

FINANCIAL INTELLIGENCE UNIT

FIU REGULATION **AML-Regulation-01**

FINANCIAL TRANSACTIONS REPORTING **REQUIREMENTS FOR BANKS**

Arrangement of Paragraphs

PART I **Preliminary**

PARAGRAPH

1. Short Title
2. Authorization
3. Application
4. Definitions

PART II **Statement of Policy**

PARAGRAPH

1. Purpose
2. Scope
3. Responsibility

PART III **Implementation and Specific Requirements**

PARAGRAPH

1. Internal Policies, Systems and Controls
2. Customer Due Diligence & Identification
3. Reporting Transactions and Information
4. Supervisory Authorities
5. Border Currency Reporting

PART IV **Corrective Measures**

PARAGRAPH

1. Remedial Measures and Sanctions

PART V **Effective Date**

PARAGRAPH

1. Effective Date

Attachments:

- (1) Cash Transaction Reporting Form
- (2) Suspicious Activity Reporting Form

Annex:

- (1) Examples of Suspicious Transactions

PART I: PRELIMINARY

- 1: **Short Title** – Financial Transactions Reporting Regulations for Banks.
- 2: **Authorization** – The Financial Intelligence Unit (the FIU) of the Republic of Palau is authorized to issue and enforce regulations under Sections 3312(d), 3313, 3314(d), 3315(c), 3316(b), 3318(a), 3321(d), 3322, 3328(b)(12), and 3329(d)(h) of the Money Laundering and Proceeds of Crime Act 2001 Act [17 PNCA Chapter 38] as amended (MLPCA). Furthermore, the Financial Institutions Commission (the FIC) of the Republic of Palau (Palau) is authorized to promulgate regulations under Sections 1019 and 10.133 of the Financial Institutions Act of 2001 [26 PNCA Chapter 10] as amended (FIA).
- 3: **Application** – This Regulation applies to all Palau banks and the branches of foreign banks, credit institutions, and Alternative Money Remittance Services (ARS) in the Republic of Palau (hereafter collectively referred to as a “Reporting Institution(s),” or “Financial Institutions,” and/or “ARS”). For purposes of this Regulation reference to Reporting Institutions and/or Financial Institutions shall mean and refer to ARS equally as defined by section 3301(l) of the Act. The Regulation address obligations placed on reporting institutions under the MLPCA, and the FIA in relation to anti-money laundering and combating the financing of terrorism.

All Financial Institutions, as defined herein and must achieve full compliance with this regulation on or before March 01, 2018.

This Regulation is a regulatory requirements only, which means that it relates to the activities of Financial Institutions and Alternative Money Remittance Services), and cannot be relied upon to interpret or determine the application of the criminal laws of the Republic of Palau.

- 4: **Definitions** – Terms used within this regulation are as defined in the Money Laundering Proceeds of Crime Act (the "Act" and/or MLPCA) and/or the Financial Institutions Act (FIA), or as reasonably implied by contextual usage. Defined terms are identified throughout these Regulations by the capitalization of the initial letter of a word or phrase. Where capitalization of the initial letter is not used, an expression has its natural meaning.
 - 1) “Financial Institution” is defined in Section 3301(l) of the Act;
 - 2) “Alternative Money Remittance Services” (ARS) are defined as “any system used for transferring money from one location to another, and generally operating outside the banking channels.”
 - 3) “Politically Exposed Person” is defined in Section 3301(p) of the Act;
 - 4) "Act" means the Money Laundering and Proceeds of Crime Act, 17 PNCA §3300 et seq.;
 - 5) "Director" means the Director of the Palau Financial Intelligence Unit;

- 6) "Unit" means and refers to the Palau Financial Intelligence Unit or the FIU;
- 7) "Legal Person" means corporate, partnership, foundations, associations or any other similar entity that can establish a permanent customer relationship with a Financial Institution or otherwise obtain title to property;
- 8) "Legal Arrangement" refers to an express trust or other similar arrangement;
- 9) "FIC" means the Palau Financial Institutions Commission;

If a provision in this Regulation refers to a communication, notice, agreement or other document in writing" then, unless the contrary intention appears, it means in legible form and capable of being reproduced on paper, irrespective of the medium used. Expressions related to writing must be interpreted accordingly. This does not affect any other legal requirements which may apply in relation to the form or manner of executing a document or agreement.

A Financial Institution may seek guidance from the FIU where clarity is needed to interpret and/or apply any part of this Regulation.

PART II: STATEMENT OF POLICY

- 1: **Purpose** – This Regulation establish requirements for reporting institutions to have in place, risk management policies and procedures that promote high ethical and professional standards, and prevent the financial institution from being used, intentionally or unintentionally, by criminal elements. Reporting institutions are required to develop and implement effective policies to combat money laundering and the financing of terrorism.

The regulation incorporates a summary of obligations placed on reporting institutions and copies of reporting forms to be submitted to the FIC and the FIU are included as attachments to the regulation. An annex to the regulation provides examples of suspicious transactions.

- 2: **Scope** – This regulation applies to all financial and credit institutions licensed by the FIC to conduct business in Palau and any ARS doing business in the Republic of Palau.

A Financial Institution may apply the requirements of this Regulation on a risk-based approach.

Without prejudice to the requirements under Part III of this Regulation, the extent of implementation by a Financial Institution may depend on the degree of risk of money laundering or terrorist financing associated with a customer, transaction or product.

The approach of a Financial Institution in applying the requirements of this Regulation must be in accordance with approved policies and procedures as specified in Part III of this Regulation.

- 3: **Responsibility** – It is the responsibility of the board of directors, agents, or owners of each Reporting Institution to adopt a written Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) policy and to establish processes which ensure that the reporting institution is in compliance with the requirements of the Act.

To ensure that Palau is not used as a channel for criminal funds, all reporting institutions should:

- Comply with the FIU and the FIC's policies, regulations, directives, the FIA and the MLPCA. The Directors and Management of reporting institutions should ensure that FIC and FIU policies and all relevant Acts are adhered to and that a service is not provided where there are reasonable grounds to believe that transactions are associated with money laundering or terrorist financing offences;
- Appoint a compliance officer to be responsible for ensuring the institution's compliance with the requirements of the MLPCA;
- Establish an audit function to test its anti-money laundering procedures and systems;
- Co-operate with law enforcement agencies including the FIU on any constraints imposed by legislation relating to customer confidentiality or where there are reasonable grounds for suspecting money laundering or the financing of terrorism;

- Implement effective procedures for customer identification, record keeping, transaction monitoring and reporting suspicious transactions;
- Screen potential employees to ensure that employees are fit and proper;
- Ensure that its officers and employees are:
 - aware of the laws relating to money laundering and financing of terrorism; and
 - aware of the procedures and policies for compliance with anti-money laundering standards
 - trained to recognize suspicious transactions.

The FIC and FIU will conduct compliance audits of credit and financial institutions to assess compliance with the MLPCA and this regulation.

PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

1: Internal Policies, Systems And Controls

1.1 Adoption and Implementation of Internal Procedures, Policies and Controls

1.1.1 For the purposes of sections 3325 and 3326 of the MLPCA and the FIA, a Financial Institution must adopt and implement effective programs against money laundering and financing of terrorism that must include:

- a.) Written procedures, policies, systems, and controls to deter and prevent money laundering and financing of terrorism in accordance with the MLPCA and the FIA and this Regulation;
- b.) Written internal procedures, policies, and controls, including compliance management arrangements, to ensure compliance with the MLPCA and the FIA and this Regulation.

1.1.2 The policies referred to in Regulation 1.1.1 must have regard to the risk of money laundering and financing of terrorism, the size and nature of business, circumstances of a particular customer, and the types of products and services offered by the Financial Institution.

1.1.3 Without limiting the generality of the requirements of section 3317 of the MLPCA and the FIA, for purposes of section 3317 of the MLPCA and the FIA, the internal controls and policies of a Financial Institution must include measures to guard and prohibit the Financial Institution against establishing a relationship with a Shell Bank.

1.1.4 In this Regulation, "Shell Bank" shall mean and refer to a bank incorporated in a jurisdiction in which it has no physical presence or which is unaffiliated with a regulated financial group.

1.2 Compliance Officer

1.2.1 For purposes of section 3325 of the MLPCA and the FIA, a Financial Institution must designate an officer at the management level as its anti-money laundering and combating the finance of terrorism compliance officer (Compliance Officer) to perform the following functions:

- a.) Be responsible for ensuring compliance with the MLPCA and the FIA and this Regulation;
- b.) Be given appropriate and adequate authority and responsibility to implement the requirements of the MLPCA and the FIA and this Regulation;
- c.) Have the authority to act independently and to report to senior management above the Compliance Officer's next reporting level.

1.2.2 The Compliance Officer and other employees designated by such officer must have timely access to customer identification data and other customer due diligence information, transaction records and other relevant information.

1.2.3 Subject to section 3328 of the MLPCA and the FIA, a Financial Institution must provide the Bank Commissioner and the Unit with the contact information, and any change to such information for its Compliance Officer.

1.2.4 The Compliance Officer's contact information must be provided to the Bank Commissioner and the Unit including name, telephone number (officer hours direct line and cell), and mailing address.

1.2.5 For the purposes of section 3325 of the MLPCA and the FIA, a Financial Institution must establish and maintain an adequately resourced and independent audit function to test compliance (including sample testing) with the procedures, policies, and controls required under this Article, including:

- a.) Attestation of the overall integrity and effectiveness of the written procedures, policies, systems, and controls and technical compliance with the MLPCA and the FIA and this Regulation;
- b.) Transaction testing in all areas of the Financial Institution with emphasis on high-risk areas, products, and services to ensure that the Financial Institution is complying with the MLPCA and the FIA and this Regulation;
- c.) Assessment of the employees' knowledge of procedures, policies, systems, and controls;
- d.) Assessment of the adequacy, accuracy, and completeness of employee training programs;
- e.) Assessment of the adequacy and effectiveness of the Financial Institution's process for identifying and reporting suspicious transaction and activities, and other reporting requirements under the MLPCA and the FIA and this Regulation.

1.2.6 A Financial Institution may provide a copy of the report of the audit function undertaken under Regulation 1.2.5 to the Unit and a supervisory authority.

1.2.7 Notwithstanding Regulation 1.2.5, an auditor of a Financial Institution must report to the Unit any suspicious information or transaction noted during the audit function.

1.2.8 For the purpose of section 3325(e) of the MLPCA and the FIA, a Financial Institution must put in place screening procedures to ensure high standards when hiring employees and to prevent the employment of persons convicted of offenses involving fraud and dishonesty.

1.2.9 Any procedure for screening employees must ensure that:

- a.) Employees have the high level of competence necessary for performing their duties;
- b.) Employees have appropriate ability and integrity to conduct its business activities;
- c.) Potential conflicts of interests are taken into account, including the financial background of the employee;
- d.) Proper code of conduct requirements are defined;
- e.) Persons convicted of offenses involving fraud, dishonesty or other similar offenses are not employed by it.

1.2.10 For purposes of section 3325(d) of the MLPCA and the FIA, a Financial Institution must establish ongoing employee training to ensure that employees are kept informed of new developments, including:

- a.) Information on current money laundering and financing of terrorism techniques, methods and trends; and
- b.) Aspects of anti-money laundering and combating the financing of terrorism laws and obligations and in particular requirements concerning due diligence and suspicious and other transactions reporting.

2: Customer Due Diligence & Identification

2.1 Requirements for Customer Due Diligence

2.1.1 Without limiting Section 3312 of the MLPCA and the FIA, a Financial Institution must undertake the customer due diligence measures set out in this Regulation including:

- a.) Identification of customers, including beneficial owners owning 25 percent (25%) or more of the vote or value of an equity interest in an entity and one controller and the verification of the customers' identity;
- b.) Gathering 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; and
- e.) Ongoing monitoring of customers and transactions

2.2 Scope of Customer Identification

2.2.1 When conducting customer identification and verification, a Financial Institution shall obtain the following information about the customer:

- a.) Full name of customer;
- b.) The residential or business address in Palau;
- c.) The date of birth;
- d.) The occupation, business or principal activity (including name of employer or nature of self employment or business);
- e.) Specimen signature;
- f.) Citizenship; and
- g.) Checked against the U.S. Office of Foreign Asset Control (OFAC) Sanctions List or similar list designated by the competent authorities of the Republic of Palau.

2.3 *Identification of Customers who are Natural Persons*

2.3.1 For a customer who is a natural person, a Financial Institution must identify the customer on the basis of one or more of the following documents:

- a.) A valid passport;
- b.) A birth certificate;
- c.) A marriage certificate;
- d.) Citizenship certificate;
- e.) A valid driver's license;
- f.) Any other unexpired government issued identification evidencing nationality or residence and bearing photograph or similar safeguards; and
- g.) Any other evidence of identity, as may be determined by the FIU.

2.3.2 The identification and verification requirements of this Regulation 2.3.1 shall not be applicable to a person that has an existing account with the Financial Institution, provided that the Financial Institution has a reasonable belief that it knows the true identity of the person.

2.4 *Identification of Customers who are Legal Persons or Arrangements*

2.4.1 For a customer that is a legal entity or other form of legal arrangement, a Financial Institution must obtain and verify:

- a.) The customer's name, address and legal form, obtaining proof of incorporation or similar evidence of establishment or existence including a certificate of registration for the Registrar of Corporations, a valid Foreign Investment Certificate, if applicable, from the Foreign Investment Board;

- b.) The identity of the natural person purporting to act on behalf of the customer using reliable, independently sourced documents as provided in regulation 2.3.1;
- c.) Where the customer is a business, either for profit or otherwise, the business license from the Minister of Finance.

2.4.2 The identification and verification requirements of this Regulation 2.4.1 shall not be applicable to a legal entity or other form of legal arrangement that has an existing account with the Financial Institution, provided that the Financial Institution has a reasonable belief that it knows the true identity of the legal entity or other form of legal arrangement.

2.4.3 A Financial Institution must take reasonable measures to understand and document the ownership and control structure of the legal person or arrangement including the name and residential street address of the natural person(s) who ultimately own or control the legal person or arrangement.

2.4.4 For a customer that is a corporation, company, limited liability company, general partnership, limited partnership, or similar form of arrangement, a Financial Institution must identify and verify the principal owner of the company, general partnership, limited partnership or similar arrangement, and must at a minimum identify:

- a.) Each natural person who owns directly or indirectly 25 percent (25%) or more of the vote or value of an equity interest in the entity; and
- b.) One person exercising effective control of the entity, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer or any other individual who regularly performs similar functions; and
- c.) Each natural person who exercises signing authority on behalf of the entity.
- d.) If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner for purposes of this Regulation 2.4.4 shall mean the trustee.

2.4.5 For a customer that is a trust or other similar arrangement, the Financial Institution must identify and verify the identity of the trustee.

2.4.6 In determining indirect ownership of equity interests:

- a.) an equity interest held by a corporation, company, limited liability company, general partnership, limited partnership, trust or other similar arrangement, must be considered as being owned proportionately by its shareholders, members, partners, or vested beneficiaries;

2.4.7 In the case of non-face-to-face customers, in addition to the requirements of regulations set forth hereinabove, a Financial Institution must use other additional procedures for identification

and verification to ensure compliance with customer identification and verification requirements including:

- a.) Use of certified documentation;
- b.) Requisition of additional documents to compliment those that are required for face-to-face customers;
- c.) Independent contact with the customer by the Financial Institution;
- d.) Third party introduction
- e.) Comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other sources;

2.5 *Identification of Customers who are Non-Profit Organizations*

2.5.1 For a customer that is a non-profit organization, group or agency (such as a charitable and religious organization), a Financial Institution must also satisfy itself as to the legitimate purpose of such organization, group or agency, such as reviewing the charter, constitution or trust instrument of the organization, group or agency as identified by the Office of the Attorney General and or the Ministry of Finance.

2.6 *Monitoring of Customers on an Ongoing Basis*

2.6.1 For purposes of section(s) 3314 and 3315 of the MLPCA and the FIA, a Financial Institution must gather and maintain customer information on an on-going basis and monitor transactions on an on-going basis.

2.6.2 The monitoring system must, taking into account the size and nature of the business of a Financial Institution, be capable of identifying any transaction that is:

- a.) From any source or to any recipient, identified as being of questionable legitimacy;
- b.) Unusual in terms of:
 - i. The amount such as by reference to predetermined limits for the customer in question or to comparative figures for similar customers;
 - ii. The type, such as international wire transfers or the customer in question;
 - iii. The number, such a high account activity in relation to the size of the balance of the customer in question; and
 - iv. Any other risk factor identified by the Financial Institution.
- c.) Identified in writing by the Unit as being a transaction that the Financial Institution must monitor.

2.7 *Customer Profile*

2.7.1 For purposes of section 3312 of the MLPCA and the FIA, a Financial Institution must create and maintain a customer profile for each customer of sufficient nature and detail to enable the Financial Institution to monitor any transaction of the customer, apply enhanced customer due diligence where necessary, and detect suspicious transactions.

2.7.2 A customer profile must include:

- a.) Relevant information as to the normal and reasonable activity for particular types of customers taking into account the nature of the customer's business;
- b.) A comprehensive accounting or summary of the customer's transactions;
- c.) Where necessary, the source and legitimacy of the funds; and
- d.) The overall relationship with the Financial Institution.

2.8 *Purpose of Transaction, Origin and Destination of Funds*

2.8.1 In addition to Regulation 2 and for purposes of section 3314 of the MLPCA and the FIA, a Financial Institution must implement internal controls and procedures that establish the type, volume and value, and the origin and destination of funds involved in a transaction.

2.8.2 An internal control and procedure referred to in Regulation 2.9.1 may include the following:

- a.) Any measure required under Regulation 2 of this Regulation;
- b.) Any other additional measure to ensure that the required information is obtained when a transaction is conducted by the customer;

2.8.3 A Financial Institution:

- a.) must not proceed with a transaction if it had failed to ascertain the required information;

2.9 *Enhanced Customer Due Diligence for Higher Risk Customers*

2.9.1 A Financial Institution must undertake enhanced customer due diligence of any customer and any transaction that the institution has determined is of higher risk of money laundering and financing of terrorism.

2.9.2 Any enhanced customer due diligence must include enhanced:

- a.) Scrutiny of customer's identity (including of the beneficial owner and controller);
- b.) Scrutiny of the source and legitimacy of funds;
- c.) Transaction monitoring; and
- d.) Customer profiling.

2.9.3 Any enhanced customer due diligence must be applied to any higher risk customer, business relationship or transaction, as appropriate at each stage of the customer identification and verification process.

2.9.4 In addition to measures required in Regulation 2, a Financial Institution must have policies and procedures in place and must ensure an effective implementation of these measures to address any specific risk associated with non-face-to-face business relationships or transactions.

2.9.5 Pursuant to section 3313 of the MLPCA, and the FIA, a Financial Institution must undertake enhanced customer due diligence in relation to a *Politically Exposed Person*, as a category of high risk customer.

2.9.6 A Financial Institution must put in place appropriate risk management systems to determine whether a customer or a potential customer or the beneficial owner is a *Politically Exposed Person*.

2.9.7 A relevant supervisory authority or the Unit may issue guidelines specifying the factors a Financial Institution must take into account when determining whether a customer is of a higher risk.

2.10 *Simplified Customer Due Diligence for Lower Risk Customers*

2.10.1 For the purposes of section 3312 of the MLPCA and the FIA, a Financial Institution may apply a simplified customer due diligence procedure in certain circumstances if:

- a.) The risk of money laundering or financing of terrorism is lower;
- b.) Information on the identity of the customer and the beneficial owner of a customer is publicly available; or
- c.) Adequate checks and controls exist in Palau.

2.10.2 For purposes of Regulation 2.11.1 customers that may be subject to “*simplified*” due diligence include:

- a.) Licensed regulated Financial Institutions;
- b.) Locally incorporated public companies in which all the share holders, directors and officers are Palauan and subject to regulatory and disclosure requirements; or
- c.) Palau government (national or state) agencies;

2.10.3 Simplified customer due diligence may include a lower level of:

- a.) Scrutiny for customer identification;
- b.) Scrutiny of the source and legitimacy of the funds;

- c.) Scrutiny of the legitimacy of the recipient of the funds;
- d.) Transaction monitoring; and
- e.) Customer profiling.

2.10.4 A Financial Institution, as a minimum requirement, must obtain information about the name and address of the customer, occupation and the legal form and nature of business activity conducted by the customer.

2.10.5 A Financial Institution must terminate simplified customer due diligence procedures when there is suspicion of money laundering or terrorist financing or conditions under regulation 2.10 apply.

2.10.6 The relevant supervisory authority or the Unit may issue guidelines specifying what factor a financial institution must take into account when determining whether customer are of a lower risk.

2.11 Due Diligence of Existing Customers

2.11.1 A Financial Institution must:

- a.) Apply customer due diligence requirements on existing customers on the basis of materiality and risk; and
- b.) Conduct due diligence on such existing relationships at appropriate times as specified in the Financial Institution's internal policies and procedures.

3: Reporting Transaction And Information

3.1 Reporting of Suspicious Transactions

3.1.1 For the purposes of section 3314 of the MLPCA and the FIA, a Financial Institution must report any transaction referred to in section 3314 of the MLPCA and the FIA in the form as outlined in this Regulation, Suspicious Transaction Reports (STR):

- a) Criminal violations involving insider abuse in any amount.
- b) Criminal violations aggregating \$5,000 or more when a suspect can be identified.
- c) Criminal violations aggregating \$25,000 or more regardless of a potential suspect.
- d) Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating \$5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
 - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
 - Is designed to evade MLPCA and the FIA regulations
 - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to be engaged in, and the bank

knows of no reasonable explanation for the transaction after examining the available facts. Including the background and possible purpose of the transaction.

- a.) All suspicious funds and transactions, including attempted transactions, and all suspicious information;
- b.) Pursuant to section 3321(b) of the MLPCA and the FIA, all transactions and attempted transactions for which satisfactory evidence of identity has not been obtained under the MLPCA and the FIA and this Regulation; or
- c.) Pursuant to sections 3320 and 3321 of the MLPCA and the FIA, information relating to terrorist groups.

3.1.2 A relevant supervisory authority and the Unit may issue guidelines relating to the reports to be made under section 3314 of the MLPCA and the FIA.

3.2 *Reporting Cash Transactions*

3.2.1 For the purposes of section 3322 of the MLPCA and provisions of the FIA, a Financial Institution must report to the Unit any transactions of any amount in cash more than \$10,000 (U.S.) or its equivalent in foreign currency except as provided for in sub Regulation 3.2.2.

3.2.2 A Financial Institution need not report the following class of transactions of an amount in cash of more than \$10,000 (U.S.) or its equivalent in foreign currency if:

- a.) Transactions with established retail customers, as specified in writing by the Unit except transactions involving the selling of vehicles, vessels, farm machinery, aircraft, jewellery, or other high value commodities;
- b.) Transactions with the Palau government authorities;
- c.) Routine payroll transactions; and
- d.) Transactions with other class or type of customers, as specified by the Unit.

3.2.3 A Financial Institution may transmit to the Unit a report referred to in sections 3314 and 3321 of the Act through the following methods:

- a.) Electronically by a secure reporting system established by the Unit;
- b.) Electronically by secure email;
- c.) In a diskette, compact disk or other similar form;
- d.) By submitting the completed forms in writing by hand delivery;
- e.) By submitting the completed form in writing by facsimile;

3.2.4 Notwithstanding Regulation 3.2.3, a Financial Institution must report to the Unit the reports referred to in sections 3314, 3321 and 3322 of the Act electronically by a secure reporting system established by the Unit if 50 transactions either CTR/STR are reported on an annual basis.

3.2.5 The report referred to in Regulation 3.2.4 shall be submitted as soon as practical after the Financial Institution forms the suspicion or obtains the information referred to in sections 3314, 3321 and 3322 of the MLPCA and the FIA but no later than 30 (thirty) calendar days from the date of the initial detection of facts that may constitute a basis for filing a STR. If no suspect can be identified, the time period for filing a STR is extended to 60 (sixty) calendar days.

3.2.6 A CTR report required under Regulation 3.2.4 shall be transmitted to the Unit:

- a.) No later than the end of 15 (fifteen) calendar days after the day in which the transaction was undertaken;

3.2.7 The reports may be transmitted by batch, and the Unit and a Financial Institution must agree as to what constitutes a batch.

3.2.8 A relevant supervisory authority or the Unit shall issue guidelines in relation to the reporting of transactions referred to in Regulations 3.2.3 and 3.2.4.

3.2.9 The suspicious transactions report referred to in Regulation 3.1 must contain all relevant information concerning the customer, transaction and financial institution, as set out in the guidelines provided by the Unit.

3.2.10 The cash transaction report referred to in Regulation 3.2 must contain all relevant information concerning the customer, transaction and Financial Institution as set out in the guidelines provided by the Unit.

4: Supervisory Authorities

4.1.1 The relevant Supervisory Authority as defined in section 3328 of the Act or the Unit may issue guidelines in relation to the development and implementation of internal procedures, policies, controls, and programs by Financial Institutions.

4.1.2 The relevant Supervisory Authority may issue guidelines to the Financial Institutions for the purpose of implementing the requirements relating to customer due diligence, record keeping and retention and reporting obligations and internal controls and programs necessary to implement the obligations of the MLPCA and to provide guidance to the Financial Institutions on the implementation of requirements of the MLPCA and this Regulation.

4.1.3 The relevant Supervisory Authority may issue guidelines specifying what factors the Financial Institutions must take into account when determining whether customers are of a high risk.

4.1.4 The relevant Supervisory Authority may issue guidelines specifying what factors the Financial Institutions must take into account when determining whether customers are of a lower risk.

4.1.5 The relevant Supervisory Authority may issue guidelines in relation to the reporting of financial transactions referred to in section 3314, 3321 and 3322 of the MLPCA.

4.1.6 The relevant Supervisory Authority may issue guidelines in relation to the reporting of suspicious transactions referred to in section 3321 of the MLPCA.

5: Border Currency Reporting

5.1.1 A person who departs from or arrives in the Republic of Palau with more than \$10,000 in U.S. currency or its equivalent or in negotiable bearer instruments on his or her person or in his or her baggage must be:

- a.) Declared in the first instance on the Palau Travellers' Information Card on arrival or declared at departure; and
- b.) Reported to the Palau Customs Authority who in turn must report all such cross-border currency whether declared or not to the Unit.

5.1.2 For the purposes of sharing and the exchange of information under section 3334 of the MLPCA, the FIU may enter into an agreement or arrangement with the following agencies and authorities:

- a.) The Ministry of Justice;
- b.) The Minister of Finance;
- c.) The Bureau of Customs & Border Protection, including the sharing of Cross-Border Currency Reports;
- d.) The Attorney General's Office;
- e.) The Immigration Office;
- f.) The Foreign Investment Board; and
- g.) Any other government institution, agency, or department.

PART IV: CORRECTIVE MEASURES

- 1: **Remedial measures and sanctions** – If any reporting institution fails to comply with the MLPCA or the FIA, the FIC and/or FIU may impose any one or more of the remedial measures or penalties provided in the MLPCA and the FIA.

PART V: EFFECTIVE DATE

1: **Effective date** – The effective date of this regulation shall be NOVEMBER 28 2017.

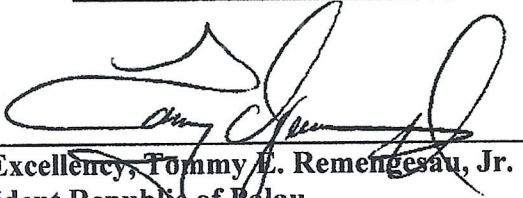
Questions relating to this regulation may be addressed to the Financial Intelligence Unit of the Republic of Palau.

Adopted November 15, 2017



Governing Board
Financial Institutions Commission
Republic of Palau

Approved NOVEMBER 28, 2017



His Excellency, Tommy E. Remengesau, Jr.
President Republic of Palau

Attachments:

- (1) Sample Currency Transaction Report Form
- (2) Sample Suspicious Activity Report Form

Annex:

- (1) Examples of Suspicious Transactions

ATTACHMENT 1

CURRENCY TRANSACTION REPORTING FORM

Financial Intelligence Unit Koror, Palau 96940		Currency Transaction Report ➤ Please type or print <i>(Complete all parts that apply)</i>				
Check all that apply: a. ☐ Amends prior report b. ☐ Multiple Persons c. ☐ Multiple Transactions						
Part I. Person(s) Involved in Transaction(s)						
Part I(a) Person Whose Behalf Transaction is Conducted						
Last Name or Entity Name			First Name		Middle Name	
Doing Business As (DBA)					SSN or EIN	
Mailing Address					Date of Birth MM / DD / YYYY	
City	State	Zip Code	Country		Occupation	
Type of Identification			a. ☐ Driver's License		b. ☐ Passport	
Alien Registration					c. ☐	
d. ☐ Other			e. Issued by:		f.	
Number:						
Part I (b) Person(s) Conducting Transaction(s) *Mark (X) all that applies if this part is left blank. ↓						
a. ☐ Night Deposit or Automated Teller Machine b. ☐ Multiple Transactions c. ☐ Conducted On Own Behalf						
Last Name			First Name		Middle Name	
Title					SSN	
Mailing Address			Telephone		Date of Birth MM / DD / YYYY	
City	State	Zip Code	Country			
Type of Identification			a. ☐ Driver's License		b. ☐ Passport	
Alien Registration					c. ☐	
d. ☐ Other			e. Issued by:		f.	
Number:						
Part II. Amount and Type of Transaction						
Total Cash In \$			Total Cash Out \$			Date of Transaction MM/DD/YYYY
Foreign Cash In			Foreign Cash Out			
☐ Foreign Country Instrument(s) Purchased			☐ Wire Transfer			☐ Negotiable
☐ Negotiable Instrument(s) Cashed Deposit(s)/Withdrawal(s)			☐ Currency Exchange(s)			
☐ Account Number(s) Affected			☐ Other (Specify)			

Part III. Reporting Financial Institution				
Name of Financial Institution				EIN or TIN
Address				Routing Number
City, State		Country	Zip Code	Date of Signature ____/____/____ MM/ DD/YYYY
Sign Here →	Title of Approving Official	Signature of Approving Official		Telephone Number
	Preparer's Name and Title	Person to Contact		

ATTACHMENT 2

SUSPICIOUS ACTIVITY REPORTING FORM

SUSPICIOUS TRANSACTION REPORT		Republic of Palau Financial Intelligence Unit		1
Part I Reporting Financial Institution Information				
Name of Financial Institution		EIN		
Address of Financial Institution	City	State	Zip Code -	
Branch Office(s) where activity occurred	☐ Multiple Branches (include information in narrative, PART V)		If Institution closed, date closed MM DD YYYY	
Part II Suspect Information		☐ Suspect Information Unavailable		
Last Name or Name of Entity	First Name	Middle		
Address of Branch Office		City	Country	Zip Code -
Account Number(s) affected, if any		Closed?		
a	☐ Yes ☐ No	c	☐ Yes ☐ No	
b	☐ Yes ☐ No	d	☐ Yes ☐ No	

Address				Palau ID			
City		State	Zip Code		Country		
					-		
Phone Number – Residence (include area code) ()				Phone Number – Work (include area code) ()			
Occupation/Type of Business		Date of Birth _____ MM DD YYYY			Admission/Confession?		
					a ☐ Yes b ☐ No		
Forms of Identification for Suspect:							
Number _____				Issuing Authority _____			
Relationship to Financial Institution:							
a ☐ Accountant	d ☐ Attorney	g ☐ Customer		j ☐ Officer			
b ☐ Agent	e ☐ Borrower	h ☐ Director		k ☐ Shareholder			
c ☐ Appraiser	f ☐ Broker	i ☐ Employee		l ☐ Other: _____			
Is the relationship an insider relationship? a ☐ Yes b ☐ No				Date of Suspension, Termination, Resignation			
If Yes, specify: c ☐ Still employed at financial institution e ☐ Terminated				_____ MM DD YYYY			
d ☐ Suspended f ☐ Resigned							

Part III Suspicious Transaction Information

2

Date or date range of suspicious transaction				Total dollar amount involved in known or suspicious transaction													
From		To		\$													
MM DD YYYY		MM DD YYYY															
Summary characterization of suspicious transaction:																	
a	☐	Money Laundering and Proceeds of Crime Act				f	☐	Computer Intrusion				l	☐	Debit Card Fraud			
b	☐	Bribery/Gratuity				g	☐	Consumer Loan Fraud				m	☐	Defalcation/Embezzlement			
c	☐	Check Fraud				h	☐	Counterfeit Check				n	☐	False Statement			
d	☐	Check Kiting				i	☐	Counterfeit Credit/Debit Card				o	☐	Misuse of Position or Self Dealing			
e	☐	Commercial Loan Fraud				j	☐	Counterfeit Instrument (other)				p	☐	Mortgage Loan Fraud			
s	☐	Other				k	☐	Credit Card Fraud				q	☐	Mysterious Disappearance			
												r	☐	Wire Transfer Fraud			
												t	☐	Terrorist Financing			
												u	☐	Identity Theft			
(type of transaction)																	
Amount of loss prior to recovery (if applicable)								Dollar amount of recovery (if applicable)								Has the suspicious activity had a material impact on, or otherwise affected the financial soundness of the institution?	
\$.00								\$.00									
Has the institution's bonding company been notified?														a ☐ Yes b ☐ No			
a ☐ Yes b ☐ No																	

Part IV Contact for Assistance

Last Name		First Name		Middle
Title/Occupation		Phone Number (include area code) ()		Date Prepared MM DD YYYY
Agency (if not filed by financial institution)				

Part V	Suspicious Transaction Information Explanation/Description	3
--------	--	---

--

ANNEX 1**EXAMPLES OF SUSPICIOUS TRANSACTIONS****Account transactions**

Transactions conducted through accounts operated in the following circumstances may give reasonable grounds for suspicion:

- Customers who wish to maintain a number of trustee or client accounts that do not appear consistent with the type of business, including transactions involving nominee names.
- Customers who, for no apparent or logical reason, have numerous accounts and deposit cash to each of them in circumstances where the total credit, if or when combined together, would be a large amount.
- Customers who have active accounts with several financial institutions within the same locality, particularly when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of funds.
- Matching payments paid-out with credits paid-in by cash on the same or previous day.
- Payments in large third party checks endorsed in favor of the customer.
- Customers who give conflicting information to different staff members.
- Large cash withdrawals from a previously inactive account, or from an account which has just received an unexpected large credit from abroad.
- Reluctance to use normal banking facilities, for example, avoiding high interest rate facilities for large balances.
- Large number of individuals making payments into the same account without adequate explanation.
- Customers who appear to be acting together, simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.
- Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

Cash Transactions

Cash transactions involving the following types of activities may give reasonable grounds for suspicion:

- Company accounts that are dominated by cash transactions, for example, an absence of other monetary instruments normally associated with commercial businesses, such as checks or credit cards.
- Frequent exchanges of cash into other currencies, where there appears to be no logical explanation for such activity.
- Transfers of large sums of money to or from overseas locations with instructions for payment in cash.

- Accounts operated by customers who refuse to provide appropriate identification or use misleading identification, or make it difficult to verify information. Bank accounts may be opened with forged documentation, which is difficult to detect.
- Several transactions conducted on the same day and at the same branch of a financial institution with a deliberate attempt to use different tellers.
- Cash deposits or withdrawals fall consistently just below occasional transaction thresholds. This practice is commonly referred to as structuring or smurfing and is often used to avoid threshold amounts that trigger identification requirements.

Customer Characteristics

Unusual transactions that are out of character with known customer routines or behavior may give reasonable grounds for suspicion:

- Stated occupation of an individual does not correspond with the type or size of transactions conducted.
- Unusual discrepancies in identification, such as, name, address or date of birth.
- Individuals involved in cash transactions who share addresses, particularly when the addresses are also business locations.
- Customers seemingly acting together simultaneously using separate tellers to conduct large cash transactions or foreign exchange transactions.
- Company representatives who avoid contact with bank staff when opening accounts or making business transactions.

Deposits and Withdrawals

The following types of deposits and withdrawals may give reasonable grounds for suspicion:

- Inactive accounts that contain a minimal sum and then unexpectedly receive a deposit, or several deposits, followed by constant withdrawals that continue until the sum has been completely removed.
- Deposits that contain counterfeit notes or forged instruments, as well as cash that has an unusual appearance or smell.
- Large cash deposits using automatic teller machines (ATMs) or drop boxes to avoid direct contact with bank staff.

International Transactions

The following types of off-shore international activity may give reasonable grounds for suspicion:

- Use of letters of credit and other methods of trade finance to move money between countries, where such trade is not consistent with the customer's usual business.
- Customers who make regular, large payments, including electronic transfers, that are unable to be clearly identified as genuine transactions to, or receive regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs or transnational crimes; or tax haven countries.

- Build up of large balances, not consistent with the known turnover of customer's business, and subsequent transfer to accounts held overseas.
- Unexplained electronic fund transfers by customers on an in-and-out basis or without passing through an account.
- Frequent cashing of travelers' checks or foreign currency drafts, particularly if originating from overseas.

Wire transfers

Wire transfers have long been considered one of the more popular and convenient means of transferring money across international borders. The speed and sheer volume in which wire transfers are carried out makes them an ideal mechanism for criminals to hide transactions.

Examples of potentially suspicious wire transfers include:

- Multiple personal, business or non-profit organization accounts are used to collect then channel funds to a small number of foreign recipients.
- Client orders wire transfers in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Client transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash.
- Client receives large sums of money from an overseas location via electronic funds transfer that includes instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Client receives electronic funds transfers and immediately purchases monetary instruments prepared for payment to a third party which is inconsistent with or outside the normal course of business for the client.
- Client requests payment in cash immediately upon receipt of a large electronic funds transfer.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client shows unusual interest in electronic funds systems and questions limit of what amount can be transferred.
- Client transfers funds to another country without changing the form of currency.
- Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities having no apparent business connection with client.
- Size of electronic transfers is out-of-keeping with normal business transactions for that client.
- Wire transfers do not have information about the beneficial owner or originator when the inclusion of this information would be expected.
- Stated occupation of the client is not in keeping with the level or type of activity (for example a student or an unemployed individual who receives or sends large numbers of wire transfers).
- Beneficiaries of wire transfers involve a large group of nationals of countries associated with terrorist activity.

- Client conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices.
- Client makes electronic funds transfers to free trade zones that are not in line with the clients business.

Loan transactions

The following scenarios may give reasonable grounds for suspicion:

- Client suddenly repays a problem loan unexpectedly.
- Client's employment documentation lacks important details that would make it difficult for you to contact or locate the employer.
- Client has loans to or from offshore companies that are outside the ordinary course of business of the client.
- Client offers you large dollar deposits or some other form of incentive in return for favorable treatment on loan request.
- Client asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known.
- Loan transactions are entered into in situations where the client has significant assets and the loan transaction does not make economic sense.
- Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
- Client applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate law and the application is outside the ordinary course of business for the client.