FSP is unable to comply with this Section 3K.7, it should consider making a report under Section 5.

3K.8 For life insurance policies, banks and FSPs shall take reasonable measures to determine whether a beneficiary or Beneficial Owner of a beneficiary are politically exposed persons. This should be done at the latest during the time of payout. Where higher risks are identified, banks and FSPs should inform senior management before the payout of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a report under Section 5.

Section 3L: Simplified CDD for Lower Risk Customers.

3L.1 Banks and FSPs may apply to the Banking Commissioner for authorization to apply simplified customer due diligence procedures to a particular business relationship or transaction. Permission may be granted by the Banking Commission only if (a) a lower

risk has been identified, (b) allowing simplified measures is consistent with Marshall Islands' national risk assessment, (c) the bank or FSP complies with Section 2 of these Regulations, and (d) the bank or FSP presents a simplified CDD procedure for the business relationship or transaction that complies with this Section 3L.

3L.2 In general, customers must be subject to the full range of CDD measures as provided in these Regulations, including the requirement to identify the Beneficial Owner. Where the risk of money laundering and terrorist financing is lower and where information on the identity of the customer and the Beneficial Owner of the customer is publicly available, or where adequate checks and controls exist in national systems, in such circumstances it would be reasonable for permission to be granted for banks and FSPs to apply simplified CDD measures when identifying and verifying the identity of the customer or Beneficial Owner.

3L.3 Simplified CDD measures when applied to customers that are residents in another country is limited to countries that are in compliance with and have effectively implemented the FATF Recommendations and are not included among lists of tax or money laundering havens.

3L.4 Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering, terrorist financing, proliferation financing or specific higher risk scenarios.

Examples of lower risk factors are set forth in Appendix 1 Part C of these Regulations.

Section 3M: Policies and Procedures on Wire Transfers

Ordering Banks and Financial Services Providers

3M.1 Ordering banks and FSPs must ensure that all cross-border transfers (including wire transfers, batch transfers, alternative remittance transfers, and transactions using a credit or debit card to effect a funds transfer) always include full originator information and must verify that the originator information is accurate. Full originator information includes:

a. the name of the originator;

b. the originator's account number (or a unique reference number that permits the transaction to be traced if there is no account); and

c. the originator's address, national identity number, customer identification number, or date and place of birth.

3M.2 Ordering banks and FSPs must ensure that all cross-border transfers (including wire transfers, batch transfers, alternative remittance transfers, and transactions using a credit or debit card to effect a funds transfer) always include full beneficiary information. Full beneficiary information includes:

a. name of the beneficiary; and

b. the beneficiary account number (or a unique reference number that permits the transaction to be traced if there is no account).

3M.3 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they are exempt from the originator information requirements of Section 3M.1 provided that:

a. they include the originator's account number (or unique reference number); and

b. the batch file contains full and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

The bank or FSP should ensure that non-routine transactions are not batched where this would increase the risk of money laundering or terrorist financing.

3M.4 For domestic transfers (including wire transfers, batch transfers, alternative remittance transfers, and transactions using a credit or debit card to effect a funds transfer), the ordering bank or FSP must include either:

a. full originator information as specified in Section 3M.1 in the message or payment form accompanying the wire transfer, or

b. only the originator's account number or, where no account number exists, a unique identifier, within the message or payment form.

3M.5 Section 3M.4 b. may be used only if the number or identifier will permit the transaction to be traced back to the originator or the beneficiary and full originator information as specified in Section 3M.1 can be made available by the ordering bank or FSP to the beneficiary bank or FSP and the Banking Commission within three (3) working days of receiving a request. If requested by a law enforcement authority, this information must be produced immediately.

3M.6 Ordering banks and FSPs may apply to the Banking Commission for authorization to exempt wire transfers below $1,000 from the requirements of Section 3M.1 and 3M.2. Permission may be granted by the Banking Commission only if the bank or FSP presents a procedure that complies with this Section 3M.6. If permission is granted, then for all wire transfers below $1,000 the bank or FSP must:

a. ensure that all such transfers include the name of the originator, the name of the beneficiary, and an account number (or, in the absence of an account, a unique reference number that permits the transaction to be traced) for each; and

b. verify the information pertaining to its customer if there is a suspicion of money laundering or terrorist financing.

3M.7 The ordering bank or FSP shall maintain all originator and beneficiary information collected in accordance with Section 4 of these Regulations.

3M.8 The ordering bank or FSP shall not execute the wire transfer if it does not comply with the requirements of Section 3M.1 to 3M.7 above.

Beneficiary Banks and Financial Services Providers

3M.9 Beneficiary banks and FSPs shall take reasonable measures, which may include post event monitoring or real-time monitoring where feasible, to identify cross-border transfers that lack required originator information or required beneficiary information. For cross-border wire transfers of $1,000 or more, a beneficiary bank or FSP shall verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Section 4.

3M.10 Beneficiary banks and FSPs shall have risk-based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow up action. Procedures to address these cases should include first requesting the missing originator information from the ordering bank or FSP. If the missing information is not forthcoming, the beneficiary bank or FSP must reject the transaction and send a suspicious activity report to the Banking Commission under Section 5. In appropriate circumstances, beneficiary banks and FSPs should consider restricting or terminating business relationships with banks and FSPs that do not comply with this Section.

Intermediary Banks and Financial Services Providers

3M.11 For cross-border transfers, the bank or FSP processing an intermediary element of any chain of transfers shall ensure that all originator and beneficiary information that accompanies a transfer is retained with it.

3M.12 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the intermediary bank or FSP shall keep a record for at least six (6) years of all the information received from the ordering bank or FSP or another intermediary bank or FSP.

3M.13 Intermediary banks and FSPs shall take reasonable measures, which are consistent with straight-through processing, to identify cross-border transfers that lack originator or beneficiary information required under Section 3M.1 and 3M.2.

3M.14 Intermediary banks and FSPs must have risk-based policies and procedures for determining (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow up action.

Money or Value Transfer Service (MVTS) Providers

3M.15 MVTS providers must comply with all relevant requirements of this Section 3M in the countries in which they operate, directly or through their agents.

3M.16 For a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider shall (a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious activity report has to be filed, and (b) file a suspicious activity report in any country affected by the

suspicious wire transfer, and make relevant transaction information available to the Banking Commission, auditors, and any other competent authorities.

Implementation of Targeted Financial Sanctions

3M.17 With respect to processing wire transfers, banks and FSPs shall take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in applicable Marshall Islands laws and regulations.

Section 3N: Policies and Procedures on Cross Border Correspondent Banking and Similar Relationships

3N.1 Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of banking services, including cash management (for example, interest-bearing accounts in a variety of currencies), international wire transfers, check clearing, payable-through accounts, and foreign exchange services. This Section 3N also applies to other similar relationships, including MVTS acting as intermediaries for the transfer of funds or value.

3N.2 Banks and FSPs must develop and implement policies and procedures concerning correspondent banking and other similar relationships. In order to provide correspondent services, a bank or FSP must first assess the respondent's controls against money laundering and terrorist financing and determine that they are adequate and effective. To do so, banks and FSPs must gather sufficient information about respondents to understand their business and determine from publicly available information the reputation of the institution, quality of supervision, and whether they have been subject to a money laundering or terrorism financing investigation or regulatory action. New correspondent banking or other similar relationships must be approved by a bank's or FSP's senior management. A bank or FSP should, in general, establish or continue a correspondent banking or other similar relationship with a foreign respondent only if it is satisfied that the respondent is effectively supervised by the relevant authority. In particular, a bank or FSP should not establish or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e. a shell bank).

3N.3 The information to be collected may include, but is not limited to, details about the respondent's management, major business activities, where it is located, its money laundering and terrorist financing prevention efforts, the system of regulation and supervision in the respondent's country and the purpose of the account.

3N.4 A bank or FSP should pay particular attention when maintaining a correspondent banking or other similar relationship with respondents incorporated in jurisdictions that do not meet international standards for the prevention of money laundering and terrorist financing. Enhanced due diligence will generally be required in such cases, including obtaining details of the Beneficial Ownership of such respondents and more extensive information about their policies and procedures to prevent money laundering and terrorist financing.

3N.5 A bank or FSP must develop and implement policies and procedures concerning the ongoing monitoring of activities conducted through such correspondent accounts and must clearly understand the respective AML/CFT responsibilities of each institution in the correspondent banking or other similar relationship.

3N.6 Particular care should also be exercised where the respondent allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e. payable-through accounts). A bank or FSP must be satisfied that the respondent has performed the customer due diligence required in these Regulations for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent.

Non-face-to-face transactions and new technologies

3N.7 Banks and FSPs are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Banks and FSPs must (a) undertake the risk assessment prior to the launch or use of such products, practices, and technologies; and (b) have policies in place and take such measures as are needed to manage and mitigate the risks.

3N.8 Banks and FSPs are required to have policies and procedures in place to address specific risks associated with non-face-to face business relationships or transactions. These policies should apply when establishing customer relationships and when conducting ongoing due diligence. This should include specific and effective CDD procedures that apply to non-face-to-face customers.

Shell Banks

3N.9 It is not permissible to establish or accept the operation of a shell bank in the Marshall Islands.

3N.10 Banks and FSPs must not enter into correspondent banking relationships with shell banks.

3N.11 Banks and FSPs must satisfy themselves that respondent banks and FSPs in a foreign country do not permit their accounts to be used by shell banks.

Section 4. Transactions, Recordkeeping.

(a) Every bank and FSP shall retain records regarding all transactions to the extent and in the manner required by this Section 4.

(b) *Recordkeeping*. All banks and FSPs shall retain records necessary to reconstruct all transactions and sufficient to identify:

(1) the name, address and occupation/business or principal activity of each person conducting or involved in a transaction or on whose behalf a transaction is conducted;

(2) the identity of all banks and FSPs involved;

(3) the nature and date of the transaction, together with all advices, requests, or instructions given or received;

(4) the type and identification numbers of all accounts involved;

(5) the type and amount of currency involved, if any;

(6) if a negotiable instrument other than currency is involved:

(i) the name of the drawer;

(ii) the name of institution on which it is drawn;

(iii) the name of the payee, if any;

(iv) amount and date of the instrument;

(v) the number of the instrument, if any; and

(vi) details regarding all endorsements appearing on the instrument; and

(7) the name(s) and address(es) of the bank or FSP and of the officer(s), employee(s), and agent(s) of the bank or FSP who prepared the records, and the method(s) used to verify the information required by this subsection (b).

(c) Each bank or FSP shall, in addition to the records in subsection (b), retain the following:

(1) each check, clean draft, or money order drawn on the bank or issued and payable by it, except those drawn for $100 or less or those drawn on accounts which can be expected to have drawn on them an average of at least 100 checks per month over the calendar year or on each occasion on which such checks are issued, and which are:

(i) dividend checks,

(ii) payroll checks,

(iii) employee benefit checks,

(iv) insurance claim checks,

(v) medical benefit checks,

(vi) checks drawn on government agency accounts,

(vii) checks drawn by brokers or dealers in securities,

(viii) checks drawn on fiduciary accounts,

(ix) checks drawn on other financial institutions, or

(x) pension or annuity checks; and

(2) each item in excess of $100 (other than bank charges or periodic charges made pursuant to agreement with the customer) comprising a debit to a customer's deposit or share account, including those not required to be kept, and not specifically exempted, under paragraph (c)(1)of this section.

(d) *Retention of records*.

(1) A bank or FSP shall maintain either the original or a microfilm, electronic or other copy or reproduction of all records, documents, advice requests and instructions regarding any transaction subject to Section 4 recordkeeping requirements for a period of six (6) years from the date of the completion of the transaction;

(2) all records shall be filed or stored in a readily recoverable manner as to be accessible within a reasonable time; and

(3) all records shall be available on a timely basis (and in no event later than five (5) working days) to the Banking Commissioner or other domestic competent authority upon appropriate authority.

(e) *Exemption*. Nothing in these Regulations shall be construed as requiring the production of any evidence of identity where there is a transaction or a series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.

Section 5. Reports of Suspicious Transactions.

(a) *General*.

(1) Every bank and FSP shall file with the Banking Commissioner, to the extent and in the manner required by this Section 5, a Suspicious Activity Report (SAR) of any suspicious transaction. A bank or FSP may also file a SAR regarding any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by this section.

(2) For the purposes of reporting under this Section 5, a suspicious transaction is a transaction conducted or attempted by, at, or through the bank or FSP that the bank or FSP knows, suspects, or has reason to suspect that:

(a) involves funds or other assets that are the proceeds of crime or are otherwise derived from illegal activity, including, but not limited to, tax matters; or

(b) was intended, conducted, or attempted to be conducted:

(i) in order to hide or disguise funds or assets that are the proceeds of crime or are otherwise derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets); or

(ii) as part of a plan to violate or evade any Marshall Islands law or regulation or to avoid any transaction reporting requirement under Marshall Islands law or regulation; or

(c) involves a transaction or transactions which:

(i) is/are complex or unusual; or

(ii) present an unusual pattern; or

(iii) has/have no apparent economic or lawful purpose; or

(iii) is/are not the sort of transaction in which any person or entity involved would normally be expected to engage; or

(d) could constitute or be related to terrorist financing, terrorist acts, a terrorist organization, an individual terrorist or to terrorist property or proliferation financing.

(b) *Filing procedures*.

(1) A suspicious transaction shall be reported by completing a SAR form pursuant to the SAR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 5.

(2) The SAR shall be filed with the Banking Commissioner, as indicated in the instructions to the SAR.

(3) The SAR shall be filed no later than three (3) working days after the date of initial detection by the bank or FSP of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, a bank or FSP may file a SAR and submit an additional SAR (referencing the first) when such information becomes available.

(4) In situations involving violations that require immediate attention, such as, for example, ongoing money laundering, terrorist financing or proliferation schemes, the bank or FSP shall immediately notify the Banking Commissioner, or his designee, in addition to a later filing of the SAR within the 3 working day timeframe.

(c) *Retention of records*. A bank or FSP shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of fifteen (15) years from the date of filing the SAR. Supporting documentation shall be identified, and maintained by the bank or FSP as such, and shall be deemed to have been filed with the SAR. A bank or FSP shall make all supporting documentation available to the Banking Commission and any appropriate law enforcement agencies upon request.

(d) *Confidentiality of reports*. Banks and FSPs, its employees, officers, directors, and agents shall not notify any person or entity other than those authorized by law that a suspicion has

been formed or that a SAR or related information is being or has been filed in accordance with this Section 5.

(e) *Confidentiality of individuals*. The identity of any bank or FSP, its employees, officers, directors, or agents who submit a SAR to the Banking Commissioner, Attorney General, court of competent jurisdiction, or other lawfully recognized person, shall remain confidential.

Section 6. Currency Transaction Reporting.

(a) Every bank and FSP shall obtain the requisite information and file with the Banking Commissioner reports of transactions in currency to the extent and in the manner herein required.

(b) For the purposes of obtaining, information and reporting under this Section 6, a transaction in currency is:

(1) a deposit, withdrawal, exchange of currency, or other payment or transfer;

(2) involving currency of any country of a value greater than US$10,000:

(i) in a single transaction; or

(ii) in multiple transactions taken by or on behalf of a single person within a 24-hour period when aggregated.

(c) Prior to concluding any transaction in currency all banks and FSPs shall obtain and verify the following information:

(1) the name, address, citizenship/residency status, social security number or passport number and occupation/business or principal activity of each person conducting or involved in a transaction or on whose behalf a transaction is conducted;

(2) the nature and date of the transaction;

(3) the type and identification numbers of all accounts involved;

(4) the type and amount of currency involved, and

(5) name(s) of officers, employees and agent(s) and method(s) used to verify the information required by this subsection (c).

(d) *Verification – records to be examined*. Banks and FSPs satisfy their requirement to verify information required by Section 6(c) records by obtaining from and examining:

(1) from individuals – original official unexpired documents bearing a photograph or reasonable alternative;

(2) from legal persons and legal arrangements – articles of incorporation, charters, trust deed or their equivalents, or any other official documentation establishing that it

has been lawfully registered and is in existence at the time of identification and which delineates the powers of their legal representatives; and

(3) the appropriate documentation for all persons acting, or appearing to act, in a representative capacity including all the beneficiary(ies).

(e) *Reporting – transactions in currency. Filing procedures*.

(1) Information regarding transactions in currency not otherwise exempted pursuant to subsection (g) and (h) of this Section 6 shall be reported by completing a Currency Transaction Report form (CTR) pursuant to the CTR's instructions, and collecting and maintaining supporting documentation as required by paragraph (c) of this Section 6.

(2) The CTR shall be filed with the Banking Commissioner, as indicated in the instructions to the CTR.

(3) The CTR shall be filed no later than ten (10) working days after the date of transaction in currency.

(f) *Retention of records*. A bank or FSP shall maintain a copy of any CTR filed and the original or a microfilm, electronic or other copy or reproduction, or business record equivalent of any supporting documentation of a CTR for a period of six (6) years from the date of filing the CTR. Supporting documentation shall be identified, and maintained by the bank or FSP as such, and shall be deemed to have been filed with the CTR. A bank or FSP shall make all supporting documentation available to the Banking Commissioner and any appropriate law enforcement agencies upon request.

(g) *Transactions eligible for exemption from filing report*.

(1) A transaction to which a bank or FSP is party is also eligible for exemption if:

(i) the other party to the transaction is a government agency of the Marshall Islands; and

(ii) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of that agency.

(2) A transaction is eligible for exemption if the transaction is between a bank and FSP and another bank and FSP; or

(3) A transaction is also eligible for exemption if:

(i) the transaction is between a bank and FSP and another person (in this subsection called the "customer");

(ii) the customer has had, at the time when the transaction takes place, an account verified pursuant to Section 3 with the bank and FSP for one year;

(iii) the transaction consists of a deposit into, or a withdrawal from, an account maintained by the customer with the bank and FSP;

(iv) the transaction does not involve any party representing anyone in a representative capacity;

(v) the customer carries on a commercial enterprise (other than business that includes the selling of vehicles, vessels, aircraft, real estate brokerage, mobile home dealers, accountants, lawyers, doctors, pawnbrokers, title insurance/closing companies, trade unions, and auctioneers);

(vi) the account is maintained for the purposes of that business; and

(vii) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of the customer.

(4) A transaction is also eligible for exemption if:

(i) the transaction is between a bank and FSP and another person (in this subsection called the "customer");

(ii) the customer has had, at the time when the transaction takes place, an account verified pursuant to Section 3 with the bank and FSP for one year;

(iii) the transaction consists of a withdrawal from an account maintained by the customer with the bank and FSP;

(iv) the withdrawal is made for payroll purposes;

(v) the customer regularly withdraws, from the account, currency of a value not less than $10,000 to pay the customer's staff and employees; and

(vi) the amount of currency involved in the transaction does not exceed an amount that is reasonably commensurate with the lawful business activities of the customer.

(h) *Exemption registry*. A record of each exemption granted under this section and the reason therefore must be kept by a bank and FSP in an exemption registry.

(1) For a transaction exempted under subsection (g)(1) or (2) of this Section 6, the exemption registry should include the reason for the exemption and the names and addresses of the banks, FSPs, and/or government agencies involved in the transaction.

(2) For exempted transactions between a bank and FSP and a customer, as defined in subsection (g)(3) and (4) of this Section 6, the exemption registry must include the following information:

(i) the reason for exemption;

(ii) the customer's name, business or residential address, and his/her occupation, business or principal activity;

(iii) a statement whether the exemption covers deposits, withdrawals or both;

(iv) a signed statement by the customer that states the following:

(A) the party believes that the transaction is eligible for exemption under Section 6(g), and

(B) the information provided by the party to the institution in relation to the transaction is, to the best of his or knowledge and belief, true and correct;

(v) the name and title of the person making the decision to grant the exemption; and

(vi) any other information mandated by the Banking Commission.

(3) *Class transactions*. An exemption can apply to a class of transactions between a bank and FSP and eligible parties designated under Section 6(g). For class transactions, the exemption registry must also include in, addition to the requirements of Section 6(h)(1) and (2), the following:

(i) the range of the amounts of currency involved in the class of transactions;

(ii) the range amount of the class of transactions;

(iii) the period during which the class of transactions is to be exempt; and

(iv) any other information mandated by the Banking Commission.

(4) Banks and FSPs must monitor the exemptions they have granted on a continual basis. A change in circumstances may warrant removal from the registry or require amending the exemption record in the registry. In addition to monitoring, each bank or FSP must commission an annual review of its exemption registry. A bank or FSP must contact each customer who has an exemption to determine whether there is a change in the customer's situation since the last date of review.

(5) The Banking Commission has the right to review the exemption registry at any time. The Bank Commission may, by appropriate order, direct the deletion of any.

Section 7. Assessment of Civil Money Penalties.

(a) In addition to any criminal penalties authorized by the Act, each bank and FSP, and any partner, director, officer, employee, or person participating in the conduct of the affairs of a bank or FSP who violates any provision of Part XIII of Title 17 or any of its implementing regulations shall forfeit and pay a civil money penalty to the extent and in the manner hereafter specified by this Section.

(b) For any willful violation of any recordkeeping, reporting or verification requirement of Part XIII of Title 17 or any of its implementing regulations, the Banking Commissioner may recommend to the Office of Attorney General that it assess upon any bank or FSP, and upon any partner, director, officer, or employee thereof, or person participating in the conduct of the affairs of a bank or FSP who willfully participates in the violation, a civil money penalty not to exceed $10,000 per violation.

(c) For any negligent violation of any requirement of Part XIII of Title 17 or any of its implementing regulations, the Banking Commissioner may recommend to the Office of the Attorney General that it assess upon any bank or FSP, and upon any partner, director, officer, or employee thereof, or person participating in the conduct of the affairs of a bank or FSP who participates in the violation, a civil money penalty not to exceed $500 per violation.

(d) *Assessment.*

(1) The Banking Commissioner shall inform the Office of the Attorney General of a violation and provide a detailed recommendation on the amount of the civil money penalty that should be sought.

(2) Upon receipt of the recommendation, the Office of the Attorney General must determine whether there is sufficient evidence to have the assessment enforced by the High Court.

(3) If the Office of the Attorney General decides to enforce the assessment, written notice must be provided to the entity(ies) or person(s) from whom payment is sought. The notice must be sent out before the enforcement action is filed with the High Court.

(e) All civil money penalties collected under this Section shall be paid over to the Treasury of the Republic of the Marshall Islands.

(f) The resignation, termination of employment or termination of participation in the affairs of any partner, director, officer, employee, or person participating in the conduct of the affairs of a bank or FSP shall not affect the jurisdiction and authority of the Banking Commissioner to issue any Notice of assessment against such person or entity if such Notice is served within six (6) years of their resignation, termination of employment or termination of participation in the affairs of the bank or FSP.

Section 8. Exceptions and Exemptions.

(a) Subject to the provisions of the Act and these Regulations, the Banking Commissioner may, by written order or authorization, make exceptions to or grant exemptions from the requirements of Sections 1 – 7 and 9 – 11 of these Regulations if:

(1) there is a proven low risk of ML/TF, the exception or exemption occurs in strictly limited and justified circumstances, and it relates to a particular type of financial institution or activity, or DNFBP; or

(2) a financial activity (other than the transferring of money or value) is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria), such that there is a low risk of ML/TF.

(b) Exceptions or exemptions granted under this Section may be conditional or unconditional, may apply to particular persons or classes of persons, and may apply to particular transactions or classes of transactions. They shall, however, be applicable only as expressly stated in the order or authorization. Any exception or exemption shall be revocable in the sole discretion of the Banking Commissioner.

Section 9. Application to Branches and Subsidiaries.

(a) Banks and FSPs must ensure that their foreign branches and subsidiaries observe AML/CFT measures consistent with the requirements in the Marshall Islands and the FATF Recommendations.

(1) Banks and FSPs must pay particular attention to this principle with respect to branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations.

(2) Where the minimum AML/CFT requirements of the Marshall Islands and the host country differ, branches and subsidiaries in host countries must apply the higher standard to the extent that the host country laws and regulations permit.

(3) Banks and FSPs must inform the Banking Commissioner when a foreign branch or subsidiary is unable to observe appropriate AML/CFT measures because this is prohibited by host country laws, regulations or other measures.

(b) Financial groups must implement group-wide AML/CFT programs applicable and appropriate to all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in Section 2A and 2B.3 and also:

(1) policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

(2) the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done). Similarly, branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and

(3) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Section 10. Designated Non-Financial Businesses and Professions (DNFBPs).

Risk Assessment. Every DNFBP must undertake and maintain a Risk Assessment to identify, assess and understand the money laundering, terrorist financing and proliferation financing risks that they face.

(1) In performing the Risk Assessment, a DNFBP must incorporate information from the Marshall Islands National Risk Assessment as well as any Sectoral or Thematic Risk Assessments provided by Marshall Islands authorities and any information or guidance provided by the Banking Commission. The Risk Assessment must consider all relevant risks, including those associated with:

(i) the customers and countries or geographic areas it serves, the products and services it provides, the transactions it undertakes, the industries in which its customers operate, the use those customers make of the products and services, and the delivery channels it uses;

(ii) its reliance on third parties under Section 3F of these Regulations; and

(iii) new products, practices, and technologies.

(2) The nature and extent of risk assessments performed a DNFBP under this subsection must be appropriate to the nature, size, and complexity of its business. An entity's Risk Assessment must consider the risk presented to other jurisdictions by the products and services it offers and must include the collection and examination of open-source intelligence on money laundering, terrorist financing and proliferation financing using the types of products and services offered by the entity.

(3) Risk assessments performed under this subsection must be documented in writing in a manner that demonstrates their basis, kept up to date, and provided to the Banking Commissioner upon request.

(4) A risk assessment must be performed and documented under this subsection as soon as reasonably practicable, but in no case more than three (3) months after commencing business as a DNFBP. DNFBPs existing on the effective date of this subsection must perform and document a risk assessment within 12 months of this subsection entering into effect.

(a) *Risk-Based Customer Due Diligence (CDD).*

(1) DNFBPs must comply with the requirements set out in Sections 3A to 3L of these Regulations in the following situations:

(i) *Casinos* – when customers engage in financial transactions of $3,000 or more.

(ii) *Real estate agents* – when they are involved in transactions for a client concerning the buying and selling of real estate.

(iii) *Dealers in precious metals and dealers in precious stones* – when they engage in any cash transaction with a customer of $15,000 or more.

(iv) *Lawyers, notaries, other independent legal professionals and accountants* – when they prepare for or carry out transactions for their client concerning the following activities:

(A) buying and selling of real estate;

(B) managing of client money, securities, or other assets;

(C) management of bank, savings, or securities accounts;

(D) organization of contributions for the creation, operation, or management of companies;

(E) creation, operation, or management of legal persons or legal arrangements, and buying and selling of business entities.

(v) *Trust and company service providers* – when they prepare for or carry out transactions for a client concerning the following activities:

(A) acting as a formation agent of legal persons;

(B) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

(C) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal person or arrangement;

(D) acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

(E) acting as (or arranging for another person to act as) a nominee shareholder for another person.

(2) In the situations set out in paragraph (1) above, DNFBPs must comply with the recordkeeping requirements in Section 4 of these Regulations.

(3) In the situations set out in paragraph (1) above, DNFBPs must comply with the non-face-to-face transactions and new technologies requirements in Section 3N.7 and 3N.8 of these Regulations.

(b) *Reports of Suspicious Transactions*. The requirements to report suspicious transactions set out in Section 5 of these Regulations apply to all DNFBPs, subject to the following qualifications:

(1) *Dealers in precious metals or stones* – the requirements of Section 5 apply when they engage in a cash transaction with a customer of $15,000 or more.

(2) *Lawyers, notaries, other independent legal professionals and accountants* – the requirements of Section 5 apply when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in subparagraph (b)(1)(iv) of this Section unless the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

(3) *Trust and company service providers* – the requirements of Section 5 apply when, on behalf or for a client, they engage in a transaction in relation to the activities described in subparagraph (b)(1)(iv) of this Section.

(c) *Internal Controls*. In the situations set out in subsection (c) above, DNFBPs must comply with the internal policies, procedures, controls, and training requirements in Section 2A.1 to 2A.6 and with the monitoring requirements in Section 2B.3 of these Regulations.

(d) *Higher Risk Countries*. In the situations set out in subsection (c) above, DNFBPs must comply with the requirements in Section 3I.3 of these Regulations.

(e) *Supervision of DNFBPs*. The Banking Commissioner is responsible for supervising DNFBPs for compliance with Part XIII of the Act and these Regulations. The Banking Commissioner shall have all necessary powers to carry out the functions under this subsection.

(f) *Examination of DNFBPs*. The Banking Commissioner shall evaluate DNFBPs for compliance with Part XIII of the Act and these Regulations. Examinations shall be carried out pursuant to the Anti-Money Laundering Examination Procedures Manual: Standards and Associated Risks and on a risk-sensitive basis. The frequency and intensity of examinations should be determined on the basis of the Banking Commissioner's understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number. Examiners should take into account the ML/TF risk profile of DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies, and procedures of DNFBPs.

Section 11. Virtual Assets and Virtual Asset Service Providers.

(a) *General Requirements*. VASPs must comply with the requirements applicable to all FSPs under the Act and these Regulations, subject to the qualifications set forth in subsections (b) and (c) of this Section 11.

(b) *Customer Due Diligence*. For VASPs, a "threshold occasional transaction" for purposes of Section 3B of these Regulations is one or more occasional transactions when the total value of the transactions exceeds $1,000.

(c) *Virtual Asset Transfers*. All virtual asset transfers must be treated as cross-border transfers and subject to the requirements for cross-border wire transfers under Section 3M of these Regulations as follows:

(1) Originating VASPs must:

(i) obtain and hold full originator information as specified in Section 3M.1 and verify that the originator information is accurate;

(ii) obtain and hold full beneficiary information as specified in Section 3M.2;

(iii) submit the information obtained and held under (i) and (ii) to the beneficiary VASP or financial institution (if any) immediately and securely; and

(iv) make the information obtained and held under (i) and (ii) available on request to appropriate authorities.

(2) Beneficiary VASPs must:

(i) obtain and hold full originator information as specified in Section 3M.1;

(ii) obtain and hold full beneficiary information as specified in Section 3M.2 and verify that the beneficiary information is accurate, and

(iii) make the information obtained and held under (i) and (ii) available on request to appropriate authorities.

(3) All other requirements of Section 3M (including the monitoring requirements of Section 3M.9 and targeted financial sanctions requirements of Section 3M.17) apply on the same basis as set out in Section 3M.

(4) The same obligations as set out in this subsection (c) apply to non-VASP financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

Section 12. Guidelines.

(a) The Banking Commissioner may issue guidelines to assist banks, FSPs and DNFBPs to implement and comply with their AML/CFT requirements, including lists of higher risk countries for which enhanced CDD is required under Section 3I.3 of these Regulations.

(Rev. 05/13/2010)
(Rev. 01/30/2014)
(Rev. 05/16/2019)
(Rev. 05/27/2021)

(b) Guidelines issued by the Banking Commissioner may provide for the application of countermeasures by banks, FSPs, and DNFBPs when called upon to do so by the FATF, the Asia/Pacific Group on Money Laundering, or the Marshall Islands. These countermeasures should be effective and proportionate to the risks.

Section 13. International Cooperation.

(a) The Financial Intelligence Unit (Unit) may seek information or assistance from foreign competent authorities as necessary to fulfill its responsibilities under the Act.

(1) Information exchanged should be used only for the purpose for, and by the authorities, for which the information was sought or provided, unless prior authorization has been given by the requested competent authority.

(2) Appropriate confidentiality should be maintained for information exchanged, consistent with both parties' obligations concerning privacy and data protection. At a minimum, exchanged information should be protected in the same manner as similar information received from domestic sources.

(3) The Unit may provide feedback to its foreign counterparts, upon request and whenever possible, on the use of the information provided and on the outcome of the analysis conducted based on the information provided.

(b) The Unit may provide international cooperation and exchange information on money laundering, associated predicate offences, and terrorist financing with the instruction of the Banking Commissioner as outlined under §167 of the Act.

(1) The Unit may exchange: (i) all information required to be accessible or obtainable directly or indirectly by the Unit under the FATF Recommendations, and (ii) any other information which the Unit has the power to obtain or access directly or indirectly at the domestic level, subject to the principle of reciprocity.

(2) Appropriate confidentiality should be maintained for any request for cooperation.

(3) The Unit may refuse to provide information requested if the requesting competent authority cannot protect the information effectively.

Appendix 1

Part A: Delayed Verification

1. Examples of situations where it may be essential not to interrupt the course of the normal conduct of business include:

    a. non-face-to-face business;

    b. securities transactions; and

    c. life insurance in relation to identification and verification of the beneficiary under the policy, which may take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

Part B: Enhanced CDD for Higher Risk Customers

1. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, potentially higher-risk situations include, but are not limited to:

    <u>Customer risk factors:</u>

    a. a business relationship conducted in unusual circumstances;

    b. a non-resident customer, or if the nationality, current residency, and previous residency of the customer suggests greater risk of ML or TF;

    c. a business that is cash-intensive;

    d. a customer who is a politically exposed person;

    e. a high net worth customer, especially if the potential customer is a private banking customer or the source of funds is unclear;

    f. a business that is particularly susceptible to money laundering or terrorism financing;

    g. a legal person or arrangement that is a personal asset-holding vehicle;

    h. a legal person or arrangement whose ownership structure appears unusual or excessively complex given the nature of the company's business;

    i. a company with nominee shareholders or shares in bearer form;

    j. a customer who is a beneficiary of a life insurance policy;

Country or geographic risk factors:

k. countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as lacking proper standards in the prevention of ML or TF;

l. countries that are subject to sanctions/embargos or similar measures;

m. countries identified by credible sources as having significant levels of corruption or other criminal activity;

n. countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country;

Product, service, transaction or delivery channel risk factors:

o. private banking;

p. anonymous transactions (which may include cash);

q. non-face-to-face business relationships or transactions;

r. payment received from unknown or un-associated third parties;

Other risk factors:

s. any risk specifically identified or categorized as a higher risk, or that otherwise matches criteria identified as higher risk, in the Marshall Islands' national risk assessment; and

t. any situation that is higher risk for other reasons based on relevant information.

2. Non-face-to-face transactions include but are not limited to:

a. business relationships concluded over the Internet or by other means such as through the post;

b. services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services;

c. use of ATM machines;

d. mobile telephone banking;

e. transmission of instructions or applications via facsimile or similar means; and

f. making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or re-loadable or account-linked value cards.

3. Enhanced CDD procedures for non-face-to-face transactions may include:

a. certification of documents presented;

b. requisition of additional documents to complement those that are required for face-to-face customers;

c. development of independent contact with the customer.

4. Procedures for determining who is a PEP may include:

a. seeking relevant information from the potential customer;

b. referring to publicly available information; and

c. making access to commercial electronic databases of PEPs.

5. In applying enhanced due diligence, banks, FSPs, and DNFBPs must take care not to engage in unlawful discrimination on the basis of race, color, religion, or national origin.

Part C: Simplified CDD for Lower Risk Customers

1. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include:

Customer risk factors:

a. other banks, FSPs, and DNFBPs (other entities that are subject to supervision by the Banking Commission under these Regulations);

b. non-resident financial institutions that are subject to adequate regulation and supervision as limited by Section 3L of these Regulations;

c. public companies (or other legal persons or legal arrangements) quoted on an exchange regulated by the Banking Commission, and certain public companies quoted on a foreign exchange approved for this purpose by the Banking Commission that is subject to adequate supervision and providing the company is subject to adequate regulatory disclosure requirements, as limited by Section 3L;

d. domestic government administrations or enterprises, and certain foreign government administrations or enterprises as limited by Section 3L;

Product, service, transaction or delivery channel risk factors:

e. life insurance policies where the annual premium is no more than $1,000.00 or a single premium of no more than $2,500.00;

f. insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

g. pension, superannuation, or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

h. Beneficial Owners of non-resident pooled accounts, provided they are subject to adequate regulation and supervision as limited by Section 3L;

i. small scale accounts and micro-credit accounts with an annual turnover of under $200.00;

Country risk factors:

j. countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and

k. countries identified by credible sources as having a low level of corruption or other criminal activity.

2. Non-resident and foreign entities described in b., c., d., and h. may only qualify for simplified CDD if they are located in a jurisdiction that is implementing effectively the FATF Recommendations. In making this determination, banks, FSPs and DNFBPs should take into account the information available on whether these countries adequately apply the FATF Recommendations, including by examining the approved list provided by the Banking Commission and reports, assessments, and reviews published by FATF, International Monetary Fund, and World Bank publications.

3. Simplified CDD measures are not acceptable whenever a customer has been identified by the Banking Commission as non-complying with the FATF Recommendations, or for which the bank, FSP or DNFBP has independent credible reason to believe are not complying with the FATF Recommendations, or for any reason that there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

Schedule 1

A. Procedure for verification of individuals

1. Where a bank, FSP, or DNFBP is required to verify the identity of a person, the following information is required:

   (a) full and correct name of person and any other names previously held;

   (b) permanent address;

   (c) telephone (not including mobile phone number) and fax number (if any);

   (d) date and place of birth;

   (e) nationalities and citizenships held currently and previously by the applicant;

   (f) occupation and name of employer (if self employed, the nature of the self employment);

   (g) copy of first two pages of passport or copy of national identity card showing the following details:

      i. number and country of issuance;

      ii. issue and expiry date;

      iii. signature of the person (applicable only to national identity card);

   (h) signature;

   (i) purpose of the account and the potential account activity;

   (j) written authority to obtain independent verification of any information provided;

   (k) source of income or wealth;

   (l) written confirmation that all credits to the account are and will be beneficially owned by the bank and FSP holder;

   (m) any documentary or other evidence reasonably capable of establishing the identity of that person.

2. Paragraph 1 shall also apply to the verification of identity of the Beneficial Owners of all banks and FSPs.

B. Procedures for verification of corporate entities

Where a bank, FSP, or DNFBP is required to verify the identity of a corporate entity whether incorporated in the Marshall Islands or elsewhere, the following information is required:

(a) certified copy of the certificate of incorporation;

(Rev. 05/13/2010)
(Rev. 01/30/2014)
(Rev. 05/16/2019)
(Rev. 05/27/2021)

(b) certified copy of the Articles of Association of the entity;

(c) address of the registered office or registered agent of the corporate entity;

(d) resolution of the Board of Directors authorizing the opening of the account and conferring authority on the person who will operate the account;

(e) confirmation that the corporate entity has not been struck off the register or is not in the process of being wound up;

(f) names and addresses of all officers and directors of the corporate entity;

(g) names and addresses of the Beneficial Owners of the corporate entity, except a publicly traded company;

(h) description and nature of the business including:

i. date of commencement of business;

ii. products or services provided;

iii. address of principal place of business;

(i) purpose of the account and the potential parameters of the account including:

i. size, in the case of investment and custody accounts;

ii. balance ranges, in the case of deposit accounts;

iii. the expected transaction volume of the account;

(j) written authority to obtain independent verification of any information provided;

(k) written confirmation that all credits to the account are and will be beneficially owned by the bank and FSP holder;

(l) any other official document and other information reasonably capable of establishing the structural information of the corporate entity.

C. Verification of identity of partnerships or unincorporated businesses

Where a bank, FSP, or DNFBP is required to verify the identity of partnerships or other unincorporated businesses, the following information is required:

(a) verification of all partners or Beneficial Owners in accordance with the procedure for the verification of individuals;

(b) copy of partnership agreement (if any) or other agreement establishing the unincorporated business;

(c) address of the registered office or registered agent (if any) of the partnership or unincorporated business;

(d) description and nature of the business including:

i. date of commencement of business;

ii. products or services provided;

iii. address of principal place of business

(e) purpose of the account and the potential parameters of the account including:

i. size in the case of investment and client accounts;

ii. balance ranges, in the case of deposit and client accounts;

iii. the expected transaction volume of the account;

(f) mandate from the partnership or Beneficial Owner authorizing the opening of the account and conferring authority on those who will operate the account;

(g) written confirmation that all credits to the account are and will be beneficially owned by the bank and FSP holder;

(h) any documentary or other evidence reasonably capable of establishing the identity of the partners or Beneficial Owners.

D. Verification of trusts or other legal arrangements

Where a bank, FSP, or DNFBP is required to verify the identity of a trust or other legal arrangement, whether domestic or foreign, the following information is required:

(a) verification of all Beneficial Owners in accordance with the procedure for the verification of individuals;

(b) certified copy of the original trust agreement or other document forming the basis of the legal arrangement's existence and any amendments thereto;

(c) copy of any other document (if any) appointing, or providing for the appointment of, trustees (or trustee equivalents) or establishing the nature of their duties;

(d) the address of the registered office and, if different, a principal place of business;

(e) description and nature of the trust or other legal arrangement, including its formal name and date of commencement;

(f) purpose of the account and the potential parameters of the account including:

i. size in the case of investment and client accounts;

ii. balance ranges, in the case of deposit and client accounts;

iii. the expected transaction volume of the account;

(g) written authority from the settlor or trustee (or trustee equivalent) to open the account and to obtain independent verification of any information provided;

(h) written confirmation that all credits to the account are and will be beneficially owned by the bank and FSP holder; and

(i) any other reliable, independent source documents, data or information reasonably required to prove the legal arrangement's existence or establish the identity of its Beneficial Owners.

E. Verification of facilities established by telephone or Internet

1. Where a request is made to a bank or FSP by telephone, Internet, or written communication for a person, corporate entity, or partnership to become a bank and FSP holder, the bank or FSP shall verify the identity of that person, corporate entity, or partnership as provided in the relevant verification procedures in items A to C as appropriate.

2. Where the bank or FSP has obtained in writing confirmation from a foreign bank or FSP located in a country determined by the Banking Commissioner as having acceptable due diligence procedures, and that the other bank or FSP has verified the identity of the person or of the corporate entity specified in paragraph 1, no further verification of identity is necessary.