Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism Procedures for Reporting Entities in Seychelles

The Financial Intelligence Unit

June 2015 update

Table of Contents

1. Introduction

These guidelines are issued by the Seychelles Financial Intelligence Unit (FIU) under the Anti-Money Laundering Act, 2006 as amended by the Anti-Money Laundering (Amendment) Acts, 2008 and 2011 (the AML Act). They provide updated general guidance on applying the laws which have been enacted in Seychelles to comply with international standards for Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) procedures.

The guidelines focus on the AML Act and the Regulations made thereunder, and on the obligations of 'reporting entities' as defined in the AML Act. Reference is also made to the Prevention of Terrorism Act, 2004 (the Prevention of Terrorism Act) and to other Acts which impose significant obligations in relation to AML/CFT procedures.

These guidelines take account of the law of Seychelles and the Recommendations of the international Financial Action Task Force (FATF) as at 1 December 2014. They do not however purport to be a comprehensive summary of the AML Act, the Prevention of Terrorism Act, or any other relevant legislation. Reporting entities and others should always refer directly to legislation when considering their statutory obligations.[1] Reporting entities are responsible for continuously monitoring developments in the law and, where applicable, keeping their own internal procedures effective and up to date.

1.1 The need to combat money laundering and terrorist financing

It is now universally recognised that failure by national authorities to participate in international efforts to prevent, detect and punish money laundering makes crime a viable proposition. Money laundering destabilises financial institutions, compromises the integrity of financial systems, distorts commerce, harms victims, and by distorting markets prejudices the rights and opportunities of ordinary citizens, for example in domestic land purchases.

Criminals will seek to make use of national and international financial systems to carry out and to benefit from the proceeds of their crime. Money launderers attempt to conceal the true origin and ownership of criminal proceeds by converting ('laundering') those proceeds into apparently legitimate assets. Financiers of terrorism may begin with legitimately sourced funds, but then misuse the financial system in a similar way as other criminal organisations to obscure both the source

[1] Consolidated unofficial versions of all legislation in force in Seychelles, including the AML Act (current to 1 December 2014), are freely available at www.seylii.org.

and destination of those funds. It is essential that criminals are prevented from enjoying the fruits of these criminal activities.

The Seychelles AML Act and Prevention of Terrorism Act were enacted to prevent, detect, and combat the use by criminals of financial and non-financial institutions for the purpose of the laundering of criminal proceeds or the financing of terrorist acts, activities or groups. The overriding principle is that reporting entities as defined in the AML Act should follow and apply the provisions of the law which reflect the FATF's international standards for the prevention and detection of money laundering and terrorist financing.

2. Money laundering

2.1 The offence of money laundering

Section 3 of the AML Act establishes the criminal offence of money laundering in Seychelles. The core offence provision is as follows:

> *3. (1) A person is guilty of money laundering if, knowing or believing that property is or represents the benefit from criminal conduct or being reckless as to whether the property is or represents such benefit, the person, without lawful authority or excuse (the proof of which shall lie on him) —*
>
> *(a) converts, transfers or handles the property, or removes it from the Republic;*
>
> *(b) conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or*
>
> *(c) acquires, possesses or uses the property.*

Money laundering is viewed as an extremely serious, extraditable, offence. Individuals are liable on conviction in Seychelles to a fine of up to R 5 million and/or 15 years in prison. Legal persons face a fine of up to R 10 million.

2.2 Who can be charged?

The offence of money laundering is committed by every person who participates in prohibited conduct, even where that participation is indirect (for example, counseling or concealment). All participants are liable to be tried and punished as principal offenders.

The concept of dealing with assets is itself widely defined. 'Handling' property, for example, includes assisting or arranging to assist in its retention, removal, disposal or realisation by or for the benefit of another person. Where a person knows, believes, or is reckless as to whether a particular asset is tainted, possessing it or concealing or disguising its possession by another is an offence in itself, even where the asset is not 'used' in any way.

2.3 Benefit from criminal conduct

"Criminal conduct" is defined for the purposes of the AML Act as any act or omission punishable in Seychelles or any other country by three or more years in prison and/or a fine exceeding R 50,000. Any offence of terrorist financing qualifies automatically. So does money laundering itself.

Money laundering is accordingly not restricted to particular kinds of criminal activity, but can arise in connection with all serious crime that yields proceeds, such as drug or people trafficking, corruption, fraud (including tax fraud), robbery or theft, forgery, smuggling, counterfeiting, and extortion.

It is not necessary to show that any person has been convicted of a predicate crime, nor is it necessary to specify a particular crime.

It is no defence that relevant criminal conduct was committed before the commencement of the AML Act, or outside Seychelles, as long as it is also a crime under the law of the country where it occurs. It is also no defence that criminal conduct was committed by someone else, as long as the person charged has the requisite knowledge/belief (see below).

Judges deciding whether particular property is the benefit from criminal conduct are directed to apply the civil standard of proof (balance of probability), and the burden of proof shifts to the defendant as soon as the Court is satisfied that the evidence supports a reasonable inference. Judges will have regard to the defendant's particular circumstances, including their financial resources and any explanation provided about their connection with the property.

2.4 Knowledge, belief, and recklessness

'Mens rea' or guilty knowledge covers all persons who know, believe, or are reckless as to whether property represents the benefits of criminal conduct. Recklessness is defined as disregarding a substantial risk that property is or represents the benefit from criminal conduct, and is

assessed in all the circumstances. Belief includes thinking that something is probably true.

Whenever it is objectively reasonable in the circumstances to conclude that a person had the required mental state, the burden of proof shifts to the defendant to raise a reasonable doubt. Actual knowledge does not have to be specifically proved.

Money laundering can be committed by body corporates. In those cases, it is sufficient to prove knowledge, belief, or recklessness by any director, officer, employee or agent acting in the course of his or her duty. The relevant individual may also be prosecuted personally. Auditors, accountants, and persons directing or controlling a body corporate are also vulnerable to prosecution if they assisted or consented to the offending.

It should be carefully noted that in circumstances where a suspicious transaction report (STR) is made to the FIU under s 10 of the AML Act, and the FIU does not issue a direction preventing the relevant service or transaction from proceeding, if that service or transaction does in fact constitute the crime of money laundering, the fact that an STR was made will not be a defence. Any participant with the required mens rea is vulnerable to prosecution.

3. Financing of terrorism

The objective of terrorist activity is to intimidate a population or compel a government to do something. This is done by intentionally killing, harming or endangering people, causing property or environmental damage, or by disrupting services, facilities, or systems.

The financing of terrorism is defined in s 2 of the AML Act by reference to the provisions of the Prevention of Terrorism Act. It covers a range of serious criminal offences (including certain acts committed outside Seychelles) by which a person, directly or indirectly, provides, collects or makes available funds, property, or a related financial service intending or knowing that they be used, or in the knowledge that they will be used in whole or in part, to facilitate the commission of a terrorist act or to benefit a person who is committing or facilitating the commission of a terrorist act.

There are two key differences between terrorist property and criminal property more generally:

- The sums needed to fund terrorist attacks are not always large (although terrorist organisations may require quite significant

assets to support their infrastructure), and the associated transactions are not necessarily complex.

- Terrorists can be funded from legitimately obtained income, including charitable donations, and it may be very difficult to identify the stage at which legitimate funds become terrorist property.

Terrorism may be state-sponsored, although this source of funding is believed to have declined in recent years.

Terrorist groups may resort to criminal acts such as kidnapping and extortion, which serve the dual purpose of providing needed financial resources while at the same time furthering the main terrorist objective of intimidating a target population. Terrorist groups may also resort to tobacco and fuel smuggling, fraud, theft, robbery, and drug trafficking to generate funds.

Terrorist groups also generate legitimately earned income. Groups collect subscriptions, sell publications, organise cultural and social events, and make appeals to the community they purport to represent. Such fundraising initiatives may be carried out be in the name of charitable organisations and donors may genuinely understand they are funding a legitimate cause. Alternatively non-profit organisations or charitable organisations may be infiltrated so as to divert a portion of donations to terrorist activities.

3.1 Assessing the risk of terrorist financing

Sections 34 and 35 of the Prevention of Terrorism Act require all persons (not just reporting entities under the AML Act) to disclose to the Police any information that will assist in the prevention or detection of terrorist acts, including information about any property in his or her possession or control that is known to be owned or controlled by or on behalf of a terrorist group.

Due diligence and proper record keeping are essential to ensure as far as practicable that no reporting entity in Seychelles is used to facilitate the financing of terrorism. In conducting a risk assessment of their business, reporting entities must consider any vulnerabilities arising from the nature of their products or services which could be exploited for this purpose. Controls should be designed, documented, and implemented to seek to mitigate such risks.

It is important to note that a risk-based approach to the financing of terrorism may differ substantially from the approach required to detect

potential money laundering. This is because, as noted above, activity by or on behalf of terrorists may involve legitimately sourced funds, may be carried out on a small or intermittent scale, and may involve the kinds of overt and outwardly innocent transactions that are generally considered low-risk with regard to money laundering.

Ongoing monitoring of transactions and scrutiny of the source of wealth or funds for those transactions are key to identifying patterns of activity that could indicate the financing of terrorism. The screening of customers and potential customers against relevant international financial sanctions list is also essential.

Reporting entities should pay particular attention to their responsibilities under s 8 of the AML Act (discussed in section 5.8 of these guidelines) regarding the provision and retention of accurate and detailed information in respect of electronic funds transfers. Similar provisions are found almost universally in modern financial systems. They were developed with the objectives of preventing terrorists in particular, but also other criminals, from having unfettered access to wire transfers for moving their funds and of detecting such misuse when it does occur.

As discussed later in these guidelines, reporting entities must be in a position to immediately comply with any relevant information requests from the FIU or other law enforcement agencies.

4. Reporting entities and the FIU

While any person may commit the offence of money laundering, and any person may provide assistance to law enforcement authorities in preventing or detecting that offence, the focus of the AML Act is on 'reporting entities'. These entities have been identified by profession/occupation as playing a critical role in the prevention and detection of money laundering and associated criminal conduct. It is essential that all reporting entities understand their special status under the AML Act and the responsibilities that accompany this status.

The core obligations of reporting entities relate to verification of customer identity ('Know Your Customer' or KYC), risk-based monitoring of transactions and relationships through ongoing due diligence, record-keeping and compliance protocols, and the identification and reporting to the FIU of suspicious transactions or proposed transactions. These obligations are discussed in detail in the next section of these guidelines.

4.1 Who is a reporting entity?

Reporting entities are defined in the Second Schedule to the AML Act. There are two broad categories of reporting entity.

The first category (Part 1) includes all persons carrying on a business which requires a licence under specified Acts.[2]

This definition covers providers of international corporate services (including nominee directors and shareholders), international trustee and foundation services; banks and bureaux de change; insurance companies, managers, brokers, and agents; mutual funds and fund administrators; and securities exchanges and facilities, clearing agencies, securities dealers and investment advisors.

The second category (Part 2) covers specific professions and trades: accountants, legal professionals (in certain aspects of their practice), estate agents, high value dealers (engaged in trades of any goods worth at least R 200,000), and casinos.

The second category also covers all persons, including all entities supervised by the Central Bank, engaged in a very wide range of other business activities, such as money transmission services, lending and financial leasing, hire purchase and credit transactions, company and trustee services, currency changing and trading, and any form of managing funds or money on behalf of third parties.[3] This extended definition of reporting entity (in paragraph 7.1(g) of the Second Schedule) should be carefully studied by all persons engaging in business in Seychelles, particularly when the nature of their business changes or expands. Whether or not an activity is carried on by way of business is ultimately a question of judgement that takes account of several factors (none of which is likely to be conclusive). These include the degree of continuity, the existence of a commercial element, and the scale of the activity, both in absolute terms and relative to other activities carried on by the same person which are not regulated. The nature of the particular activity that is carried on will also be relevant to the factual analysis.

These guidelines concentrate on those institutions which tend to be most vulnerable to money laundering, and in particular on banks and CSPs. That should not be taken to imply any lesser responsibility for other

[2] The Financial Institutions Act, the International Corporate Service Providers Act, the Insurance Act, the Mutual Funds and Hedge Funds Act, and the Securities Act.

[3] Note that any person providing payment services as defined in the National Payment System Act, 2014 (including funds transfers and cash deposits) who chooses to act through an agent or third party must also provide a guarantee to the Central Bank that the agent or third party will comply with AML/CFT requirements (s 15(2) of that Act).

reporting entities, which may have to take different or additional steps to comply with their statutory obligations.

4.2 Role of the Financial Intelligence Unit

Part 3 of the AML Act establishes the Financial Intelligence Unit (FIU) as a specialised financial intelligence and assets recovery unit for Seychelles.[4] The FIU has extensively defined statutory objectives, functions, and powers, with core responsibilities including:

- monitoring, training, and enforcing compliance by reporting entities;
- investigating criminal conduct; and
- identifying, restraining, and recovering the proceeds of crime.

All reporting entities are accountable to the FIU for compliance with their AML/CFT obligations. Those obligations expressly override any duty of confidentiality or non-disclosure that might otherwise apply to the reporting entity (s 58 of the AML Act).

The FIU is responsible for receiving and acting on all suspicious transaction reports (STRs), discussed later in these guidelines. The FIU also has wide-ranging general powers to monitor reporting entities, including powers to inspect business premises and to issue statutory information requests, and can direct individual reporting entities to take any steps necessary to secure compliance with the AML Act.

The FIU is also expressly empowered to issue guidelines and prescribed forms, such as those in this document, and to provide training to reporting entities in relation to customer identification, record keeping and reporting obligations, and the identification of suspicious transactions.

5. Core obligations of reporting entities

The core AML obligations of reporting entities are set out in Part 2 of the AML Act and in the Anti-Money Laundering Regulations, 2012 (the AML Regulations).

[4] The provisions establishing the FIU cross-refer to the Proceeds of Crime (Civil Confiscation) Act, 2008 (the POC Act), which introduced special Court procedures for asset restraint and forfeiture.

These core obligations can be summarised as follows:

- To appoint an appropriately qualified and experienced compliance and reporting officer (CRO) with responsibility for AML compliance, and to establish and maintain procedures and systems (including an audit function and training programme) sufficient to ensure compliance (s 15); and
- To apply customer due diligence (CDD) measures, also known as 'Know Your Customer' (KYC) measures, using a risk-based approach, in respect of all customers, business relationships and transactions (s 4 and the AML Regulations);
- To conduct ongoing monitoring of business relationships, including paying special attention to complex, unusual or large transactions with no apparent economic/lawful purpose, and relationships and transactions with persons in high-risk jurisdictions (ss 4 and 9 and the AML Regulations);
- To stop acting and terminate any existing business relationship whenever unable to apply CDD or ongoing monitoring (s 5);
- To maintain records, including records of all prescribed CDD measures and all transactions and related correspondence, for at least seven years from the transaction or correspondence date or the end of the business relationship (s 6);
- To report suspicious transactions or attempted transactions to the FIU (ss 5 and 10); and
- To make disclosures required by the Prevention of Terrorism Act.

Failure to comply with these core obligations may result in compliance action by the FIU, disciplinary action by the relevant supervisory authority (for example, the FSA), and potentially in criminal prosecution for breach of the AML or Prevention of Terrorism Acts or complicity in money laundering.

It is important to appreciate that the AML Regulations (2012) reflect a risk-sensitive approach to due diligence and monitoring by reporting entities. This means that reporting entities are permitted to adopt different approaches to CDD and ongoing monitoring of customers according to the different risk ratings of those customers. A reporting entity may be allowed to apply 'simplified due diligence' in certain situations that are deemed to be low-risk for money laundering and financing of terrorism, and required to implement enhanced measures in situations that are deemed to be high-risk.

The ability of reporting entities to rely on exemptions or exceptions to CDD in particular cases does not detract from the ultimate responsibility of the reporting entity to identify and address the actual risks arising in the course of its business.

The ultimate risk run by non-compliant reporting entities is a charge of money laundering and/or terrorist financing (extremely serious criminal offences) for complicity in the criminal conduct of clients or customers. Full compliance with AML/CFT good practices removes that risk while preserving the integrity and reputation of the reporting entity.

5.1 Internal controls, policies, and procedures

Every reporting entity must take appropriate measures to ensure that all officers, employees, and agents engaged in dealing with customers or processing business transactions understand and comply with all applicable AML/CFT procedures.

Reporting entities who are individuals with no employees or associates do not have to appoint a separate compliance and reporting officer (CRO) to implement the procedures and systems set out in s 15(1) of the AML Act. That does not, however, excuse the individual from compliance with the core obligations of CDD, ongoing monitoring, record-keeping, and reporting suspicious transactions.

All other reporting entities must appoint a CRO with overall responsibility for AML/CFT compliance.

The CRO must be a senior officer who is sufficiently qualified and experienced to comply with the detailed requirements in s 15(1) of the Act, to act as the liaison point with the FIU and relevant supervisory authorities in Seychelles, and to command the necessary independence and authority to train and supervise all other officers, employees, and agents within the organisation.[5]

The CRO should at all times be resident in Seychelles. In addition, it is highly recommended that an alternate to the CRO is appointed to assume the prescribed responsibilities and duties in the CRO's absence. When several entities operate closely together within a group, a single CRO at group level may be designated.

[5] While the "necessary qualifications and experience" for a CRO are not specified in the AML Act and must be assessed on a case by case basis, reference may usefully be made to the concept of a "fit and proper" person in the CSP context, as explained in section 20 of the Code for International Corporate Service Providers issued by the FSA: http://www.fsaseychelles.sc/documents/ICSP%20Code.pdf.

The CRO's specific responsibilities include:

- establishing and maintaining a manual of compliance procedures;
- establishing an audit function to test AML/CFT procedures and systems;
- taking overall responsibility for all STRs; and
- ensuring that all officers, employees, and agents:
    - are screened by the CRO and other appropriate officers before recruitment;
    - are trained to recognise suspicious transactions and trends and particular risks associated with money laundering and financing of terrorism; and
    - comply with all relevant obligations under AML/CFT laws and with the internal compliance manual.

CROs and reporting entities should review their arrangements on a regular basis, both to verify compliance with internal procedures and to ensure that those procedures are updated in light of any amendments to the AML/CFT legislation.

These guidelines do not specify the nature, timing, or content of the training that must be provided within individual reporting entities: this is a matter that must be addressed by each CRO.

5.2 Customer due diligence

Customer due diligence (CDD), as defined in r 3 of the AML Regulations, has four key components:

(a) identifying customers, including any person acting on behalf of a non-individual customer, and verifying their identity;

(b) where the customer is not the beneficial owner, identifying the beneficial owner and taking reasonable measures to verify the beneficial owner's identity;

(c) obtaining enough information about the nature of the business relationship and the customer or beneficial owner's business to identify complex or unusual transactions or patterns of transactions and other high-risk activity; and

(d) taking reasonable measures to ascertain the purpose of one-off transactions (defined in r 5 as transactions outside an existing business relationship that exceed R 100,000 or R 50,000 in cash,

whether in a single or several linked operations), and the origin and ultimate destination of all funds transfers.

The first two requirements are concerned with the identity of the person who the reporting entity is dealing with; the second two requirements are focused on the nature and purpose of the service or transaction which the reporting entity is being asked to facilitate.

Note that the concept of 'beneficial owner' is now extensively defined in r 4 of the AML Regulations. This regulation should be carefully studied by all CROs.[6] It is critical to emphasise that the concept of beneficial ownership is not the same as legal ownership and cannot be determined by reference to the legal position alone. Beneficial ownership is a broader concept which focuses on real benefit and/or ultimate effective control.

The four core CDD obligations apply across the full range of business relationships and transactions that may be undertaken by reporting entities, and continue after a business relationship has been established.

5.3 Ongoing monitoring

The CDD obligations are supplemented by the general obligation of all reporting entities to conduct ongoing monitoring of all business relationships (r 9). Ongoing monitoring has two key components:

- Scrutinising transactions for consistency with the customer's business, risk profile, and source of funds/wealth; and
- Keeping all CDD information and documentation up to date.

The objective of the ongoing monitoring obligation is to identify activities of customers during the course of a business relationship which are not consistent with the reporting entity's knowledge of the customer, or the purpose and intended nature of the business relationship, and which need to be assessed for the possibility that the reporting entity may have grounds to report a suspicion of money laundering or terrorist financing. A reporting entity is accordingly obliged to monitor all dealings with a customer, to the extent reasonably warranted by the customer's risk profile, for consistency with the entity's knowledge of the customer and the customer's business and pattern of transactions.

[6] All CROs should also be familiar with the *Guidance on Transparency and Beneficial Ownership* issued by the FATF in October 2014, available from www.fatf-gafi.org.

When scrutinising the source of funds a reporting entity should seek to discover the origin and the means of transfer for funds that are directly involved in the transaction (for example, business activities, proceeds of sale, corporate dividends). When scrutinising the source of wealth a reporting entity should seek to discover the activities that have generated the total net worth of the customer (that is, the activities that produced the customer's funds and property).

Given the significant differences between reporting entities in Seychelles in terms of customer numbers and the nature and scale of activities entered into by those customers, how ongoing monitoring is undertaken will vary considerably in practice. Ongoing monitoring is nevertheless a specific statutory obligation placed on all reporting entities (regardless of their individual circumstances), and failure to develop or implement the required procedures may result in criminal prosecution.

Internalising the two key ongoing monitoring requirements is therefore fundamental to the proper discharge of CDD obligations, and should be a central focus of the CRO.

5.4 When must CDD measures be applied?

The default position (r 8 of the AML Regulations) is that CDD requirements are triggered whenever a reporting entity:

(a) establishes a business relationship;

(b) carries out a one-off transaction, outside an existing business relationship, that exceeds R 100,000 or R 50,000 in cash, whether in a single or several linked operations;

(c) has doubts about the veracity or adequacy of identification documentation; or

(d) reasonably suspects money laundering, terrorist financing, or other serious criminal conduct.

In the first two situations, the customer's identity and the nature of the relevant business or transaction must be verified before the business relationship is established or the transaction carried out. The only exception is for CDD conducted during the establishment of a business relationship, which is permissible in low-risk situations when necessary to avoid interruption to the normal conduct of business. In this case the CDD must still be completed as soon as practicable after the relationship is established (r 10). What constitutes an acceptable time for this process must be determined in the light of all the circumstances, including the nature of the business, the geographical location of the

parties, and whether it is practical to obtain all necessary documents before commitments are entered into or money changes hands.

Regulation 11 of the AML Regulations provides for 'simplified due diligence' in certain circumstances. This allows reporting entities to choose not to apply CDD in situations (a), (b), and/or (c) in respect of certain customers and transactions that are deemed to be low-risk: licensed banks in Seychelles and in FATF member countries; public bodies in Seychelles; publicly listed entities; and certain transactions involving personal pension schemes.

Simplified due diligence is not available in any situation raising an actual suspicion of money laundering, terrorist financing, or other criminal conduct.

Reporting entities are also required to apply CDD measures to existing customers "at appropriate times on risk-sensitive basis" (r 8(2)). This is an overarching, continuing requirement which applies to all customers, even those deemed to be low-risk. Reporting entities must ultimately be able to demonstrate to their supervisory authority (eg the FSA), and to the FIU, that their internal procedures for ongoing CDD are sufficient in light of the particular risks inherent in their business.

Once the identity of a particular customer has been verified and the nature of their business sufficiently understood, no further evidence of identity is needed unless the reporting entity has any reason for suspicion, for instance if there is a marked change in the nature or volume of business passing through the account. However, as set out below, the reporting entity must be able to identify the origin and ultimate destination of all funds transfers related to that customer.

There is no requirement to verify the identity of one-off customers for isolated transactions under the threshold of R 100,000 or R 50,000 in cash, unless the circumstances are suspicious.

All reporting entities should develop customer profiles based on CDD information obtained. A customer profile will facilitate the ongoing monitoring of accounts and transactions and assist the reporting entity to identify suspicious transactions or patterns of transactions. For banks and other financial institutions it is recommended that proof of sources of wealth and initial source of funds are identified at the outset of a customer relationship.

5.5 Enhanced due diligence

A number of situations are deemed by the AML Regulations to be sufficiently high-risk to trigger independent or additional CDD requirements. However, the ultimate responsibility for identifying high-risk situations, and responding to those risks through enhanced CDD and ongoing monitoring, rests with reporting entities (r 15(1)).

A clear example provided for in the Regulations is one-off transactions over the defined monetary threshold (R 100,000, or R 50,000 in cash), for which full CDD is required. That monetary threshold does not apply in existing business relationships. Reporting entities must however still be vigilant in monitoring their customers' transactions for suspicious activity.

Another clear high-risk situation is any business relationship or transaction involving a country which does not apply or fully apply the FATF Recommendations (r 15(2)). Updated lists of the relevant countries can be obtained from the FATF website.[7] All such relationships and transactions trigger both enhanced CDD and enhanced ongoing monitoring obligations (on a risk-sensitive basis). Reporting entities should have adequate systems in place to identify in advance the countries in which their customers will be operating or transacting and, if necessary, to obtain additional supporting documentation, such as contracts and invoices, to verify the purpose and commercial reality of a relationship or transaction.

5.5.1 Politically exposed person (PEP)

Enhanced CDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a customer, or any beneficial owner of a customer, is or becomes a politically exposed person (PEP). A 'customer' for this purpose includes any person entering a business relationship or undertaking a one-off transaction with the reporting entity.

A PEP is defined in r 6 of the AML Regulations as an individual entrusted with a prominent public function in the last three (3) years, and includes any immediate family member or close associate of such an individual. It is important to note that both local and foreign PEPs are covered by this definition.

All reporting entities should have a risk management system in place to determine if prospective clients and prospective or existing customers are PEPs. That determination is complicated by the fact that the definition of

[7] http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

a PEP includes family members and associates, who may have different names and may not publicise the fact of their association with the relevant individual. Reporting entities are allowed to rely on public information in determining whether persons are within the definition of 'close associates' (for example, partners or joint venturers), and should conduct regular searches and checks for this purpose.

Once a PEP has been identified, a business relationship can only be established with the approval of senior management, and the reporting entity must take adequate measures to establish the source of wealth and the source of funds involved in any proposed relationship or transaction.

5.5.2 Correspondent banking

Licensed banks in Seychelles may not enter into cross-border correspondent banking relationships without satisfying a number of additional controls set out in r 14 of the AML Regulations, including:

- fully understanding the nature of the business of the proposed correspondent bank or credit institution;
- being satisfied on reasonable grounds as to the reputation, quality of supervision, and AML/CFT financial controls of the proposed correspondent;
- documenting the responsibilities of the proposed correspondent in applying AML/CFT controls;
- being satisfied on reasonable grounds that CDD and ongoing monitoring measures are being properly applied to customers with direct access to any payable-through account held with the bank in the name of the proposed correspondent, and that CDD documentation is available to the bank on request; and
- obtaining approval of the Board of Directors.

High-risk 'shell banks' are defined in r 17 as banks or similar institutions that have no meaningful presence in their country of incorporation and are not subject to effective supervision by a foreign regulatory authority. Licensed banks in Seychelles are not permitted to enter into or continue correspondent banking relationships with shell banks, nor with banks that permit their accounts to be used by a shell bank.

5.6 Reliance on intermediaries for CDD

Regulation 12 of the AML Regulations allows some reporting entities to rely on intermediaries to apply CDD measures on their behalf, but only in tightly prescribed circumstances.

Reliance on intermediaries does not excuse reporting entities from their obligation to make CDD records available on request by the FIU and other regulatory bodies (s 6(3) and (5) of the AML Act and r 8(6) of the AML Regulations). Regulation 12(6) expressly provides that the ultimate responsibility for CDD remains with the reporting entity.

Banks, bureaux de change, and other lending and deposit institutions are not permitted to rely on intermediaries in any circumstances (r 12(4) of the AML Regulations).

Other reporting entities may choose to rely on another reporting entity (other than a bureau de change) in Seychelles, or on certain foreign entities which would be reporting entities if they carried on their business in Seychelles (including but not limited to corporate service providers, lawyers, and accountants/auditors), as long as the foreign entity is subject to regulatory supervision in a country which has enacted AML/CFT laws meeting FATF requirements. The reporting entity in Seychelles has to satisfy itself that any foreign third party it intends to rely on is a regulated entity, and obtain and maintain up-to-date proof of same.

The person relied on may apply CDD measures in respect of a reporting entity's customer, any beneficial owner of the customer, any third party for whom the customer is acting (or beneficial owner of that third party), and any person purporting to act on the customer's behalf.

Reliance for this purpose is only permissible where the person relied on has provided a written undertaking that it applies CDD on an ongoing basis, will keep records of CDD measures for at least seven years, and will make those records available to the reporting entity without delay on request or if it ceases to carry out business (r 12(2) of the AML Regulations). Where a person relied on does cease to carry on business, the reporting entity must immediately take possession of all relevant CDD records (r 12(5)).

A reporting entity that has branches or subsidiaries outside Seychelles must require those branches or subsidiaries to apply CDD, ongoing monitoring, and record-keeping measures that are at least as protective as those set out in the AML Regulations (r 16).

As stated above, r 12(6) expressly provides that where a reporting entity chooses to rely on a third party intermediary to apply CDD on its behalf, the ultimate responsibility remains with the reporting entity.

5.7 Good practice for identification / verification

The following summary outlines the minimum steps expected of reporting entities as good industry practice when establishing a business relationship or preparing for a significant one-off transaction, in order to comply with the core CDD obligations and provide a sufficient information base for ongoing monitoring (refer sections 5.2 and 5.3 above).

1. All identification and verification procedures, including both internal and external communications, should be documented in writing and preserved as records under the AML Act (refer section 5.9 below) for a minimum of seven years in a form enabling immediate compliance with any information request from the FIU.

2. The reporting entity should first establish to its satisfaction that it is dealing with a real person (natural or legal) and that any person purporting to act on behalf of a non-individual client or customer is properly authorised to act.

3. Whenever possible, and particularly in the case of a politically exposed person (PEP), the individual that the reporting entity is dealing with should be interviewed personally.

4. The reporting entity should take the necessary steps to identify the beneficial owner or owners of the assets which form the basis of the proposed relationship or transaction, and make appropriate inquiries into the purpose and nature of that relationship or transaction. This may require investigation of corporate ownership and control structures and sources of wealth and/or funds.

5. The reporting entity should then take appropriate steps to verify the identity of (a) the client/customer, (b), if different, the natural person with whom the entity is dealing, and (c), if different, the beneficial owner or owners. Those steps should include checking for alternative names / aliases (s 59 of the AML Act).

6. If the client/customer and/or any beneficial owner is a PEP, the reporting entity shall pay particular attention to the source of wealth and source of funds involved, and obtain prior approval from senior management for establishing a business relationship.

7. The best possible identification documents should be obtained from the prospective client/customer, including properly certified translations of any documents not in English. No single form of identification can be fully guaranteed as genuine or representing correct identity. The identification process will generally need to be cumulative. For practical purposes a person's residential address should be regarded as an essential part of his or her identity.

8. Documents issued by reputable government sources (e.g. identity cards and passports) should be required. Where practicable, copies of the supporting evidence should be retained. Alternatively, reference numbers and other relevant details should be fully recorded.

9. In respect of joint accounts where the surname and/or address of the account holders differ, the identity of all account holders, not only the first named, should normally be verified to ensure that the account is not opened or operated in any fictitious or incorrect name (s 7 of the AML Act).

10. Where a client or customer is introduced by a branch or subsidiary of a financial institution located outside Seychelles, provided the identity of the customer has been verified by the introducing branch or subsidiary in line with requirements at least equivalent to those of Seychelles and those identification records are freely and immediately available on request to the reporting entity in Seychelles, it is not necessary for identity to be verified or for the records to be duplicated.

11. Where a prospective client or customer is introduced by an independent intermediary, the reporting entity should determine whether it is entitled to rely on that intermediary to verify the identity of that client/customer on its behalf (r 12 of the AML Regulations) and if so, should establish to its satisfaction that all relevant records kept by the intermediary will be made immediately available to it on request, to enable the reporting entity to comply with its own AML obligations.

12. Where the reporting entity is not able to identify and verify the identity of the prospective client/customer and all relevant beneficial owners in accordance with the AML Regulations, the reporting entity should (a) not establish (or terminate) any business relationship, (b) decline to carry out any transaction, and (c) make an immediate STR to the FIU.

Where business relationships are already established, good industry practice for ongoing monitoring and continuing CDD in accordance with the AML Act requires at least the following steps.

1. The reporting entity should develop and maintain a risk profile for its own business, informed by local and international trends in money laundering and financing of terrorism, which is sufficiently detailed to enable it to identify appropriate areas of focus for transaction monitoring and continuing CDD.

2. Individual client/customer profiles maintained by the reporting entity should include sufficiently detailed information about the nature of the relevant business to enable the early detection of unusual transactions or patterns of transactions and other high-risk activity.

3. All documents, data and information relating to CDD for each client or customer, including alternative names or aliases, should be kept up to date, if necessary by requesting additional or better information from that client/customer or conducting independent inquiries, and regularly reviewed.

4. The reporting entity should have systems in place to ensure that (a) all complex, unusual or large transactions with no apparent economic/lawful purpose, (b) all transactions involving high-risk jurisdictions, and (c) all funds transfers that do not contain complete originator information, are promptly identified and adequately examined, with the findings recorded in writing (s 9 of the AML Act).

All reporting entities which do not operate solely as individuals (including, eg, partners in a law firm) should develop their own manual of compliance procedures, which may involve a number of checks additional to those set out above, and all reporting entities should regularly review their internal arrangements on a risk-sensitive basis. Internal procedures and systems adopted must remain consistent with these guidelines and with the provisions of the law.

5.8 Electronic funds transfers

Section 8 of the AML Act applies specifically to reporting entities which are licensed as financial institutions or money transmission service providers in Seychelles. When these entities provide electronic funds transfers for their customers, they are required to include accurate originator information and other related messages on the transfer and to ensure that the information remains with the transfer.

This obligation should be read together with the requirements of the National Payment System Act, 2014 (which came into effect in August 2014) and the Electronic Transactions Act, 2001.

Reporting entities should ensure that they obtain full name and address information from the ordering customer for all credit transfers made by electronic means, both domestic and international, regardless of the payment or message system used. To ensure that the SWIFT system is not used by criminals as a means to break the audit trail, when sending SWIFT MT 100 messages (customer transfers), reporting entities should complete the fields for both the ordering and beneficiary customers with their respective names and addresses.

Funds transfers where both the ordering and beneficiary customers are financial institutions acting on their own behalf are exempted from the s 8 obligation. In addition, when the transfer is the result of a credit or debit card transaction, it is not necessary to include or keep originator information as long as the credit or debit card number is included with the transfer.

Records of electronic payments and associated messages must be treated in the same way as any other transaction records and kept by the reporting entity in an accessible form for a minimum of seven years (refer section 5.9 below and s 16 of the National Payment System Act).

5.9 Record keeping

Section 6 of the AML Act requires every reporting entity to maintain records for potential use by the FIU and other agencies in the investigation and prosecution of offences related to money laundering or terrorist financing. This is a core obligation of reporting entities throughout the world and fundamental to the successful implementation of AML/CFT legislation. Failure to comply is regarded very seriously by the FIU and may result in regulatory and/or criminal sanctions.

The nature of the records that must be maintained reflects the customer due diligence and ongoing monitoring procedures outlined above, and the transactions and other business carried out by a particular reporting entity.

All records must be kept for a minimum period of seven (7) years from the date of the relevant event or, in the case of an ongoing business relationship, after the business relationship ceases, in a form which is immediately accessible upon request.

Records do not have to be kept in hard copy. It is recognised that reporting entities will find it necessary to rationalise their hard copy filing requirements. Most will have standard procedures which seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be by way of original documents, or by way of copies in any machine-readable or electronic form from which a paper copy can be readily produced (refer s 6(4) of the AML Act and s 4 of the Electronic Transactions Act, 2001).

Electronic records must however be kept in a form that enables appropriate authentication (s 6(4) of the AML Act). This requirement should be read in light of the provisions of s 3 of the Electronic Transactions Act, 2001 (which provides for the authentication of electronic records in Seychelles by digital signature or by the use of an asymmetric crypto system and hash function) and s 15 of the Evidence Act (which explains how documentary evidence from computer records are produced in Court).

5.9.1 Records of CDD procedures

The first category of records that must be maintained is records of all CDD measures applied in respect of the reporting entity's clients/customers. As explained in section 5.2 above, CDD relates to both identity and nature of business.

Every CDD step that is prescribed by the AML Act and Regulations must be reflected in records, including the safeguards required before relying on intermediaries. Without limiting the generality of that statement, whenever a person's identity has been verified, the records kept by or on behalf of the reporting entity should:

- indicate the nature of the evidence of identity obtained, and
- include either a copy of that evidence, or information sufficient to enable a copy to be obtained without delay.

5.9.2 Transaction and correspondence records

The second category of records that must be maintained is records of all transactions and related correspondence carried out by the reporting entity.

Regardless of the form in which the reporting entity chooses to keep them, transaction records must be sufficiently detailed to enable the transaction to be readily reconstructed at any time by the FIU or

Attorney General (s 6(1(b) and 6(3)(a) of the AML Act) and, if necessary, to be produced as evidence in criminal proceedings.

Without limiting the generality of that statement, transaction records must adequately identify the nature and date of the transaction, the type and amount of currency, the type and number of any account with the reporting entity, and the name and address of the reporting entity and the responsible officer, employee or agent. In the case of negotiable instruments other than currency, records must include particulars of the name of the drawer and the payee (if any), the institution on which it was drawn, the amount, date, and number (if any) of the instrument, and any endorsement details.

In the case of high-risk transactions (as defined in s 9(1) and (2) of the AML Act), records must also include the written findings produced by the reporting entity after examining the background and purpose of the transaction.

5.9.3 Records of FIU interactions

The third category of records which must be maintained is records of all AML/CFT enquiries received from the FIU and all reports made to the FIU under s 10 of the AML Act (including STRs and responses to information requests).

6. Identification procedures

The following section provides some more detailed practical guidance for applying CDD measures when opening customer accounts or establishing other business relationships. The suggestions which follow must be read in conjunction with section 5.7 above (Good practice for identification / verification) and with the minimum requirements prescribed by the AML Act and Regulations. They cannot be relied upon in isolation.

Particular precautions need to be taken by reporting entities in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-customers, the identification procedures set out in these guidelines should be followed.

The core obligation in verifying identity is to obtain proof of identity from a reliable and independent source (if possible) or, if not possible, from other sources that the reporting entity has reasonable grounds to believe can be relied upon (r 3(1)(a) of the AML Regulations).

6.1 Non-face-to-face situations

Any non-face-to-face transactions or contact between reporting entities and customers inevitably poses difficulties for customer identification. Reporting entities are nevertheless obliged to apply equally effective customer due diligence and ongoing monitoring procedures for non face-to-face customers.

Financial institutions in particular are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. An institution is obliged to put specific and adequate measures in place to mitigate this higher risk and to take particular care in supervising the account opening process. It may be inappropriate to accept photographic evidence of identity, for example, as there is a greater difficulty in matching the purported customer with the documentation supplied.

Examples of good practice measures for risk mitigation in the non face-to-face context include:

- requiring additional documents;
- requiring certification of documents presented by a notary, diplomatic official, or equivalent independent professional;
- independent contact with the customer;
- third party introduction, where consistent with the AML Regulations regarding reliance on intermediaries to conduct CDD on the reporting entity's behalf; and
- requiring an initial payment to be carried through an account in the customer's name with another bank subject to equivalent CDD requirements.

6.2 Confirmation of identity by other institutions

The obligation to verify identity using the best evidence and means available rests with the reporting entity opening the account or establishing the relationship. In cases where a reporting entity is not satisfied with the documentary evidence provided or with the results of public enquiries, it may need to approach another institution, on a non-competitive basis, specifically for the purpose of verifying identity. A standard format can be used for making such enquiries. It may be necessary to obtain the prior consent of the prospective client for disclosure of their information by the other financial institution.

6.3 Personal customers in Seychelles

The following minimum information should be obtained from prospective customers who are resident in Seychelles:

- true name and any other names used;
- correct permanent Seychelles residential address, and postal address if applicable;
- date of birth;
- occupation; and
- source of income and asset base.

Ideally the true name or names used should be verified by reference to a document obtained from a reputable official source which bears a photograph. A current valid full passport or national identity card, not older than 10 years, should be requested and the number registered.

In addition to name verification, it is important that the current permanent residential address is also verified. Some of the best means of verifying addresses are:

- requesting sight of a recent (not older than three months) utility bill, telephone bill, bank or other financial institution statement, or insurance policy which includes a residential address (to guard against forged or counterfeit documents care should be taken to check that the document is original);
- checking an official register such as the electoral roll;
- checking a current telephone directory; or
- receiving written confirmation from the person's landlord or employer.

An introduction from a respected customer personally known to the manager, or from a trusted member of staff, may assist the verification procedure but does not replace the need for address verification. Details of the introduction should be recorded on the customer's file.

There will be exceptional circumstances when Seychelles residents, particularly young persons, students, and the elderly, may not be able to provide appropriate documentary evidence of their identity, and/or where independent address verification is not possible. In such cases, confirmation of identity and address may be sought through family members or an educational institution in the first instance. Under

normal circumstances, for example, a minor will be introduced to a financial institution by a family member or guardian who has an existing relationship with the institution concerned. A manager in the branch may then authorise the opening of an account if satisfied with the circumstances (which should be recorded in the same manner as other identification records).

6.4 Non-resident personal customers

Persons who are not resident in Seychelles but who wish to open Seychelles bank accounts or establish other business relationships with reporting entities in the jurisdiction are subject to verification procedures similar to those for resident customers.

Address verification can pose difficulties. However, passports or national identity cards will always be available. It is impractical to set out detailed descriptions of the various identity documents that might constitute acceptable evidence of identity by foreign nationals. Reporting entities may wish to verify identity with a reputable credit or financial institution in the applicant's country of residence. Alternatively, a police character certificate from the applicant's country of residence may be sought.

For prospective non-resident customers who wish to open accounts without appearing in person, it will not be practical to seek sight of an original passport or national identity card. Copies should be certified by notaries, diplomatic officials, or equivalent independent professionals. Verification of identity and address should also generally be sought from a reputable credit or financial institution in the applicant's country of residence. Steps should be taken to verify the applicant's signature.

6.5 Companies and other legal entities

Because of the potential for concealing beneficial ownership, corporate bank accounts are one of the most high-risk vehicles for money laundering, particularly when opened and ostensibly operated by a legitimate trading company.

Additional obligations for opening corporate accounts focus on knowledge of and about the beneficial owners and any other persons authorised to act on behalf of the account holder. Obtaining information on the purpose and nature of the business relationship, including proof of sources of wealth and initial source of funds, is also particularly important, to enable the reporting entity to conduct meaningful ongoing monitoring.

Before a business relationship is established with a legal entity, and at appropriate regular intervals after the relationship is established, measures should be taken by way of a company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound up or terminated. Further checks should be made whenever the reporting entity becomes aware of changes in the management or ownership structure.

6.5.1 Seychelles companies

The following documents should be obtained:

- The original or a certified copy of the Certificate of Incorporation
- Memorandum and Articles of Association
- Business plan
- Resolution of the board of directors to open an account and confer authority on those who will operate it
- A search of the file at the Companies Registration Office

These documents should (but may not always) provide the necessary information on the legal form and control structure of the company, the beneficial owners, powers to bind the entity, the registered address, and other basic particulars.

Where the company is an International Business Company (IBC) or other special-purpose vehicle, some of this information may not be readily available. Nevertheless, the reporting entity should take all reasonable measures to obtain the required information, either by itself or through an intermediary.

In the case of a publicly listed company, a subsidiary of a publicly listed company, or a private company all of whose directors are already known to the reporting entity, the procedures in the preceding paragraph should be sufficient. Evidence that any individual representing the company has the necessary authority to do so should also be sought and retained.

In the case of a private company whose directors are not previously known to the reporting entity, the identity of all the directors, all persons authorised to operate the account, and all beneficial owners should be independently verified.

When signatories to the account change, care should be taken to ensure that the identity of the new signatories has been verified. In addition, to

discharge the ongoing CDD obligation, it may be appropriate to make periodic enquiries to establish whether there have been any changes to directors or shareholders or to the original nature of the business / activity.

6.5.2 Non-Seychelles companies

Where a company is not registered in Seychelles and is not a recognised foreign bank or publicly listed company, the identity of the directors, account signatories, and beneficial owners (if different) should be established and verified in accordance with the requirements for non-Seychelles personal customers. Enquiries made by the reporting entity should extend as far as practicable to identify those who ultimately own and control the company. Evidence that the individual representing the company has the necessary authority to do so should be sought and retained.

All comparable documents to those listed above for Seychelles companies should be obtained before the account is opened, unless the situation is considered low-risk in accordance with r 10 of the AML Regulations, in which case, within no later than one month of the date of establishing the business relationship, the company should provide certified copies, in English, of its chartered statutes, memorandum and articles or other instrument defining its constitution, a list of directors, and also the name and address of a person resident in Seychelles authorised to accept service of any legal process.

If the company is already in existence when the account in Seychelles is opened, the signatures on the mandate should be confirmed by the company's current overseas bankers who should also confirm that they can verify the identity of each signatory.

Standards of control vary between different countries and close attention should be paid to the place of origin of the documents and the background against which they are produced.

6.5.3 Trust, nominee, and fiduciary accounts

Where a prospective customer is not the beneficial owner, reporting entities are required by the AML Regulations to take reasonable measures on a risk-sensitive basis to identify the ultimate beneficial owner/s and to verify their identity.

An application to open an account or to undertake a transaction by a professional adviser, business or company acting as trustee or nominee requires satisfactory evidence of the identity of the trustee, nominee, or

fiduciary and the nature of their trustee or nominee capacity or duties. Where an individual nominee who opens an account on behalf of another is not already known to the financial institution then the identity of that nominee or any other person who will have control of the account should also be verified.

Enquiries should be made as to the identity of all parties for whom the trustee or nominee is acting and confirmation sought that the source of funds or assets under the trustee's control can be vouched for. If the applicant is unable to supply the information requested, independent enquiries should be made as to the identity of the person who has actual control or for whose ultimate benefit the transaction is undertaken. The results of the enquiries should be recorded in the account opening file.

An application to open an account or undertake a transaction on behalf of an undisclosed third party may be suspicious. Where it is not possible to identify the person(s) for whom or for whose ultimate benefit the transaction is being conducted, for example in respect of foreign trusts where the settlor and beneficiaries cannot be disclosed by the trustees, the account should be profiled as higher-risk and subject to enhanced ongoing monitoring.

Where money is received by a trust, it is important to ensure that the source of the receipt is properly identified, the nature of the transaction is understood, and where possible confirmation made that the payments are made only in accordance with the terms of the trust and are properly authorised in writing. The financial institution must be satisfied as to the bona fides of the trustee.

Stockbrokers, fund managers, solicitors, accountants, estate agents, and other intermediaries frequently hold funds on behalf of their clients in 'client accounts' with financial institutions. Such accounts may be general omnibus accounts which hold the funds of many clients or they may be opened specifically for a single client, which is either undisclosed to the reporting entity or identified for reference purposes only. Those cases, where it is the intermediary who is the customer, should be distinguished from those where an intermediary introduces a client who himself becomes a customer of the reporting entity, or where the intermediary undertakes transactions on behalf of the client, in which case the identity of the client must be independently verified.

6.5.4 Clubs, associations, and charities

Before establishing business relationships with clubs, associations, or charities, a reporting entity should satisfy itself as to the legitimate purpose of the organisation by, for example, requesting sight of the

constitution. Where there is more than one signatory to a proposed account, the identity of all signatories should be established and verified and, when signatories change, care should be taken to ensure that the identity of the new signatories has been verified. Information on the organisation's address and principal owners/controllers should also be furnished.

6.5.5 Unincorporated entities

In the case of partnerships and other unincorporated businesses whose partners/directors are not known to the reporting entity, the identity of all persons that can act on behalf of or benefit from the business should be verified in line with the requirements for personal customers.

Where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account and conferring authority on those who will operate it should be obtained.

7. Suspicious Transaction Report (STR)

Section 10 of the AML Act, 'Reporting suspicious transaction', should be carefully studied by all reporting entities and in particular by CROs.

Reporting entities are required by s 10 to make a suspicious transaction report (STR) in any situation in which the reporting entity:

- has knowledge or reasonable grounds to suspect that any service or transaction may be related, directly or indirectly, to the commission of criminal conduct (as defined in s 3 of the AML Act, including but not limited to money laundering or terrorist financing) or to money or property that is or represents the benefit of criminal conduct;
- has information that may be relevant to an act preparatory to an offence or to money or property that is or represents the benefit of criminal conduct;
- has information that may be relevant to an investigation or prosecution of a person for criminal conduct; or
- has information that may be of assistance in enforcing the AML or POC Acts.

Reporting entities are also required by s 5 of the AML Act to make either an STR or a disclosure under the Prevention of Terrorism Act (as applicable; see below) in any situation in which the reporting entity:

- is unable to carry out CDD in accordance with the AML Regulations for any one of its customers; or
- is unable to undertake ongoing monitoring of any business relationship.

It is important to appreciate that the latter two situations (inability to carry out CDD or ongoing monitoring) are not dependent on any suspicion of criminal conduct on the part of the client/customer.

It is also important to appreciate that there may be an obligation to make an STR in the absence of any transaction or proposed transaction. Reasonable grounds for suspicion can arise in the context of any service provided by a reporting entity.

It is not only reporting entities that are obliged to make STRs. Section 11 of the AML Act provides that supervisory authorities and auditors of reporting entities must make an STR where any transaction or attempted transaction by or through the entity is reasonably suspected by the authority or auditor to be related to the commission of criminal conduct (or an act preparatory thereto) or of assistance in the enforcement of the Act.

The obligation to make STRs under the AML Act complements the duties of disclosure to the Commissioner of Police under the Prevention of Terrorism Act. Sections 34 and 35 of that Act require all persons (not just reporting entities) to disclose to the Police any information that will assist in the prevention or detection of terrorist acts, including information about any property in his or her possession or control that is known to be owned or controlled by or on behalf of a terrorist group, in the circumstances set out in that Act.

It should be noted that if a reporting entity permits a service or transaction to proceed where the timely making of a STR would have prevented that service or transaction from taking place, that reporting entity is likely to have committed the offence of money laundering.

7.1 Recognising suspicious services and transactions

As the types of services and transactions which may be used by a criminal or money launderer are almost unlimited, it is impossible to provide an exhaustive list of indicators of suspicious activity.

The simplest form of money laundering is to deposit accumulated illegal cash in the banking system or to exchange it for valuable items and

thereafter to use the items or funds for legitimate purposes. Modern electronic payment systems enable cash to be switched rapidly between accounts in different names and different jurisdictions, making CDD measures particularly difficult to apply.

There may be numerous reasons why a service, transaction, or pattern of transactions could be considered suspicious, reasons which may be unrelated to the value of the transaction and appear trivial or insignificant when considered in isolation. The context in which the service or transaction occurs may also be significant, and this will vary depending on the type of business and the nature of the customer.

A transaction which is consistent in nature and extent with a customer's known, legitimate business or personal activities or with the normal business profile for that type of account is less likely to be suspicious. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a service, transaction, or pattern of transactions is unusual. Developing and maintaining customer profiles is critical in this regard.

A number of recognised general indicators for high-risk transactions, which reflect known typologies for money laundering and terrorist financing, are set out in Annex I to these guidelines. Annex II contains some examples of suspicious behaviour that local reporting entities may encounter in the course of dealing with current or prospective clients / customers. These examples are indicative only and cannot provide a substitute for ongoing research by CROs and senior officers and formal training programmes for employees.

Some useful current reference resources for typologies and risk indicators are listed in Annex IV.

7.2 STRs and the role of the CRO

Where a potentially suspicious transaction or service has been identified by a reporting entity, the compliance and reporting officer (CRO) must examine the relevant records to confirm whether there are reasonable grounds to suspect that the service or transaction may be related, directly or indirectly, to the commission of serious criminal conduct (including money laundering or terrorist financing). This is the threshold for triggering the core STR obligation under s 10 of the AML Act.

The knowledge of any officer, employee or agent of a reporting entity is taken to be knowledge of the entity. It is accordingly essential to ensure:

- that each relevant employee knows to which person he or she should report suspicions within the institution; and
- that there is a clear reporting chain under which those suspicions are communicated directly to the CRO, with all necessary supporting documentation, without delay.

The degree of decision-making responsibility placed on the CRO (or on the sole operator of the reporting entity, if an individual) is significant. In forming an independent judgement about whether there are reasonable grounds for suspicion, he/she should consider all other relevant information available within the reporting entity concerning the person or business to which the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification and other records held.

If after completing this review, the CRO decides that reasonable grounds for suspicion exist, then he/she must immediately proceed to make an STR to the FIU.

All STRs must be made within two working days of forming the relevant suspicion (or knowledge).

STRs should be submitted on the applicable prescribed form, as set out in Annex III to these guidelines. It is essential that all relevant fields are completed, that the core reason for the suspicion is explained, and that the form is dated and signed or otherwise authenticated.

When deciding to make an STR, a reporting entity should ensure that funds will not be transferred or property disposed of or put beyond reach of the courts of Seychelles. If there is any possibility of these events occurring, the reporting entity should make contact with the FIU by telephone at the earliest opportunity so that appropriate directions can be given to preserve the status quo. The STR should be submitted in writing on the prescribed form as soon as possible thereafter (refer s 10(2)(a) of the AML Act). All STRs should be hand delivered to the office of the FIU.

When submitting an STR the reporting entity should provide the FIU as a matter of course with all information that it has about the transaction or attempted transaction and the parties to the transaction, including the records prescribed under the AML Act. If it is not possible to provide this information with the STR then it should follow as soon as reasonably practicable.

Where a reporting entity has made an STR in relation to a service or transaction in respect of property in its possession or control, the entity is automatically prohibited from providing the service or proceeding with the transaction for 10 working days from the date of the STR, except with the written consent of the FIU (s 10(1)(d) of the AML Act).

After that 10-day period, unless the FIU has issued an administrative freezing direction under s 10(4) of the AML Act, the reporting entity may proceed with the service or transaction. However if a service or transaction that subsequently takes place does in fact constitute the crime of money laundering, the making of the initial STR will not be a defence for any participant with the requisite mens rea.

8. 'Tipping off' and protection from liability

The AML Act requires all officers, employees, and agents of reporting entities to exercise the utmost confidentiality on issues related to money laundering and terrorist financing. However, the Act also provides protection for CROs and others who discharge their statutory responsibilities in good faith.

It is a criminal offence for any person to disclose any information that might prejudice an investigation by the FIU, or potential proceedings under the Act, without lawful authority or reasonable excuse (s 12 of the AML Act). This is commonly known as the prohibition on 'tipping off'. For the purpose of a 'tipping off' prosecution, it does not matter whether an STR or Court application has actually been made or filed, or whether an investigation is actually underway, as long as the person making the disclosure suspects that to be the case.

The only permitted exceptions, apart from disclosures to the FIU or Police, are disclosures to:

- an officer or employee or agent of the reporting entity for any purposes connected with the performance of that person's duties;
- a legal practitioner, attorney, or legal adviser for the purpose of obtaining legal advice or representation in relation to the matter; and
- the supervisory authority of the reporting entity for the purpose of carrying out the supervisory authority's functions.

Where a reporting entity has made an STR or provided other information to the FIU under s 10 of the AML Act, there is an absolute prohibition on disclosing the contents of the STR or report or any information likely to

identify any person who prepared or made the STR or handled the underlying transaction (s 13 of the AML Act). The only exceptions are disclosures for law enforcement purposes.

No civil, criminal, or disciplinary proceedings can be taken against a reporting entity, auditor, or supervisory authority of a reporting entity, or any officer, employee, or agent of those entities (including a CRO), in relation to actions taken in good faith in relation to the monitoring and reporting of suspicious transactions or in compliance with FIU directions (s 14 of the AML Act).

9. Sanctions for non-compliance with AML obligations

All officers, employees, and agents of reporting entities need to understand that they could be personally liable for non-compliance with AML obligations. They should be supported and encouraged by the CRO and other senior officers to participate in relevant training, to make prompt reports of all suspicious transactions, and to cooperate fully with the FIU and other regulatory agencies.

The criminal offences of 'tipping off' and money laundering are discussed earlier in these guidelines. It is also a criminal offence for any person to make a false or misleading statement (or to mislead by omission) in any STR or other report to the FIU (s 50 of the AML Act), or to authorise the opening or operation of any account with a reporting entity in a fictitious, false or incorrect name (s 56 of the AML Act).

Where any body corporate is convicted of an offence under the AML Act or Regulations, and where the act or omission is shown to have taken place with the knowledge, authority, permission or consent of any director, controller, or other officer concerned in the management of the corporate, that person is also guilty of the offence (s 61 of the AML Act).

Offences by reporting entities under the AML Act cover a broad range of compliance failures, including the following:

- Failure to apply CDD and conduct ongoing monitoring
- Failure to terminate a business relationship or transaction and make an STR when unable to apply CDD or ongoing monitoring
- Failure to maintain CDD and transaction/correspondence records, in prescribed manner and for prescribed period
- Failure to maintain accounts in true name

- Failure to make STRs or to provide further information on request
- Failure to comply with a freezing direction
- Failure or refusal to comply with information request from FIU when freezing direction is in force
- Failure to appoint compliance and reporting officer
- Failure to formulate and implement internal rules for compliance
- Failure to train employees
- Assaulting, threatening, intimidating, obstructing, or delaying agents of the FIU or persons assisting them

The penalties available on conviction for compliance offences under the AML Act include fines of up to R 3 million (for failure or refusal to comply with FIU information requests, or furnishing false or misleading information) and terms of imprisonment of up to 12 years. Ignorance of the law is no excuse.

It is essential that every reporting entity supports its staff to take their compliance responsibilities seriously.

Deputy Director
Financial Intelligence Unit

June 2015

Annex I – Indicators of suspicious services and transactions

The following examples have been collated from the websites of other FIUs and the FATF. They are not comprehensive or exhaustive and are provided for indicative purposes only. Several links to more detailed reference material are provided in Annex IV.

General risk indicators

- Transactions or business relationships with countries known to have weak AML/CFT controls, as narcotic source countries, or countries known for highly secretive banking and corporate laws (high-risk countries), especially if transactions are complex and involve intermediaries

- Transactions, business activity, or frequent international travel not consistent with customer profile or known legitimate sources of income/wealth

- Unusually/unnecessarily complex or 'layered' movement of funds

- Transactions involving suspected 'shell' entities (corporations with no legitimate reason for existence)

- Large one-off cash transactions without proof of origin of funds

- Frequent and large international money transfers without clear economic reason

- Sudden changes in volume or nature of business activity

- Services or transactions for the benefit of persons suspected to be criminals, or persons related to or closely associated with them

- Uncharacteristically large transactions or deposits by family members or associates of public officials (PEPs)

- Client or customer maintains an inordinately large or complex network of accounts / business entities for the type of business purportedly being conducted

- Business client cannot be identified online or in official registers

- Use of undisclosed intermediaries/agents/nominees

Bank accounts

- Client deposits large amounts (in local or foreign currency) which are not in line with previous deposits, or are inconsistent with the known assets and income of the client, or are outside the normal course of business of the client
- Customer makes large cash deposits without counting the cash
- Customer tries to exchange large quantities of low denomination notes for those of a higher denomination
- Customer makes deposits containing counterfeit notes or forged instruments
- Cash is deposited in amounts just below the reporting limit, with several transactions during a day or over a few days
- Cash is frequently deposited in rounded-off large amounts
- Client maintains cash deposits in several accounts amounting to large sum in total
- Customer attempts to take back a portion or all of cash deposit that exceeds the threshold limit after learning that the transaction will be reported
- Non-active accounts are reactivated, large transactions are performed, and then the account is inactive again or cancelled
- Client makes large deposits and then liquidates the account quickly, without explanation
- Account shows high velocity in movement of funds but maintains low beginning and ending daily balances
- Account activity far exceeds activity projected at time of opening
- Large number of apparently unrelated persons make deposits to or receive payments from one account without rational explanation
- Payments out match credits paid in cash on the same or previous day

- Client purchases large number of traveler's cheques or other securities for cash, or exchanges a large number of securities for cash, especially if outside normal course of business

- Client requests opening of a letter of credit or other bank instrument based on securities, or through offshore banks, or banks located in high-risk countries

- Client deposits cash in several accounts, then combines the amounts in one account for transfer abroad or withdrawal from a foreign ATM

- Client withdraws large amounts of cash from an account on which he has just received large and unexpected transfers from abroad

- Company does not want to submit all information about its business activities, and the company's representatives avoid contact with the branch whenever possible

- Nature of business is described vaguely as 'consultancy' or 'investment' and unsupported by a detailed business plan or proof of source of funds

- Deposits and withdrawals from a company's bank account are performed in cash and not in the form of cheques or wire transfers

- Account is used for receiving and making large payments, but no normal business transactions are recorded on the account, eg salaries or invoice payments

- Client makes cash deposits to business account with the purpose of payment described as 'loan from founder' or 'increasing capital assets'

- Client makes numerous cash deposits for a company that normally does not deal with cash

- Significant increase in the number of cash deposits for a company that provides professional consultancy services, especially if the amounts are quickly transferred out of the account

- Frequent unexplained transactions between a client's personal and business accounts

Wire transfers

- All transfers to or from high-risk countries that are inconsistent with a customer's business or profile or not satisfactorily explained
- Frequent wire transfers in large round amounts
- Large number of wire transfers between two accounts without clear economic or business purpose, especially if performed through high-risk countries
- Client sends wire transfers to a country where his company has no business relations or receives wire transfers from legal entities with which he has no business relations
- Client sends periodic wire transfers from a personal account to a high-risk country without reasonable explanation
- Large incoming wire transfers on behalf of a foreign client without reasonable explanation, particularly if described as loans from foreign lender
- Funds transferred in and out of an account on the same day or within a relatively short period of time, without reasonable explanation
- 'U-turn' transactions – funds transferred out of jurisdiction and then portion quickly returned, or vice versa
- Wire transfer payments or receipts with no apparent links to legitimate contracts for goods or services
- Transfers routed through multiple foreign or domestic banks
- Payment instructions received to wire funds abroad, and at the same time to expect an incoming wire transfer of funds in an equivalent amount of currency from other sources

Lending

- Sudden or frequent early repayment of loans with no reasonable explanation for source of funds
- Significant amounts of cash used as security for loans, especially where loan is repaid before it falls due
- Multiple loans obtained over short period of time with repayments made in cash
- Customer provides no record of past or present employment on a loan application
- Request to borrow against assets held by a third party, where the origin of the assets are unknown or the assets are inconsistent with the customer's profile

Insurance

- Cancellation of recently purchased insurance policy for refund in the form of cash or cheque
- Request to make a policy cancellation payment to a third party
- Request to send policy documents to another person's address
- Request for insurance policy with very high premium, particularly when client wishes to pay on an annual basis or in full
- Sudden request by policy holder for bigger insurance policy with larger premium
- Sudden request by policy holder to change from paying monthly for the premium to paying annually or in full
- First (or only) insurance premium is paid for in foreign currency
- Client accepts insurance conditions clearly unfavourable in relation to his health or age
- Client emphasises secrecy and/or seeks to persuade or bribe the insurance agent not to report the transaction

Safe deposit boxes

- Safe deposit boxes opened in name of non-residents
- Large amounts of cash on deposit
- Multiple safe deposit boxes opened by single customer
- Unusually frequent visits to a safe deposit box or significant changes in usage patterns

Legal professionals

- Client is vague or evasive about themselves, their principal (if any), the nature of their business, the reason for a proposed transaction, or their source of funds
- Client seems to be using an intermediary or actively avoiding personal contact without good reason
- Client offers substantially higher fees than normal
- Client has changed attorney repeatedly or retained multiple attorneys without reasonable explanation
- Client is reluctant to provide normal information and documents or provides suspicious or inconsistent documents
- Client requests shortcuts or unexplained speed in completing transactions or alters instructions at last minute for no reason
- Client uses multiple accounts / corporate vehicles or requests unnecessarily complicated ownership structures or transactions without economic justification
- Person actually controlling a transaction is not a party, or the person giving instructions does not appear to be a suitable representative
- Client is known to be related to or associated with suspected criminals
- Proposed transaction involves persons or entities associated with high-risk countries

- Unusual source of funds or method of payment for a proposed transaction, eg third party funding with no reasonable explanation

- Unusually short repayment terms or repeated early repayments

- Client requests payments to third parties without reasonable explanation or corresponding transaction

- Unexpected dramatic increase in capital or asset base of client with no reasonable explanation

- Transaction being notarised is clearly inconsistent with size, age, activity, or relationship of persons or entities involved, or reflects an obvious difference between declared price and approximate actual value

- Documents produced for notarisation are incomplete, in foreign language without certified translation, or in copy only

Annex II – Examples of suspicious activity

Below are some examples of suspicious activity that reporting entities in Seychelles may encounter in the course of conducting business.

1. Suspicious customer behaviour

- Customer is secretive and reluctant to meet in person
- Customer has an unusual, nervous, or excessive demeanour
- Customer is accompanied and watched
- Customer insists that a transaction be done quickly or volunteers the information that a transaction is 'clean'
- Customer shows uncommon curiosity or level of knowledge about record keeping or reporting requirements
- Customer attempts to deter compliance with record keeping or reporting duties, through threats or otherwise
- Customer presents inconsistent or confusing details about a transaction or does not appear to understand it
- Customer appears to have only informal records of significant or large volume transactions
- Customer is reluctant to proceed with a transaction after being told it must be reported
- Customer suggests payment of a gratuity or unusual favour
- Family members or close associates of public officials (PEPs) begin making large transactions not consistent with their known legitimate sources of income

2. Suspicious customer identification circumstances

- Agent, attorney, or financial advisor acts for another person without proper proof of authority

- Customer is unwilling to provide personal identity information or wants to establish identity using unofficial documents

- Customer furnishes unusual, suspicious, or inconsistent identification documents

- Customer is unusually slow in providing supporting documentation or cannot provide properly certified copies

- Customer spells name differently from one transaction to another, uses alternative names, or uses a consistent address but frequently changes the names of persons involved

- Customer's telephone is disconnected

- Business customer is reluctant to reveal details of business activity or beneficial ownership

- Business customer is reluctant to provide financial statements and other documents or presents documentation noticeably different from those of similar businesses

3. Suspicious employee activity

- Employee exaggerates the credentials, background, financial ability, and/or resources of a customer in internal reporting

- Employee lives a lifestyle that cannot be supported by his/her salary

- Employee frequently overrides internal controls or established approval authority or circumvents policy

- Employee permits or facilitates transactions where the identity of the ultimate beneficiary or counterparty is not disclosed

- Employee avoids taking holidays

Annex III – Prescribed form for STR
(a) Banks

Return AML-CFT/BANKS (i)

FINANCIAL INTELLIGENCE UNIT

ANTI-MONEY LAUNDERING & TERRORIST FINANCING

REPORTING OF SUSPICIOUS TRANSACTIONS

Part 1	**Disclosing Party**

1. Name of Institution .....
2. Address .....
3. Telephone Number .....
4. Report Related to: Money Laundering ☐
   Terrorist Financing ☐
   Other Criminal Activities ☐

Part 2	**Information on Person/Entity Engaging in Suspicious Activity or Transactions**

1. Account Type Individual ☐ Company ☐ Trust ☐
2. Account Name(s) .....
3. Account Number .....
4. Date Opened DD/MM/YYYY ……/……../…….
5. Registered Address .....
6. Operating Address .....

Identification Details of Account Holder(s) and Other Persons Authorized on the Account

1. Name .....
2. Date of Birth DD/MM/YYYY ……/……../…….
3. ID Number .....

4. Passport Number ……..

5. Nationality ……

Identification Details of Person Executing the Transaction if different than Account Holder or Authorized Person

1. Name ……

2. Date of Birth DD/MM/YYYY ……/……...../…….

3. ID Number ……

4. Passport Number ……

5. Nationality ……

Identification Details of the Business Entity

1. Place of Incorporation ……

2. Date of Incorporation DD/MM/YYYY ……/……...../…….

3. Business Activity ……..

……

Identification Details of the Company Director(s)

A (i) Name ……

A (ii) Date of Birth DD/MM/YYYY ……/……...../…….

A (iii) ID Number ……..

A (iv) Passport Number ……..

A (v) Nationality ……..

A (vi) Occupation ……

B (i) Name ……..

B (ii) Date of Birth DD/MM/YYYY ……/……...../…….

B (iii) ID Number ……..

B (iv) Passport Number ……

B (v) Nationality ……

B (vi) Occupation ……

C (i) Name ……

C (ii) Date of Birth DD/MM/YYYY ……/……...../……

C (iii) ID Number ……..

C (iv) Passport Number ……..

C (v) Nationality ……..

C (vi) Occupation ……

Identification Details of Beneficial Owners

A (i) Name ……

A (ii) Date of Birth DD/MM/YYYY ……/……...../……

A (iii) ID Number ……..

A (iv) Passport Number ……..

A (v) Nationality ……..

A (vi) Occupation ……

A (vii) Date of Appointment DD/MM/YYYY ……/……...../……

A (viii) Date of Resignation (if relevant) DD/MM/YYYY ……/……...../……

B (i) Name ……..

B (ii) Date of Birth DD/MM/YYYY ……/……...../……

B (iii) ID Number ……..

B (iv) Passport Number ……

B (v) Nationality ……

B (vi) Occupation ……

B (vii) Date of Appointment DD/MM/YYYY ……/……...../…….

B (viii) Date of Resignation (if relevant) DD/MM/YYYY ……/……...../…….

If more than two Beneficial Owners, please fill details in on a separate page

Other Known Information Associated Persons/Companies..etc

……

……

……

……

……

……

……

……

……

……

Part 3	**Information about Suspicious Activity or Transaction**

1. Date of Transaction DD/MM/YYYY ……/……...../…….
2. Date of Detection DD/MM/YYYY ……/……...../…….
3. Amount Involved ……
4. Currency ……

5. Type of Transaction

Cash	☐
Swift Transfer	☐
Cheque	☐
Card	☐

6. Full Details and Description of Transaction

……

……

……

……

……

……

……

……

……

If the Transaction is a Transfer, Details of the Beneficiary of the Transfer

1. Name of Beneficiary ……
2. Address ……
3. Account Number ……
4. Beneficiary Bank ……
5. IBAN Number ……

7. Reasons why the transaction was reported as suspicious:.....

……

……

……

……

……

……

……

……

……..

……

……

……

……..

……

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the Financial Intelligence Unit, i.e. statement, correspondence, vouchers, transfers, account opening and identification documents, etc.

----------	----------	----------
Signature of Official	**Designation**	**Institution's Stamp**

Date: ----------

Annex III – Prescribed form for STR
(b) Bureaux de Change

Return AML-CFT/Bureau de Change (iii)

FINANCIAL INTELLIGENCE UNIT

ANTI-MONEY LAUNDERING & TERRORIST FINANCING

BUREAU DE CHANGE - REPORTING OF SUSPICIOUS TRANSACTIONS

Part 1	**Disclosing Party**

1. Name of Individual / Company .....
2. Address .....
3. Telephone Number .....
4. Report Related to: Money Laundering ☐
   Terrorist Financing ☐
   Other Criminal Activities ☐

Part 2	**Information on Person/Entity Engaging in Suspicious Activity or Transactions**

1. Full Name of Person or Company .....
2. Date of Incorporation DD/MM/YYYY ……/……../…….
5. Registered Address .....
6. Operating Address .....

Identification Details of the Company Director(s)

A (i) Name .....

A (ii) Date of Birth DD/MM/YYYY ……/……../…….

A (iii) ID Number .....

A (iv) Passport Number ……..

A (v) Nationality ……

A (vi) Occupation ……

B (i) Name ……..

B (ii) Date of Birth DD/MM/YYYY ……/……/……

B (iii) ID Number ……..

B (iv) Passport Number ……

B (v) Nationality ……

B (vi) Occupation ……

If more than two Company Directors, please fill details in on a separate page

Identification Details of the Beneficial Owner(s)

A (i) Name ……

A (ii) Date of Birth DD/MM/YYYY ……/……/……

A (iii) ID Number ……..

A (iv) Passport Number ……..

A (v) Nationality ……

A (vi) Occupation ……

B (i) Name ……..

B (ii) Date of Birth DD/MM/YYYY ……/……/……

B (iii) ID Number ……..

B (iv) Passport Number ……

B (v) Nationality ……

B (vi) Occupation ……

If more than two Company Directors, please fill details in on a separate page

Other Known Information Associated Persons/Companies..etc

.....

.....

.....

.....

.....

.....

.....

.....

.....

Part 3	**Information about Suspicious Activity or Transaction**

1. Date of Transaction DD/MM/YYYY ……/……...../…….
2. Date of Detection DD/MM/YYYY ……/……...../…….
3. Amount Involved ……
4. Currency ……
5. Type of Transaction
   - Cash ☐
   - Swift Transfer ☐
   - Cheque ☐
   - Card ☐

6. Full Details and Description of Transaction

……

……

……

……

……

……

……

……

……

……

7. Reasons why the transaction was reported as suspicious:.....

……

……

……

……

……

……

……

……

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the Financial Intelligence Unit, i.e. statement, correspondence, vouchers, transfers, account opening and identification documents, etc.

---------- ---------- ----------

Signature of Official **Designation** **Institution's Stamp**

Date: ----------

Annex III – Prescribed form for STR
(c) DNFBPs & other non-financial reporting entities

Return AML / CFT/NON-BANKS (ii)

FINANCIAL INTELLIGENCE UNIT

ANTI-MONEY LAUNDERING & TERRORIST FINANCING

REPORTING OF SUSPICIOUS TRANSACTIONS

Part 1	**Disclosing Party**

1. Name of Company .....
2. Address .....
3. Telephone Number .....
4. Report Related to: Money Laundering ☐
   Terrorist Financing ☐
   Other Criminal Activities ☐

Part 2	**Information on Person/Entity Engaging in Suspicious Activity or Transactions**

1. Full Name of Person or Company .....
2. Date of Incorporation DD/MM/YYYY ……/……../…….
5. Registered Address .....
6. Operating Address .....

Identification Details of the Company Director(s)

A (i) Name .....

A (ii) Date of Birth DD/MM/YYYY ……/……...../……

A (iii) ID Number ……..

A (iv) Passport Number ……..

A (v) Nationality ……..

A (vi) Occupation ……

B (i) Name ……..

B (ii) Date of Birth DD/MM/YYYY ……/……...../……

B (iii) ID Number ……..

B (iv) Passport Number ……

B (v) Nationality ……

B (vi) Occupation ……

If more than two Company Directors, please fill details in on a separate page

Identification Details of the Company Beneficial Owner(s)

A (i) Name ……

A (ii) Date of Birth DD/MM/YYYY ……/……...../……

A (iii) ID Number ……..

A (iv) Passport Number ……..

A (v) Nationality ……..

A (vi) Occupation ……

A (vii) Date of Appointment DD/MM/YYYY ……/……...../……

A (viii) Date of Resignation (if relevant) DD/MM/YYYY ……/……...../……

B (i) Name ……..

B (ii)	Date of Birth	DD/MM/YYYY ……/……...../……
B (iii)	ID Number	……..
B (iv)	Passport Number	…….
B (v)	Nationality	……
B (vi)	Occupation	…….
B (vii)	Date of Appointment	DD/MM/YYYY ……/……...../……
B (viii)	Date of Resignation (if relevant)	DD/MM/YYYY ……/……...../……

If more than two Beneficial Owners, please fill details in on a separate page

Other Known Information Associated Persons/Companies..etc

……

……

……

……

……

……

……

……

……

……

……

……

……

……

Part 3	**Information about Suspicious Activity or Transaction**

1. Date of Transaction DD/MM/YYYY ……/……...../…….
2. Date of Detection DD/MM/YYYY ……/……...../…….
3. Amount Involved ……
4. Currency ……

5. Type of Transaction
   - Cash ☐
   - Swift Transfer ☐
   - Cheque ☐
   - Card ☐

6. Full Details and Description of Transaction

……

……

……

……

……

……

……

7. Reasons why the transaction was reported as suspicious:.....

……

……

……..

……

……

When submitting this report, please append any additional material that you may consider suitable and which may be of assistance to the Financial Intelligence Unit, i.e. statement, correspondence, vouchers, transfers, account opening and identification documents, etc.

----------	----------	----------
Signature of Official	**Designation**	**Institution's Stamp**

Date: ----------

Annex IV – Reference sources for AML typologies and risk indicators

- *AUSTRAC Typologies and Case Studies Report 2013*
  http://www.austrac.gov.au/sites/default/files/documents/typ13_full.pdf

- FIC (South Africa), *Combating Financial Crime in South Africa: Typologies Report* (2014)
  https://www.fic.gov.za/DownloadContent/NEWS/PRESSRELEASE/FIC_Typologies_report_FINAL.pdf

- FINTRAC (Canada), *Guideline 2: Suspicious Transactions* (2010)
  http://www.fintrac-canafe.gc.ca/publications/guide/Guide2/2-eng.pdf

- Financial Action Task Force (FATF), *Methods and Trends*
  http://www.fatf-gafi.org/topics/methodsandtrends/

- Eastern and Southern African Money-Laundering Group (ESAAMLG), *Typologies*
  http://www.esaamlg.org/reports/typologies.php