FINANCIAL INTELLIGENCE UNIT

FIU REGULATION
AML/CFT-Regulation-02

FINANCIAL TRANSACTIONS REPORTING REQUIREMENTS FOR DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

Arrangement of Paragraphs

PART I
Preliminary

PARAGRAPH

PART II
Statement of Policy

PARAGRAPH

PART III
Implementation and Specific Requirements

PARAGRAPH

PART IV
Reporting Requirements

PARAGRAPH

PART I: PRELIMINARY

1: **Short Title** – Financial Transactions Reporting Regulations for Designated Non-Financial Businesses and Professions (DNFBP).

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).

3: **Application** – These Regulations apply to all DNFBPs as defined herein. The Regulations address obligations placed on DNFBPs reporting under the MLPCA. All DNFBPs must achieve full compliance with these regulations on or before January, 2022.

These Regulations are regulatory requirements only that relate to the activities of DNFBPs under the supervision of the Financial Intelligence Unit (FIU) and/or the Financial Institutions Commission (FIC), 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 these regulations are as defined in the MLPCA (and/or the "Act"), 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) "*Designate Non-Financial Business And Profession* is defined in §3301(j) of the Act;
2) "*Act*" means the Money Laundering and Proceeds of Crime Act, 17 PNCA §3301 et seq.;
3) "*Director*" means the Director of the Palau Financial Intelligence Unit;
4) "*Unit*" means and refers to the Palau Financial Intelligence Unit or the FIU;
5) "*Legal Person*" means corporate, partnership, foundations, associations or any other similar entity that can establish a permanent customer relationship with a Financial Institution;
6) "*Legal Arrangement*" refers to an express trust or other similar arrangement;
7) "*Politically Exposed Person*" is defined in section 3301(q) of the Act;
8) "*Lawyers and other Independent Legal Professionals*" are defined in section 3301(j)(4) of the Act.

If a provision in these Regulations refers to a communication, notice, agreement of 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 DNFBP may seek guidance from the FIU where clarity is needed to interpret and/or apply any part of these Regulations.

PART II: STATEMENT OF POLICY

1: **Purpose** – These Regulations establish requirements for DNFBPs to have in place risk management policies and procedures that promote high ethical and professional standards and prevent the DNFBP from being used, intentionally or unintentionally, by criminal elements. DNFBPs 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 DNFBPs and copies of reporting forms to be submitted to the FIU are included as attachments to the regulation. An annex to the regulations provides examples of suspicious transactions.

2: **Scope** – These regulations apply to all DNFBPs doing business in Palau.

2.1 These Regulations apply to the following DNFBP:

2.1.1 Real Estate Agents (defined as any person (real or legal) licensed to negotiate and arrange real estate sales who is involved in transactions for a client concerning the buying, selling, or leasing of real estate in relation to both the purchasers and vendors of property, meaning an individual who negotiates and arranges or shows property for sale and performs any task involved in the sale or leasing of real property, including, but not limited to, listing property, filling in contracts, listing agreements, and purchase contracts. Real Estate Agent includes any person who has obtained a business license from Bureau or Revenue and Taxation to operate a business buying, selling, leasing, purchasing real property for a client whether that person is working for or under a licensed broker or not.)

2.1.2 Dealers in precious metals and dealers in precious stones when they engage in any cash transactions with a client the value of which singularly, or in several transactions, that appear to be linked, equal to or exceeding $10,000.

2.1.3 Casinos authorized by the appropriate government agency to engage in gaming activities and defined as any business, private or public, engage in the act or practice of gambling which is defined as "*an agreement between two or more individuals to play collectively at a game of chance for a stake or wager, which will become the property of the winner and to which all involved make a contribution.*" Casino includes, without limitation, stand alone casinos, casino hotels, ocean going casinos (with a home port in Palau), bingo halls, gambling machine manufacturers, lottery services, Internet gambling services, bookmaking and other gambling services or as otherwise determined by the FIU.

2.1.3 Dealers in High Value Goods and services when they engage in any cash transactions with a client the value of which singularly, or in several transactions that appear to be linked, equal to or exceeding $10,000. "High Value Goods" includes:

a.) Vehicles;

b.) Boats and boat engines;

c.) Electronics:

d.) Antiquities;

e.) Art Work; and

f.) Sports Memorabilia

2.1.4 Lawyers, notaries, other independent legal professionals and accountants, including auditing service providers when they prepare for or carry out transactions for their clients concerning:

a.) buying and selling or leasing of real estate;

b.) management of client money, securities or other property;

c.) management of a 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 arrangements, and buying and selling of business entities.

f.) Company service providers when they prepare for or carry out transactions for a client concerning:

i. acting as a formation agent of legal persons;

ii. 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;

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

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

2.2 A DNFBP may apply the requirements of these Regulations on a *Risk-Based Approach.* (*Risk-Based Approach* is defined as the process of determining the likelihood of a given event based on a proportionate assessment of the threat of that event occurring.)

2.3 Without prejudice to the requirements under Part III of these Regulations, the extent of implementation by a DNFBP may depend on the degree of *risk* of money laundering or terrorist financing associated with a customer transaction or product.

2.4 The approach of a DNFBP in applying the requirements of these Regulations must be in accordance with approved policies and procedures as specified in Part III of these Regulations.

3: **Responsibility** – It is the responsibility of the DNFBP to adopt a written Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) policy and to establish processes which ensure that the DNFBP is in compliance with the requirements of the MLPCA.

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

3.1.1 Comply with the regulations, directives of the FIU and the MLPCA. The DNFBP should ensure that FIU policies and all relevant laws 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;

3.1.2 Where appropriate, appoint a compliance officer to be responsible for ensuring the DNFBP's compliance with the requirements of the MLPCA or the DNFBP himself/herself must ensure compliance individually;

3.1.3 Establish an audit function to test its anti-money laundering procedures and systems;

3.1.4 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;

3.1.5 Implement effective procedures for customer identification, record keeping, transaction monitoring and reporting suspicious transactions;

3.1.6 Screen potential employees to ensure that employees are fit and proper;

3.1.7 Ensure that its officers and employees are:

a.) aware of the laws relating to money laundering and financing of terrorism; and

b.) aware of the procedures and policies for compliance with anti-money laundering standards

c.) trained to recognize suspicious transactions.

3.1.8 The FIU will conduct compliance audits of DNFBPs to assess compliance with the MLPCA and these regulations.

4: **Interpretation** -- 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.

4.1 If a provision in these Regulations refers to a communication, notice, agreement of 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.

4.2 A DNFBP may seek guidance from the FIU where clarity is needed to interpret and/or apply any part of these Regulations.

4.3 These Regulations are regulatory requirements only that relate to the activities of DNFBPs under the supervision of the FIU and cannot be relied upon to interpret or determine the application of the criminal laws of the Republic of Palau.

PART III: IMPLEMENTATION AND SPECIFIC REQUIREMENTS

1: **Adoption of Implementation of Internal Procedures, Policies and Controls** -- A DNFBP shall establish, implement, monitor, and maintain, an effective program of compliance with these Regulations.

1.1 A DNFBP shall put in place relevant policies, procedures, processes and controls designed to prevent and detect potential Money Laundering and Terrorist Financing activity.

1.1.1 Such measures should consider the following:

a.) Compliance Management Arrangements;

b.) Risk Assessment and Management;

c.) Customer Due Diligence;

d.) Record retention;

e.) Training and awareness;

f.) Employee screening;

g.) Detection of unusual and/or suspicious transactions; and

h.) Monitoring and Reporting obligations.

1.2 In the case of any DNFBP consisting of five (5) or more persons including staff and management, including, but not limited to, partnerships, limited liability companies, professional organizations, corporations and any other business form other than sole proprietorships shall appoint a Money Laundering Reporting Officer (MLRO) at a management level who will be

responsible for the day-to-day oversight of relevant policies, procedures, processes and controls to prevent and detect Money Laundering and Terrorist Financing. Any DNFBP with less than five (5) persons, the owner and/or senior management of the DNFBP business shall be responsible for compliance with these regulations.

1.3 A DNFBP shall ensure that relevant policies, procedures, processes and controls are communicated to all relevant employees.

1.4 A DNFBP shall establish ongoing employee training to ensure that employees are kept informed of new developments, including information on current anti Money Laundering and anti Terrorist Financing risks, techniques, methods and trends.

1.5 A DNFBP shall put in place independent controls that will test and assess the effectiveness of the program of compliance with these Regulations on a *Risk-Based* basis with a defined minimum frequency.

1.6 A DNFBP shall put in place appropriate screening procedures to ensure high ethical standards when hiring employees.

1.7 A DNFBP shall have relevant policies, procedures, processes and controls in place to prevent the misuse of technological development in Money Laundering or Terrorist Financing schemes.

2: **Compliance Management Arrangements** -- A DNFBP shall ensure that a program of compliance with these Regulations is executed and managed appropriately.

2.1 A DNFBP, as qualified hereinabove, shall appoint an MLRO who shall have responsibility for establishing and maintaining policies, procedures, processes and controls with AML/CFT legislation and regulation and exercising day-to-day operational oversight of the DNFBP's compliance with AML/CFT policies, procedures, processes and controls.

2.2 The MLRO's responsibilities shall also include identifying and taking appropriate action on matters of Money Laundering or Terrorist Financing concerns that are identified as part of the risk assessment process or by the competent authorities listed in MLPCA.

2.3 The MLRO shall be responsible for establishing, implementing, monitoring, and maintaining an appropriate ongoing program of AML /CFT training and awareness and making annual reports to senior management concerning the level of compliance adherence to policies, procedures, processes and controls.

2.4 The MLRO shall be responsible for receiving internal suspicious activity reports submitted by employees of the DNFBP, investigating the internal suspicious activity report and taking appropriate action that includes, where appropriate, making external suspicious transaction reports to the FIU.

2.5 The MLRO will be responsible for acting as the point of contact in the FIU, the regulatory authorities, and relevant agencies concerned with AML/CFT matters and responding

promptly to any request for information made by regulatory authorities or other *Competent Authorities* of the Republic of Palau including the Bureau of Public Safety, FIU, FIC, the Narcotics Enforcement Agency, and the Terrorist Coordinator/Minister of Justice.

2.6 The MLRO will notify FIU promptly regarding any communication from other authorities or regulators concerning Money Laundering or Terrorist Financing matters.

2.7 A DNFBP shall make appropriate provisions for any absence of the MLRO and shall appoint a suitable deputy to assume the responsibilities set out above.

2.8 The MLRO should be sufficiently senior and independent to act on his/her own authority, have direct access to senior management, and have sufficient resources including appropriately trained and effective employees.

2.9 The MLRO shall have access to relevant information concerning the DNFBP's clients, representatives of the clients, business relationships and transactions and the details of such transactions which a DNFBP enters into, or considers entering into, with or for a client or other party.

2.10 A DNFBP shall commission an annual report from its MLRO which will report the level of compliance adherence to relevant policies, procedures, processes and controls with respect to regulatory obligations.

3: **Risk Assessment and Management:** A DNFBP shall adequately assess its *Money Laundering and/or Financing of Terrorism* (ML/FT) risk in relation to its clients, its business, products and services, and appropriately define and document its *Risk-Based Approach.*

3.1 A DNFBP shall have appropriate risk management systems to determine whether a potential client, client or beneficial owner is a *Politically Exposed Persons ("PEP")* defined in section 3301(q) of the Act.

3.2 A DNFBP shall maintain *Anti-Money Laundering and Counter Financing Terrorism* (AML/CFT) policies, procedures, processes and controls that are relevant and up-to-date in line with the dynamic risk associated with its business, products and services and that of its clients.

3.3 A DNFBP shall establish, implement, monitor, and maintain satisfactory controls that are commensurate with the level of ML/FT risk.

3.4 Should a DNFBP consider a more stringent application of systems and controls be applied to its business than is otherwise directed within these Regulations, the DNFBP should not be restricted in such application provided that these Regulations are also implemented as a minimum standard.

4: **Know Your Customers and Customer Due Diligence:** A DNFBP shall properly identify its clients, and maintain client identification records of reliable documentation. Such client

identification records shall be made available to the FIU or to any Competent Authority promptly upon request.

4.1 A DNFBP shall apply a minimum standard of *Customer Due Diligence* (CDD) to all business relationships, and shall adopt a risk-based approach to determine the extent of additional CDD measures commensurate with the level of risk posed by the client type, business relationship, transaction or product.

4.2 DNFBP shall always conduct the minimum level of CDD, unless a specific exemption is applicable. Any risk-based measures considered and implemented shall be consistent with the Regulations and guidance.

4.3 A DNFBP shall not conduct reduced CDD measures where there is a suspicion of Money Laundering or Terrorist Financing activity, or where high-risk circumstances are identified.

4.4 *Timing:* A DNFBP shall undertake satisfactory CDD measures when:

4.4.1 Establishing a business relationship;

4.4.2 Carrying out:

a.) occasional transactions the value of which singularly or in several operations that appear to be linked, equal or exceed $10,000.00;

b.) occasional transactions that are wire transfers, and each equaling or exceeding US$10,000.00 ;

c.) there is any suspicion of Money Laundering or Terrorist Financing; or

d.) the DNFBP has doubts about the integrity or adequacy of previously obtained client identification data.

4.5 A DNFBP should verify the identity of each client and beneficial owner when establishing a business relationship or conducting transactions for occasional clients.

4.6 *Application:* A DNFBP shall implement the following standards or CDD measures:

4.6.1 Identify and verify the identity of a Client that is a natural person, using relevant and reliable independent source documents, data or information ("Identification Data");

4.6.2 If the client is not a natural person the DNFBP shall:

a.). Identify and verify the name, address and legal status of the client by obtaining proof of incorporation issued by the relevant authority, or similar formal evidence of establishment and existence; any person purporting to

act on behalf of the client; directors and controllers; provisions regulating the power to bind the legal entity or arrangement; and

b.) Verify that any person purporting to act on behalf of the client is authorized to do so, and that such person's identity is properly verified; and

c.) Identify the beneficial owner, taking reasonable measures to verify the identity of the beneficial owner using identification data obtained such that the DNFBP is satisfied that it knows who the beneficial owner is;

d.) Understand the ownership and control structure of the client; and

e.) identify the natural persons that ultimately own and control the client.

f.) Establish and record the purpose and intended nature of the business relationship; and

g.) Conduct ongoing due diligence on the business relationship and apply scrutiny to transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the DNFBP's knowledge of the particular clients, their business and risk profile, including, where necessary, the source of funds.

4.6.3 A DNFBP shall ensure that identification data is kept up-to-date and relevant and shall review the records of higher risk customers or business relationships as appropriate.

4.6.4 Where a DNFBP is unable to comply with any of the CDD measures, it shall not open an account, commence business relations, accept instructions or perform the transaction.

4.7.5 Where CDD obligations for existing business relationships and clients are not met, as a result of the client's refusal to comply or causing unacceptable delays, the DNFBP shall terminate the business relationship, and consider making a Suspicious Transactions Report (STR) to the FIU.

4.6 These CDD measures shall apply to all of a DNFBP's new clients. A DNFBP shall apply relevant CDD measures to existing clients at least when:

a.) Receiving or disbursing funds on behalf of a client in a transaction that singularly, or in several transactions that appear to be linked, equal or exceed $10,000.00; or

b.) the client's documentation standards are changed substantially with the introduction of compliance requirements with these Regulations; or

c.) there is a material change in the nature of the relationship with the client; or

d.) there are anonymous accounts, accounts in fictitious names or numbered accounts identified; or

e.) the DNFBP becomes aware that it lacks sufficient information about an existing client, or is concerned of the accuracy of information recorded; or

f.) where a STR has been reported, or a subpoena or production order has been received, or where relevant negative information is known.

5: Enhanced Due Diligence ("EDD") -- A DNFBP shall perform enhanced due diligence (EDD) for higher risk categories of customer, business relationship or transaction.

5.1 A DNFBP shall ensure it is aware of new or developing technologies that might favor anonymity and take measures to prevent their use for the purpose of Money Laundering or Terrorist Financing.

5.2 A DNFBP shall apply at a minimum enhanced due diligence in the following circumstances:

5.2.1 *Deficient Regime and Subjects of Concern.* In assessing the risks in relation to Money Laundering or Terrorist Financing, a DNFBP shall give special attention to business relationships established and transactions intended or conducted with persons and entities from or in countries that do not apply, or insufficiently apply, AML/CFT rules, as identified by

a.) the Government of the Republic of Palau;

b.) the Financial Intelligence Unit;

c.) the Asia Pacific Group on Money Laundering (APG); and

d.) the Financial Actions Task Force (FATF);

5.3 A DNFBP shall apply systems and controls that can appropriately identify and manage the enhanced risk associated with clients or transactions in or from politically unstable countries and those that are prone to corruption.

5.4 A DNFBP shall make appropriate use of relevant findings issued by any of the above authorities concerning any named individuals, groups or entities that are the subject of money laundering or terrorist financing concern.

5.5 *Non Face-To-Face Business*: When conducting "non-face-to-face" business with clients that have not been physically present for the purposes of identification and verification, the DNFBP must have policies, procedures, systems and controls in place to manage specific risks associated with such "non-face to face" business, relationships or transactions.

5.5.1 A DNFBP shall at a minimum require two pieces of formal identification that have been certified appropriately and one formal document that will verify the physical address of the client. Where the client is a legal person, a DNFBP shall require documentary evidence of the existence of the legal person and a certified copy of acceptable identification and address documentation to verify the address of any person.

5.5.2 When conducting "non-face-to-face" business, a DNFBP shall require at a minimum that the first payment received from the non face-to-face client is carried out through an account in the client's name with a financial institution which is subject to internationally recognized due diligence standards.

5.5.3 A DNFBP shall ensure that adequate procedures for monitoring activity of "non-face to face" business are implemented and managed effectively.

5.6 A DNFBP shall record in writing the approval of its senior management to enter into a business relationship with a PEP.

5.6.1 If an existing client or beneficial owner of an existing client of a DNFBP is subsequently found to be, or becomes, a PEP, the senior management of that DNFBP must record in writing its approval to continue the business relationship or resolve its termination.

5.7 When dealing with a client that is a PEP or which has a PEP as its beneficial owner, a DNFBP shall:

a.) clearly establish the source of wealth and source of funds of each; and

b.) conduct on-going and intensified monitoring of the client and business relationship.

6: <u>Prohibited Activities</u> -- A DNFBP shall not do the following:

6.1 A DNFBP shall not create, operate, manage, or facilitate activity for or on behalf of a Shell Bank (defined as a financial institution that does not have a physical presence in the jurisdiction) or Shell Company (defined as an inactive company without business operations and/or significant assets that is used as a vehicle for financial maneuvers or kept dormant for future use in some other capacity);

6.2 A DNFBP shall not keep anonymous accounts or accounts in fictitious names; and

6.3 A DNFBP is prohibited from participating in any manner, in any form of gaming activity unless licensed to do so by an appropriate government agency.

7: **Reliance And Outsourcing** A DNFBP may outsource the technical aspects of CDD process only to qualified service providers duly regulated and supervised in the country where they are based and incorporated, as long as such outsourcing allows for:

7.1 The DNFBP to promptly obtain from the CDD service provider the information under Article 7; and

7.2 The DNFBP ability to obtain copies of identification data and other relevant documentation relating to CDD requirements promptly upon request.

7.3 The DNFBP shall have ultimate responsibility for client identification and verification, and any other service provider.

7.4 A DNFBP shall ensure that there are no secrecy or data protection issues that would restrict prompt access to data, or impede the full application of these Regulations with respect to any outsourced relationship.

PART IV: REPORTING REQUIREMENTS

1: **Suspicious Activity Reporting And Monitoring --** A DNFBP shall have relevant policies, procedures, processes and controls in place for the purposes of detecting Money Laundering and Terrorist Financing and to enable it to report any suspicion or knowledge of suspected Money Laundering or Terrorist Financing activity.

1.1 If a DNFBP suspects or has reasonable grounds to suspect that funds concerning an actual or proposed transaction are the proceeds of any criminal activity, or are related to Money Laundering or Terrorist Financing activity, the DNFBP shall promptly file a written STR with the FIU.

1.1.1 A DNFBP shall routinely monitor for and detect suspicious activity, and shall, at a minimum, examine the background and purpose of the following:

a.) Complex or unusually large transactions, which have no apparent visible economic or lawful purpose.

b.) Funds received from or disbursed on behalf of the DNFBP clients the value of which singularly, or in several operations that appear to be linked, equal or exceed US$100,000.00.

c.) Transactions outside the usual pattern of the client's activity as known to the DNFBP.

d.) Transactions that are deemed to be of high risk with regard to a client or business relationship, or as they relate to high risk geography, products or services.

e.) Transactions, clients, or business relationships that cause the DNFBP to have reasonable grounds to suspect ML or TF.

1.2 Every employee of a DNFBP shall be made aware of his/her role in reporting internal suspicious activity reports.

1.3 Every employee of a DNFBP shall be informed and fully aware of their duty to submit internal suspicious activity reports.

1.4 The MLRO shall record the steps that are taken with regard to investigating an internal report and the decision on whether or not to make an external STR. Where appropriate the MLRO shall make the STR to the FIU.

1.5 The background and purpose of the activity in question shall, as far as possible, be examined by the MLRO and the findings shall be established in writing.

1.6 Where the MLRO decides that no external report should be made, the reason why shall be recorded.

1.7 A DNFBP shall institute disciplinary measures against any employee that fails to make an internal suspicious activity report where there are grounds for him/her to do so.

2: **Prohibition To Disclose Reporting** -- DNFBPs, their directors, officers and employees (permanent and temporary) shall not disclose to the subject or any person other than one with a legitimate right or need to know, and only in accordance to the direction provided by FIU's Regulations and guidance on these Regulations, the fact that a STR or related information has been or will be reported or provided to the FIU.

3: **Reporting Indemnity** -- A DNFBP, its directors, officers and employees (permanent and temporary) shall be protected from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. Such immunity operates even if the person filing the report does not know precisely what the underlying criminal activity is, and regardless of whether an illegal activity has actually occurred.

3.1 The names and personal details of the DNFBP, its directors, officers and employees filing an STR shall be maintained in strict confidence by the receiving authorities.

4: **Lawyer Exception (Judicial Proceedings) and American Bar Association Rules** – Lawyers and independent legal professionals have no obligation to report information required to be reported under the Act and these Regulations that they receive or obtain from a client in the course of developing a legal position for a client, or performing the task of defending a client or representing a client in, or concerning a judicial proceeding, including rendering advice on how to avoid such judicial proceedings, regardless of whether such information is received or obtained before, during, or after such judicial proceeding. The reporting required of lawyers and other legal professionals required under the Act and these Regulations is hereby deemed to be in accordance with the American Bar Association Rules of Professional Conduct No. 1.6(b)(2) and (3) as a

permissible disclosure to prevent, mitigate, rectify a crime, fraud, or substantial injury to the financial interests or property of another that is reasonably certain to occur, or that has occurred, and in furtherance of which the lawyer's legal services have been utilized by the client.

5: Staff Awareness And Training -- A DNFBP shall establish on-going and up-to-date relevant AML/CFT employee training that appropriately covers their obligations under the laws, regulations, policy procedures, processes and controls.

5.1 A DNFBP shall establish measures to ensure that employees are kept informed of up-to-date risk vulnerabilities, including information on current AML/CFT techniques, methods and trends.

5.2. A DNFBP shall ensure that training is sufficiently tailored in its content and frequency to the operations and business of the DNFBP, its employees, and its clients.

5.3 DNFBP shall keep employees informed on an ongoing basis of the type of suspicious activity that is pertinent to the type of business of the DNFBP and to the context of the employees function.

5.4 Except in respect of senior managers and MLROs whose training must be provided immediately on assumption of their duties, a DNFBP shall ensure that all relevant employees receive appropriate training within 60 days of commencement of employment.

6: Record Keeping -- A DNFBP shall maintain all records on any transaction for at least six (6) years following the completion of the transaction, regardless of whether the account or business relationship is ongoing or has been terminated.

6.1 The transaction records kept in accordance these regulations must be sufficient to permit reconstruction of individual transactions,

6.1.1 The Transaction Records, at a minimum, must include the following:

a.) client's name and physical address;

b.) beneficiary's name and physical address;

c.) nature and date of transactions;

d.) type and amount of currency involved; and

e.) type and identifying number of any account involved in the transaction.

6.2 Where maintenance of client records is outsourced to qualified service providers in accordance these Regulations, DNFBPs shall take reasonable steps to ensure that such records are held in a manner that conforms to these Regulations.

6.3 A DNFBP shall maintain information, correspondence and documentation for client identification and verification, and associated due diligence for a period of at least six (6) years from the end of the business relationship with the client or the last transaction conducted.

6.4 A DNFBP shall maintain records concerning the internal reporting of unusual or suspicious transactions and all records of investigations of those reports together with the decision made shall be retained for a period of six (6) years after the report has been made, or as otherwise directed by the FIU.

6.5 A DNFBP shall maintain records of the dates of training sessions, a description of training provided and names of the employees that received training for a period of at least 6 years from the date on which training was received.

6.6 A DNFBP shall maintain records of the annual report, and any other reports that highlight the level of compliance, deficiencies and actions, that it submits to senior management.

6.7 The transaction records and other identification data shall be made available to the FIU or any other Competent Authority, immediately upon request.

7: Regulatory Cooperation -- In order to ensure that the all reports contemplated by these Regulations and the law are submitted in accordance with the law, all DNFBPs shall submit to inspection by the FIU to determine compliance with these Regulations.

7.1.1 It is not a reasonable excuse for a DNFBP to refuse or fail a request to:

a.) permit inspection and copying of any information or document;

b.) give or produce, or procure the giving or production of, any information or document; or

c.) answer questions regarding a reported and/or unreported transaction.

8: Attorney Reporting Requirements -- Where the FIU or Competent Authority requires a Professional Legal Advisor to give information or to produce a document or to answer a question, and the giving of the information or the production of the document or the answer to the question would involve disclosing a Privileged Communication made by, on behalf of, or to, the Professional Legal Advisor in his capacity as a Professional Legal Advisor, the Professional Legal Advisor is entitled to refuse to comply with the requirement unless:

8.1 The person to whom, or by, or on behalf of whom, the communication was made is a body corporate that is under official management or is being wound up, and the official manager or liquidator of the body as the case may be consents to the lawyer complying with the requirement; or b. otherwise, the person to whom, or by, or on behalf of whom, the communication was made consents to the Professional Legal Advisor complying with the requirement.

8.2. If a Professional Legal Advisor so refuses to comply with a requirement, he/she shall, as soon as practicable, give to the FIU a written notice setting out:

8.2.1 where the Professional Legal Advisor knows the name and address of the person to whom, or by whom, or on behalf of whom, the communication was made, then that name and address; and where the requirement to give information or produce a document relates to a communication which was made in writing, then sufficient particulars to identify the document containing the communication.

PART V: CORRECTIVE MEASURES AND FINES

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.

1.1 Irrespective of the criminal liability or sanctions applicable under the Act, where the Regulatory Authority considers that a DNFBP, its directors, officers or employees (permanent or temporary) has committed a contravention of any provision referred to in these Regulations, the FIU can impose appropriate enforcement and sanctions including unlimited fines on the DNFBP, its directors, senior managers, officers or employees.

1.2 The DNFBP shall agree with the steps towards rectifying any deficiencies that the FIU identifies, or are brought to the attention of the FIU, in an appropriate manner and timeframe.

1.3 The FIU shall provide within its Rulebook appropriate guidance on the formal process for the imposition of any fines and/or penalties for violations of these Regulations. .

PART VI: EFFECTIVE DATE

1: **Effective date** – The effective date of this regulation shall be upon approval and signing by the President of the Republic of Palau or as otherwise prescribed by law.

Adopted December 21, 2021

Governing Board
Financial Institutions Commission
Republic of Palau

Approved March 11, 2022

His Excellency Surangel Whipps, 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 ***(Complete all parts that apply)***	

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 c.__ Alien Registration
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 c.__ Alien Registration
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)

_____ _____

_____ _____

_____ _____

<table>
<tr><td colspan="5">Part III. Reporting Financial Institution</td><td></td></tr>
<tr><td colspan="5">Name of Financial Institution</td><td>EIN or TIN</td></tr>
<tr><td colspan="5">Address</td><td>Routing Number</td></tr>
<tr><td colspan="3">City, State</td><td>Country</td><td>Zip Code</td><td>Date of Signature
_____/_____/_____
MM/ DD/YYYY</td></tr>
<tr><td rowspan="2">Sign Here →</td><td>Title of Approving Official</td><td colspan="2">Signature of Approving Official</td><td></td><td>Telephone Number</td></tr>
<tr><td>Preparer's Name and Title</td><td colspan="4">Person to Contact</td></tr>
</table>

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?		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

If Yes, specify: c ☐ Still employed at financial institution e ☐ Terminated
d ☐ Suspended f ☐ Resigned

Date of Suspension, Termination, Resignation
MM DD YYYY

Part III Suspicious Transaction Information

2

Date or date range of suspicious transaction
From ___ ___ ___ To ___ ___ ___
MM DD YYYY MM DD YYYY

Total dollar amount involved in known or suspicious transaction
$ .00

Summary characterization of suspicious transaction:

a	☐	Money Laundering and Proceeds of Crime Act	f	☐	Computer Intrusion	l	☐ Debit Card Fraud
			g	☐	Consumer Loan Fraud	m	☐ Defalcation/Embezzlement
b	☐	Bribery/Gratuity	h	☐	Counterfeit Check	n	☐ False Statement
c	☐	Check Fraud	i	☐	Counterfeit Credit/Debit Card	o	☐ Misuse of Position or Self Dealing
d	☐	Check Kiting	j	☐	Counterfeit Instrument (other)	p	☐ Mortgage Loan Fraud
e	☐	Commercial Loan Fraud	k	☐	Credit Card Fraud	q	☐ Mysterious Disappearance
						r	☐ Wire Transfer Fraud
						t	☐ Terrorist Financing
s	☐	Other				u	☐ Identity Theft

_____
(type of transaction)

Amount of loss prior to recovery (if applicable)
$ .00

Dollar amount of recovery (if applicable)
$ .00

Has the suspicious activity had a material impact on, or otherwise affected the financial soundness of the institution?
a ☐ Yes b ☐ No

Has the institution's bonding company been notified?
a ☐ Yes b ☐ No

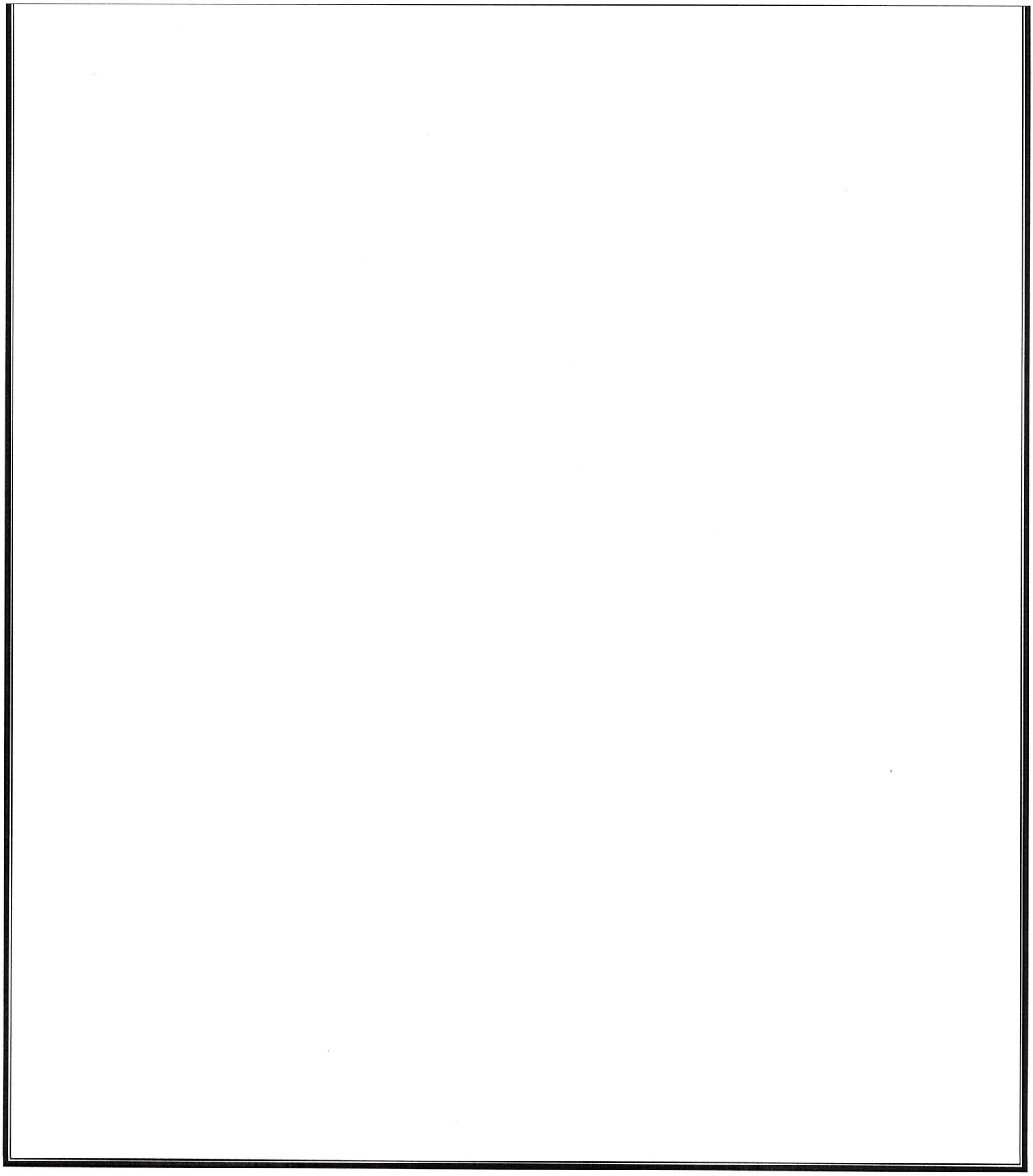
Part IV Contact for Assistance

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 insists on doing business on a significant cash basis.
- Customers who do not identify the true beneficiary of a business transaction.
- Customers that do not identify the beneficial owner(s) of a legal person or insist that such person, natural or otherwise, are not clearly or otherwise identified in public documents.
- Customers that purport to have undeclared or unidentified business partners.
- Customers who do not want to be identified in underlying transaction documents.
- Customers that engage you to deposit funds on their behalf prior to establishing legal business status in the Republic.
- 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 ($100,000 or more).
- Customers who have active accounts with several financial institutions within the same locality, particularly when the DNFBP 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 means to conduct large cash transactions or foreign exchange transactions.
- Company representatives who avoid contact with DNFBP staff when doing business with the DNFBP or making business transactions.
- Customers that request the DNFBP to assist them in substantial deposits of cash or negotiable instruments in an amount equal to or greater than $100,000 to the DNFBP client trust account or any account maintained by the DNFBP or otherwise attempting to use 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 DNFBP.
- 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 DNFBP staff when conducting business with the DNFBP 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 financial institution staff or when the customer requests the DNFBP and/or its staff to conduct banking activity on his/her/its behalf.

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.