ANTI-MONEY LAUNDERING, TERRORIST FINANCING AND CORRUPTION

PRACTICAL GUIDE

FOR TRUST AND COMPANY SERVICE PROVIDERS (TCSPs)

V1.2 - 12 September 2023

Contents

1. INTRODUCTION

1.1 The Purpose of these TCSP Guidelines

These guidelines have been prepared by the **A**ssociation **M**onégasque des **Pr**ofessionnels en **A**dministration des **S**tructures **E**trangères (AMPA) for guidance to its members[i].
The activities performed by a trust and company service provider ("TCSP") as defined in Law no. 1.362 of August 3, 2009 (as amended from time to time) on the fight against money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, and corruption, (AML Law 1.362), by Article 1(6) as follows:

- persons who, on a regular basis, set up, manage or administer legal persons, legal entities or trusts on behalf of third parties and who, in this capacity, provide one of the following services to third parties on a professional basis:

  - act as agent for the incorporation of a legal person, entity or trust;
  - act or arrange for another person to act as director or company secretary of a capital company, partner of a partnership or holder of a similar position for other legal persons or entities;
  - provide a registered office, business address or premises, administrative or postal address to a corporation, partnership or other legal person or entity;
  - intervene or arrange for another person to act as trustee of a trust;
  - intervene or arrange for another person to intervene as a shareholder acting on behalf of another person;

These TCSP Guidelines are applicable to persons and entities carrying out the services envisaged under AML Law 1.362.

The purpose of this document is:

a) to assist TCSPs with the interpretation of the AML Law 1.362. and provide sector-specific guidance on the implementation of particular anti-money laundering and the combating of funding of terrorism ("AML/CFT") obligations that warrant further elaboration at an industry-specific level; and also

b) to provide detailed information on money laundering and funding of terrorism and corruption ("ML/FT-C") risks to assist TCSPs in formulating a better understanding of the ML/FT-C risks they face and ensure that they are better equipped to detect and report ML/FT-C suspicions.

It is important that this document is read in conjunction with the *Generic Guidelines published by SICCFIN/AMSF*.

2. TCSP RISK ASSESSMENT

2.1 External Risk Assessments

TCSPs should to take into consideration any relevant risk information emerging from risk assessments and guidance such as the National Risk Assessment and any relevant sectoral risk assessments, as well as the Financial Action Task Force (FATF) guidance for a risk based approach for Trust and Company Service Providers (latest version June 2019). These documents are vital for informing authorities and TCSPs on those areas and sectors that are at greater risk of ML/FT-C.

2.1.1 National and Sectoral Risk Assessments

The **NRA** and sectoral risk assessments provide information on the local ML/FT-C risk context, and so their findings are vital for strengthening risk understanding and enhancing the implementation of the Risk Based Approach (RBA) so as to mitigate risk. As the first line of defense, TCSPs have to be aware of the country's ML/FT-C risks and be able to effectively deter them from materializing or, detect them and avoid misuse. To factor findings of the NRA and sectoral risk assessments into their business and customer risk assessments, TCSPs need to understand and assess the likelihood of the risks highlighted in the results of such assessments manifesting themselves within their operations. This will require an analysis of exposure from both a qualitative and a quantitative perspective.

2.1.2 Monaco's National Ml/Ft-C Risk Assessment

Monaco's 2nd NRA included a presentation of the sector, the threats, vulnerabilities, and mitigation measures in place as summarised below:

As of 31 March 2021, there were 38 TCSPs in the Principality of Monaco. This number has been falling year on year and as at 1 August 2023 was 29.

The sector is essentially made up of small firms with fewer than ten employees, and none employs more than 50 people.

The profession is not governed by any specific laws or regulations. The Association Monégasque des Professionnels en Administration des Structures Etrangères ("AMPA"), the Monegasque Association of Corporate Service Providers") was founded in 2004, and lobbies actively and contributes to the shaping of legislation and regulations as part of the Government-led AML Committees. (n.b. membership of AMPA is recommended, but not obligatory).

The profession is a moderately-sized sector in terms of Monaco's economy. The formation, administration, and domiciliation of companies and other legal entities for nearly 70% of TCSPs' activity, trust-related business represents 10%, and other activities 20%.

2.1.2.1 Threat exposure

Money laundering typologies have been identified in this sector, and it has featured in a number of investigations or proceedings in NRA 1, and this was again the case in NRA 2. Proceedings have been filed against TCSPs by the CERC, and sanctions ranging from warnings to licence withdrawals have been imposed since the publication of NRA 2.

2.1.2.2 Vulnerabilities

The customer risk is considered to be high. Although PEPs and high-risk customers appear to make up a relatively small proportion of the total for this sector, the customer base has several noteworthy features:

- Beneficial owners are almost exclusively foreign nationals;
- A large proportion of beneficial owners reside outside Monaco, although the number has fallen slightly;
- The companies or other bodies corporate held are mostly registered in offshore jurisdictions.

It was also found that the formalities involved in creating and/or administering offshore companies require TCSPs to use the services of agents based in the country where the company is registered.

Finally, the various supervisory roles performed by SICCFIN have found that TCSPs have an uneven understanding of how to categorise customers by risk, although beneficial owners can be identified without any particular difficulties.

2.1.2.3 Mitigation measures

The majority of TCSPs in Monaco deal almost exclusively with private individuals as opposed to corporate customers for which the risk profile and services provided will require different mitigation measures.

According to the Monaco NRA professionals appear to have sound knowledge of AML/CTF matters. They have internal procedures and training is given regularly to all staff. Professionals in this sector understand the legal implications of breaching their compliance obligations.

Checks carried out by the supervisory authority have found few failings in the identification of beneficial owners.

In addition, AMPA has provided its members with a tool, created specifically for this sector by an independent local supplier, enabling them to establish a business risk assessment for their company.

Members of the profession are required to obtain an operating licence from the Business Development Agency**.**

SICCFIN audited 66% of the TCSPs operating in the Principality over the period covered by NRA 2. Its supervision is real and effective, and officers have a good level of knowledge of the risks in this sector.

2.1.2.4 Assessment of sector risk level

The level of vulnerability was assessed as medium- high. The threat level was assessed as medium-high and rising.

Given the threat level, residual vulnerability and mitigation measures put in place, the TCSP sector's overall risk level was considered as medium-high.

2.1.3 Moneyval's Fifth Round Mutual Evaluation Report

Following Moneyval's Fifth Round Mutual Evaluation Report on Monaco's Anti-money laundering and counter-terrorist financing measures issued in December 2022 the risk assessment for TCSPs is expected to be further enhanced in future national risk assessments.

2.1.4 Sectorial risk assessment - EU

The latest EU Supranational Risk Assessment (EUSNRA) carried out in 2022 concludes that, in relation to trusts and other legal arrangements, the estimated level of risk for terrorist financing is MEDIUM and for money laundering VERY HIGH. Many threats and vulnerabilities for money laundering have been identified in relation to (domestic and foreign) trusts and similar legal arrangements. They are to be considered as lucrative tools to lauder [sic] the proceeds of crime. In contrast, there is little evidence that trusts and similar legal arrangements have been misused for the purpose of financing terrorism. However, their secrecy and the possibility to use them in combination with legal entities make trusts and similar legal arrangements vulnerable to abuse for terrorist-financing purposes.

The EUSNRA dedicates a specific section under non-financial products to Nominees. This fiche distinguishes between formal and informal nominees (e.g., strawmen) and focuses on the former, i.e., nominee directors and nominee shareholders. This analysis focused on appointing nominee directors and shareholders as one of the higher risk activities of Trust and Company Service Providers (TCSPs). The EUSNRA concluded that the estimated risk level relating to nominee services in relation to terrorist financing is MEDIUM and for money laundering VERY HIGH.

Is it to be pointed out that TCSPs in Monaco should not act as "nominee" directors. TCSPs may act as a director, or make arrangements for the provision of directors in their own name and not ''on behalf of (and subject to instructions of) a "nominator". In this capacity they should be acting independently in accordance with normal corporate governance principle, and should take responsibility for the decisions that they take.

2.1.5 **Other sectorial risk assessments**

This guidance considers below some relevant TCSP service related issues as identified in other jurisdictions where TCSP services are commonly provided:

Key inherent issues for TCSPs are identified as:

a) Significant volume of high-risk customers – most notably the high incidence of non-resident beneficial owners (BOs);
b) Services provided are often risky in nature – specifically the setting up of corporate structures that are complex, and the holding of shares in a fiduciary capacity;
c) High level of geographical risk – driven by the considerable number of non-EU resident BOs of companies set up outside of Monaco, with a significant exposure to risky jurisdictions;
d) Large volume of international business handled by TCSPs;
e) Higher service interface risk – considering that a portion of TCSP customers may be on-boarded on a non-face-to-face basis, with the involvement of intermediaries.
f) The number of STR reports submitted by TCSPs in proportion to the ML/FT-C risks that they are exposed to is often low. This may be indicative of a weak awareness of ML/FT-C risks or a lack of resources;
g) Tax evasion is one of the highest drivers of ML vulnerability in the sector;
h) Specific risks related to Private Banking and Wealth Management customers result from:
    - High-profile customers, including PEPs and HNWI
    - Culture of confidentiality and the use of “secrecy jurisdictions” or “shell” companies
    - Significant profit potential for the Financial Institution and TSCPs involved
    - High Value Transactions
    - Complexity of financial services and products
    - "Commercial or “third party” transaction flows;
i) In corporate structures each element may be controlled/managed by a different TCSP, making it more difficult to identify at all times who is the UBO;
j) In corporate structures involving more than one TCSP it may be difficult for each TCSP to understand and monitor the business activities and transactions of each element of the chain.

To assess the extent of such exposure to the risk of TCSPs service being exploited for ML related to tax evasion, one needs to analyse factors such as the type of customers that are more likely to pose such a risk, and the distribution of such customers within the customer base. Self-employed persons, contractors, consultants and cash-intensive businesses are likely to pose a higher risk of tax evasion, as are those customers who have benefitted from tax amnesty schemes.

From a service point of view, TCSPs need to understand which of their services are more at risk of being misused to facilitate tax evasion or the laundering of proceeds of crime. This would then be followed by an assessment of the volume of business that such services represent.

TCSPs should consider the threat of TF due to the status of the Principality as an international Financial Centre. Historically there have been only very few TF related STRs in Monaco, and few cooperation requests sent/received by SICCFIN and/or the Police. There is an inherent risk that corporate vehicles may be used for TF, as this has occurred in other international financial centres. The TSCP sector may be involved in the transfer of funds to/from high-risk jurisdictions, or have customers who are terrorist financers. Legal entities may be used to hide the identity of terrorist financers.

TCSPs are to always refer to the latest available versions of the Monaco NRA and of any sectoral risk assessments, as the risk environment is bound to change over time. Sectors or services previously considered high risk may become less risky due to an improvement in controls by TCSPs and competent authorities, while emerging risks may also be identified based on new information.

Note:

- Keep abreast of TSCP sector risks, and ML/FT-C typologies through publications issued by international bodies.
- And through the Monaco National Risk Assessment to focus on risk of the sector locally
- Ensure staff are kept updated of changing risks faced by the TCSP.

2.2 The Value of the Professional to the Criminal

Why would criminals and money launderers seek the services of professionals such as TCSPs? This is because, whether knowingly (such as in the case of professional money launderers or even when opting to remain willfully blind to the circumstances) or unknowingly, professionals may play a role in ML/FT-C. Primarily, they have specialised knowledge to assist and/or advise their customers on financial matters, and/or provide corporate or fiduciary services. In view of the respect and trust that is associated with their profession, and the fact that they are important introducers of business to financial institutions the services of TCSPs may be invoked to provide a veil of legitimacy. The following examples show how the services provided by TCSPs are of value to criminals:

2.2.1 Incorporating Companies and Legal Arrangements

There are many legitimate uses for companies and structures such as trusts, foundations and associations. These same companies and structures are unfortunately also useful for layering and moving illicitly generated funds. Companies can be set up to carry out trading activities, with criminals creating fictitious transactions or inflating the value of specific goods or services. Illegally generated funds can then be transferred through accounts held in the name of these companies, under the guise of payments for regular activity. Legal entities and arrangements are attractive vehicles because they can be used to conceal, or make it harder to identify, the identity of the individuals controlling and benefiting from them or the underlying structures. If a customer seeks assistance to set up or service a structure with multiple entities in different countries, all known for their confidentiality and lack of transparency, a professional has to understand the purpose and rationale behind this.

2.2.2 Introducing Customers to Financial Service Providers

TCSPs have historically enjoyed the trust and respect of financial institutions and may be introducers of a significant amount of business to financial institution; a recommendation from a TCSP may provide a bridge to open a bank account in a country where the customer has no connection. This is another form of added value that can be derived when engaging TCSPs.

3. RISK AND RISK BASED APPROACH

3.1 The Risk-Based Approach

The ML/FT-C framework applicable to TCSPs adopts a RBA. This means that TCSPs are required to adopt measures, policies, controls, and procedures that are commensurate to the specific ML/FT-C risks which they are exposed to, so as to prevent or mitigate the effect of these risks.

The RBA acknowledges that the ML/FT-C risks that TCSPs face vary according to the sector and according to the individual TCSP, and in turn allows for resources to be invested and applied where they are needed the most.

A RBA envisages and permits the application of checks and controls that are proportionate to the risks identified by

TCSPs. As a fundamental principle, high-risk areas should be subjected to enhanced procedures, such as enhanced due diligence measures, while lower areas of risk can be addressed through simplified or reduced controls.

An effective RBA relies on two essential elements:

a) an understanding of the risks that a TCSP is exposed to; and
b) based on this understanding, the variation of one's controls, policies, measures, and procedures to achieve the strongest mitigating effect possible, and in a way that prioritizes resources.

The successful application of the RBA requires an assessment of the risks that a TCSP's business is exposed to, through a **business risk assessment**, as well as a specific assessment of the risk that TCSPs will be exposing themselves to when establishing a specific business relationship or carrying out a given occasional transaction, through **customer risk assessments**.

3.2 Risk Assessments

3.2.1 The Business Risk Assessment

MONACO AML Law requires subject persons to apply appropriate due diligence measures, proportionate to their nature and size, to meet their obligations in accordance with their own assessment of the risks presented by their activities with regard to money laundering, the financing of terrorism, the proliferation of weapons of mass destruction and corruption.

Section 1 of the Generic Guidelines sets out how a business risk assessment is to be conducted, with guidance on the various steps of the process, including the methodologies that can be applied, the risk factors to consider, and when and how often it is to be reviewed. This section is to be considered and applied in full, with the below being some of the key principles in relation to the BRA:

a) The BRA is a critical tool for subject persons to identify the risks that they are exposed to, and to ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate such risks.
b) Conducting a BRA is a legal obligation and a copy of the BRA is to be submitted to SICCFIN/AMSF whenever requested to do so.
c) As a minimum, the BRA must assess the risks arising from the five main risk factor categories, namely the nature of the product and services offered, the conditions of the transaction, delivery channel risk factors, the characteristics of the customer, and country and geographical zone risks. Section 3.3 of this document provides additional risk factors that are of specific relevance to TCSPs and these additional factors may need to be built into the BRA depending on the nature of the business of each TCSP.
d) The BRA must be documented in writing. The BRA and any updates thereto must be approved by the Board of Directors or equivalent management body. Naturally this does not apply with respect to sole trader TCSPs, who must sign off the BRA themselves.
e) Risk is dynamic and may be affected by external changes as well as changes in the activities, services and operations of the subject person. Consequently, the BRA is to be regularly reviewed and kept up to date.
f) The level of detail and complexity of the BRA is to be proportionate to the nature and size of the TCSP's business. By way of example, a TCSP with several employees, operating across various jurisdictions, and offering multiple types of services to a large customer base is exposed to a broader spectrum of risks, and would therefore be expected to have a BRA that appropriately reflects the size and nature of its activities and operations. On the other hand, a sole trader TCSP or a small TCSP servicing a limited number of customers will not require a complex assessment, and this can continue to be built upon as needed to reflect any substantial growth in the size and nature of the operations.

In addition to the relevant chapter in the Generic Guidelines, TCSPs may refer to the FATF Guidance for a Risk-Based Approach for Trust and Company Service Providers for best practices to be adopted when conducting a BRA.

To assist TCSPs with implementing a Risk Based Approach, AMPA has made available an automated Excel-based instrument, produced in collaboration with a local specialist provider, taking account of all the factors which are internationally recognised as having an influence on customer risk assessment, including updated country risk profiles. There is no obligation to use this instrument, although many will find it helpful, as it reduces the need to import other means of customer risk control. The Methodology Review attached to the instrument touches on the factors used and the remainder of this section elaborates on these, so that TCSPs have a full understanding of the issues involved.

Key risk factors identified in this model for each of the five risk factors are included in annex 1.

3.2.2 **The Customer Risk Assessment**

In addition to conducting a BRA, TCSPs must also assess the risks that they are exposed to when providing their services to a specific customer/client. A customer risk assessment (CRA) relates to the risks posed by a given customer, the service being provided to them, the risks associated with the jurisdictions they and their business are connected to, and the channels through which services are being provided to them.

A CRA allows TCSPs to determine the appropriate level of CDD that would need to be carried out in order to mitigate the risks identified. A high-risk business relationship would require the application of enhanced due diligence measures, while the simplified customer due diligence measures envisaged can only be applied if the CRA results in a low risk of ML/FT-C.

Part 2 of the Generic Guidelines provides detailed guidance on how to conduct a CRA, including aspects relating to timing, revisions, and the weighting and categorization of risk factors. The below are some key principles that are to be kept in mind when conducting CRAs, and must be read in conjunction with the respective sections of the Generic Guidelines:

A CRA must be carried out before entering a business relationship or carrying out an occasional transaction.

As with the BRA, the CRA must include an assessment of the risks relating to five main risk factor categories, namely the nature of the product and services offered, the conditions of the transaction, delivery channel risk factors, the characteristics of the customer, and country and geographical zone risks.

Section 3.3 below, entitled 'Sector-Specific Risk Factors' provides additional risk factors that are of specific relevance to TCSPs. The risk posed by a relationship is dynamic, which means that the CRA is to be reviewed and updated from time-to-time to ensure that it continues to reflect the risk profile of the customer. When reviewing the data, information and documentation obtained as part of one's ongoing monitoring obligations, any change in circumstances that may be noticed should trigger a review and if necessary, an update of the customer's CRA. In addition, certain events or developments that result in a material change in the nature of the relationship should equally trigger a review of the CRA. Events and developments that would normally trigger the need for a review include the detection of unusual activity, changes to the nature of the business, changes to the source of funds, a request for new services, or changes in the structure or beneficial ownership of the customer. Risks relating to the beneficial owner(s) of the customer must also be factored into the CRA.

When conducting a CRA, TCSPs are to assess all known risk factors. In addition to the five main risk factor categories indicated above, there are other factors relating to certain attributes of the customer that only arise in the context of a CRA, and so must be assessed and addressed when conducting it. These factors relate to the reputation, the nature and the behaviour of the customer and its beneficial owner(s). Key principles on these risk factors are highlighted below.

3.2.2.1 **Reputation**

a) TCSPs must assess whether there is publicly available information that links the customer or its beneficial owners to criminality or terrorism. Any such information must be factored in when assessing prospective customers and should also lead to a review of the CRA of existing customers.
b) Supervisory or regulatory action taken against the customer also needs to be factored in when assessing the ML/FT-C risk posed by the relationship. Such information is relevant if it increases the

likelihood that the customer is, has been, or may be involved in activity that generates illicit proceeds.

c) Existing customers that have been subject to an STR are considered to pose a higher ML/FT-C risk, and so any STRs filed by the TCSP should lead to a revision of the CRA.

3.2.2.2 Behaviour and Nature

The behaviour of individuals seeking a TCSP's services, as well as the structure of the entity requesting the services, can impact the ML/FT-C risk thereof. The following elements are considered to increase the ML/FT-C risk of a relationship:

a) Reluctance by the customer to provide information and/or documents that are required for CDD purposes.
b) Where doubts or concerns arise on the veracity or authenticity of any information and documents provided.
c) Where the customer has little or no connection to Monaco and requires services related to a Monaco Société Civile Particulière and there is no sound economic and legal reason for seeking such services in Monaco.
d) Where the ownership and control structure involve a request for bearer shares or nominee/fiduciary shareholders.
e) Whenever there are material changes to the customer's ownership and control structure for which there does not seem to be a legitimate rationale.

The following sections provide guidance on sector-specific risk factors applicable to TCSPs, which are to be taken into consideration when conducting and updating the BRA and CRAs. These complement the generally applicable risk factors set out above and in the Generic Guidelines.

3.3 Sector-specific Risk Factors

To conduct risk assessments, TCSPs need to identify the threats and vulnerabilities which they are exposed to. This is done by considering those areas from which risk may manifest itself – these areas are known as **risk factors**. TCSPs are required to assess at least five main categories of risk.

These categories are referred to as nature of the product and services offered, the conditions of the transaction, delivery channel risk factors, the characteristics of the customer, and country and geographical zone risks.

The Generic Guidelines explain these categories in more detail and provide examples of risk factors that apply and are relevant to all sectors.

The following section of the document explores additional elements of risk that are relevant to TCSPs. TCSPs are to bear in mind that risk factors are those elements which increase the risk of ML/FT-C, and hence increase the potential of ML/FT-C to take place.

With appropriate and commensurate controls and due diligence measures, the risks can be eliminated or reduced to a manageable level.

3.3.1 Product and Service Risk

There is an obligation to identify and exercise due diligence when a CSP enters into a business relationship, i.e. when: (arts 4-1 and 5 L and art 2 OS)

- a professional and a customer enter into a contract under which several successive transactions will

be carried out between them over a fixed or indefinite period or which creates ongoing obligations
- a customer regularly and repeatedly requests the services of the same professional to carry out separate and successive financial transactions

and for occasional customers who meet the conditions of article 4, i.e.

- a transfer of funds
- one or more transactions in excess of €15,000
- a transaction, regardless of the amount, whenever there is a suspicion of money laundering, terrorist financing or corruption

The range of services offered by TCSPs in Monaco can include higher and lower risk activities. It is important that businesses understand and properly appraise the risk presented by each business activity, customer or class of customer and properly reflect this in their risk assessment.

For example the provision of Trustee or Foundation management services where the TCSP operates independently of the settlor; and provides services to low risk trusts when the source of wealth and funds is clear, established for the benefit of disabled persons or charitable beneficiaries would normally be lower risk. In comparison the provision of director services where the TCSP is not in full control of the company assets would normally present a higher risk and require the TCSP to adapt their monitoring accordingly.

The risks related to the provision of one particular service alone (such as company secretarial services) may be mitigated by the provision of additional services (such as tax filings or bookkeeping) which may allow the TSCP to better monitor the ML/TF risks associated with the services provided.

An analysis of different types of services that may be performed by TCSPs, and the relevant type of compliance that would be expected is set out in the table below:

	IDENTIFICATION				VIGILANCE LINKED TO THE SERVICES PROVIDED		CONSTANT VIGILANCE UNTIL THE BUSINESS RELATIONSHIP IS CLOSED
Compliance required according to services provided	**Identification of UBO + identification of the structure if applicable (directors, shareholders, etc.) and control of blacklists**	**Knowledge of the socio-economic background - UBO profile**	**Determination of the level of risk**	**Identification nature and purpose of the relationship / engagement letter or service contract**	**Verification of the simple consistency of transactions**	**Control of transactions and counterparties**	**Periodic updating of identification data according to the level of risk and verification of blacklists**
	4-1 L and art 5, 6, 8,10, 11, 13, 14, 15, 15-1 OS	*art 4-3 L + art 1er pt 15 and 10 OS*	*art 4-3 et 11 L , art 25-3 and s. OS*	*art 4-3 L and art 10 OS*	*art 5 L and 26 OS*	*art 26 and 28 OS*	*art 5 L, 26 OS*
1. International legal and tax advice without movement of funds Example: advice on private international law, theoretical international tax advice,	X		X	X			X
2. International legal and tax advice with movement of funds Example: preparation of loan agreements, purchase or sale agreements, purchase or sale of foreign structures holding real estate in Monaco. Control of transactions and counterparties in the limited context of the advice provided.	X	X	X	X	X	X	X

3. Creation of structures Notes: Direct or indirect creation of any structure (including SCP Monégasque). The consistency of transactions is verified in relation to the initial purpose of the structure (in particular, in the case of the purchase of an asset by a Monegasque SCP, information should be requested on the purchase price and the method of financing). * - for an occasional transaction not strictly required by the law, but recommended, and normally undertaken as combined with other services.		X	X (*)	X(*)	X(*)	X		
4. Domiciliation of Monegasque SCPs, without management Notes: The consistency of transactions is checked solely on the basis of the information available when the company is domiciled, in particular by receiving mail and/or bank statements. If the company is managed, apply line 7.		X	X	X	X	X		X
5. Coordination between UBO and foreign agent for payment of the resident agent's annual invoice Notes: Management and shareholding provided by third parties, no monitoring of the relationship with the UBO, no legal advice or secretarial services apart from receiving		X	X	X	X			X

and returning the agent's annual invoice.								
6. Management and/or administration and/or coordination and/or operational monitoring of a foreign structure Notes: Insofar as the relationship with UBO is maintained in Monaco and the operations and documents to be signed by the legal representatives outside Monaco are prepared in Monaco, the situation is comparable to that of a de facto manager. In the event that the UBO or a third party has unlimited power to act on behalf of the structure and/or on the bank account, the same provisions apply, with the possibility of delegating this power to a financial institution, in accordance with the terms of the Law and the OS.		X	X	X	X	X	X	X
7.Function of management and/or shareholder and/or signatory on bank account Notes :See previous point		X	X	X	X	X	X	X

8. Legal secretarial services without movement of funds Example: drafting of simple minutes for a change of registered office, for opening an account, for a change of director, etc.		X		X	X			X
9. Legal secretarial services with movement of funds Example: drafting of minutes to acquire a property; to sign a loan agreement.		X	X	X	X	X	X	X
10. Agent activity L 1.381 Notes : Verification of blacklists every year during the UBO verification		X			X			
11. Accounting for a structure Notes: Keeping the accounts of a structure, without any other role in the structure.		X	X	X	X	X		X
12. Carrying out transactions on the basis of authority granted by a structure Note: Control of transactions and counterparties within the limits of the authority granted (e.g. a foreign company must sign a deed in Monaco and wishes to be represented in this specific context).		X	X	X	X	X	X	X

3.3.2 The conditions of the Transaction (Transaction Risk)

TCSPs provide a range of services and activities that differ in their methods of delivery, the depth and duration of the relationships formed with customers, and the size of their operation. The ML/FT-C risks associated with the various services can differ, depending on the inherent features of the service offered.

The level of transparency and complexity associated with the service, and the value and volume of transactions permitted through the service, drive the TCSP's risk exposure. These elements are outlined in more detail below:

Anonymity: The ML/FT-C risk is higher where the service provided by the TCSP provides or facilitates anonymity. This occurs by allowing the customer or beneficial owner to remain anonymous or by obscuring the beneficial owner's identity or the audit trail of transactions.

Complexity: Risk can also be driven by the complexity of the transactions that may be carried out through, or as a consequence of, the service provided. As an example, this would include services which facilitate or result in the movement or change in ownership of multiple assets across entities or jurisdictions.

Large value or volume of transactions: TCSPs are exposed to a higher risk when their services facilitate the planning or execution of large value transactions, for instance through their involvement in mergers or the provision of advice on the acquisition of high value assets or finance raising transactions.

3.3.3 Delivery channel Risk

The delivery channel risk, which is also known as 'interface risk' is the risk arising from how the TCSP interacts with its customer, and the channels it uses to provide a given product or service. TCSPs conduct business through varying channels, and these affect exposure to ML/FT-C. The following are a few considerations that need to be made when determining the interface risk of a given business relationship or occasional transaction:

3.3.3.1 Non-Face-to-Face Interaction

This includes non-face-to-face onboarding (the risks of which can be mitigated through the adoption of various due diligence measures), but also ongoing non-face-to-face interaction such as taking instructions and processing transactions in a non-face-to-face manner. Implementing technological means that address the risk of impersonation or identity fraud, where relevant, is one way of mitigating the risks of such exposure.

3.3.3.2 Communicating through an Intermediary

There are situations when TCSPs do not communicate directly with their customers, but through an intermediary. The TCSP's relations with the intermediary may increase the level of ML/FT-C risk. The risk arises from the lack of contact with the customer throughout the duration of the business relationship, as well as due to exposure to any risks posed by the intermediaries themselves. The reputation and integrity of the intermediary impacts the type of customers that the intermediary deals with and the way business is conducted.

Thus, prior to entertaining relations with the customer, TCSPs need to be reassured of the reputability and integrity of the intermediary. If the intermediary is not already well-known and enjoys a positive reputation, the TCSP may need to undertake checks on the intermediary using public (open source) information. Further guidance on dealing with intermediaries is provided in Section 4.1.2 of this document.

Other elements that affect the level of ML/FT-C risk of a given intermediary include for instance, when an intermediary is established or operating in a high-risk jurisdiction or a jurisdiction known to have deficiencies in its AML/CFT framework. This factor would expose a TCSP to a higher degree of ML/FT-C risk, as opposed to when dealing with an intermediary in a reputable jurisdiction that is supervised for AML/CFT purposes.

3.3.4 The characteristics of the customer - Customer Risk

The following are examples of customer risk factors that TCSPs may be exposed to and that may increase or indicate a higher risk of ML/FT-C, together with an explanation of the cause giving rise to the risk:

3.3.4.1 The customer is or forms part of a Complex Corporate Structure

Complex corporate structures are ownership structures that are not immediately transparent as to who ultimately owns or controls them. A structure may be complex due to having multiple tiers of shareholding levels. Such structures could also involve shareholding through different types of entities and arrangements, such as trusts and foundations. These entities and arrangements may also be incorporated in multiple overseas jurisdictions, further increasing the complexity. The structure becomes more complex if one or more entities involve bearer shares or shares held in a nominee or fiduciary capacity.

Servicing a complex structure increases the ML/FT-C risk for the TCSP due to the inherent opacity of the structure. This makes it more challenging to establish the ownership and control structure and determine who the beneficial owners are.

Where the entities and arrangements within the structure are established in multiple overseas jurisdictions, TCSPs may encounter obstacles in obtaining company information from reliable and independent sources to verify ownership and control.

Within complex structures, it becomes more complicated to obtain a clear understanding of the purpose of the set-up and of the customer company's role within that structure.

The use of complex corporate structures is a known means for facilitating ML/FT-C, the mentioned factors make such structures attractive vehicles to purposely obscure ownership and/or to layer transactions throughout the various entities. This increases the risk of misuse of legal entities (such as companies) and arrangements (such as trusts and foundations) for criminal purposes.

3.3.4.2 Mitigating Measures

TCSPs must ensure that they identify and verify the identity of the beneficial owners and take steps to understand and document the ownership structure. Registers of beneficial ownership information contribute to increasing transparency and TCSPs are to use these to complement their due diligence measures.

Understanding, documenting and corroborating the ownership structure together with understanding the reasons for that particular set-up provides TCSPs with much needed information for risk assessment purposes and the actual determination of ML/FT-C risk they are exposed to. There may be legitimate tax, business, or economic reasons to justify such complexity.

In addition to understanding the activity conducted by its corporate customer, where the customer forms part of a group structure, the TCSP must also seek to understand the overall activity/operations of the group, and understand the role of the subsidiary (the customer) within the group.

TSCPs should mitigate the risks that they face by being selective about the clients they accept to act for. They may prepare a risk statement which sets out the policy for the nature of acceptable client business of the TSCP.

The fact that the TCSP may have set up various structures according to its own analysis of a customer's needs, and also provides administration and management services, will help put the risks into perspective.

3.3.4.3 The Customer operates within the VFA/Crypto sector

Having customers who are active in the VFA sector may expose TCSPs to a higher risk of ML/FT-C. When assessing the risk associated with entertaining business relations with a VFA operator, or a customer who transacts in crypto currencies TCSPs should have regard to the below considerations:

a) The operator's regulatory status: an operator that carries out its activities from or in a jurisdiction that does not regulate or supervise the activity in question exposes TCSPs to a significantly high risk of ML/FT-C when compared to an operator that is regulated and supervised for AML/CFT purposes. One needs to have regard to the jurisdiction which is regulating the VFA operator in question. Being subject to regulation in a non-reputable or in a high-risk jurisdiction dilutes the relevance of regulatory oversight exercised over the VFA operator.
b) The activities of the operator: VFA operators provide different types of services, each giving rise to varying levels of ML/FT-C risks. For instance, providing services consisting in the transfer of VFAs increases the TCSP's risk, particularly due to the ability to transfer high values and volumes of transactions.
c) The transaction profile of the customer who uses Crypto currencies

3.3.4.4 **The Customer is or owns a Cash-Intensive Business**

The provision of services to entities that carry out primarily or substantially cash transactions increases the ML/FT-C risk exposure for TCSPs.

Businesses that are cash intensive receive significant amounts of payments in cash, such as catering establishments, supermarkets and fuel stations, traders in high value goods (e.g.: cars, jewelry, arts, yachts, watches, antiques), and entertainment establishments such as land-based casinos**.**

Cash has historically been the most popular means of currency in the criminal underworld, as it allows anonymous transactions, and can be moved around without leaving a trail, allowing criminals to disconnect themselves from the activity which generated the illicit cash.

Most cash intensive business operate legitimately, but nevertheless are at an increased risk of being misused for ML/FT-C purposes. Cash-intensive operations provide a potentially efficient way for commingling illicitly obtained cash with proceeds derived from the genuine operations of the business. In turn, these are placed into the financial system under the guise of legitimate business transactions and earnings.

Additionally, owners of cash intensive businesses may be less likely to declare their full earnings, exposing TCSPs to tax evasion. TCSPs should also consider the Monaco cash restriction regulations, limiting the use of cash when in transactions involving the sale or purchase of determinate high value goods. TCSPs may be especially well placed to detect if these regulations are being breached and whether the customer is in fact making use of proceeds of crime.

3.3.4.5 **The Customer is or owns a High-Volume Trading Business**

High-volume trading activity involves the processing (or facilitation) of high volumes of transactions. Examples of such operations include online and land-based casinos, financial institutions such as payment service providers and electronic money institutions, and virtual financial asset exchange services.

The risk associated with servicing these entities is driven by the high volume of transactions processed, which increases the challenges of identifying suspicious transactions. The risk is further increased by the fact that the TCSP does not have a relationship with or any control over the end customer (the customer's clients), and so is not able to conduct due diligence on such end clients. Thus, the TCSP is exposed to the many risks that may be posed by the customer's clients.

3.3.4.6 **Factors indicative of a Lower Customer Risk**

The following are examples of customers who typically present a lower customer ML/FT-C risk. This does not mean that the business relationship is one of low risk, but merely that the risk presented by the customer (prior to assessing other risk factors) may be lower. TCSPs must bear in mind that it is the customer risk assessment that ultimately dictates the level and type of risk associated with a given business relationship/occasional transaction:

a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate

transparency of beneficial ownership;

b) public administrations or enterprises in reputable jurisdictions.

3.3.5 Customer related definitions

3.3.5.1 Arranging

Monaco TCSPs may arrange for another person to act as a director or secretary of a company, a trustee or foundation council member, a partner in a partnership, or a similar position in relation to other legal entities. It should be noted that arranging does not include the process of headhunting or advertising to find a suitable candidate for a position. These services would typically be carried out by recruitment agencies.

The mere compilation of statutory forms or the carrying out of other formalities necessary for the appointment of a company director, secretary or similar positions in other legal entities is not considered to be a service of arranging for someone to act as a director, secretary or an equivalent position. ML/TF risk of this activity would be low for the TCSP.

3.3.5.2 Formation of Entities

Formation services consist in the provision of services to incorporate companies or set up trusts, foundations or other legal entities, including Sociétés Civiles, in which one would be actively assisting in the preparation, completion and submission of relevant documentation and liaising with relevant registers where appropriate.

When the services only entail the compilation and submission of ancillary statutory forms to set up a company or other commercial partnership (e.g., beneficial ownership declarations), one would not be providing a formation service for the purposes of these TCSP Guidelines.

3.3.5.3 The Customer

A customer is a legal or natural person seeking to form (i.e. a potential customer) or has formed (i.e. an existing customer) a business relationship, or a legal or natural person seeking to carry out an occasional transaction with a TCSP.

In the case of TCSPs, the type of customer varies depending on the services that are being provided. The table below provides an interpretation of who the customer is in the context of the various company services that may be provided by TCSPs:

COMPANY SERVICES	WHO IS THE CUSTOMER/CLIENT	NATURE OF SERVICE
Formation of a company or a Société Civile	The prospective shareholder/UBO/partner, for whom the company or other legal entity will be set up	For a one-off service this will normally be an Occasional transaction
Acting as a director, manager or secretary of a company, or a partner in a commercial partnership, or arranging for another person to act as such	The company or Société Civile to which such services are offered	Business relationship
Provision of registered office, business correspondence or administrative address or related services to a company or Société Civile	The company or Société Civile to which such services are offered	Business relationship

FIDUCIARY SERVICES		
Formation of a Trust or Foundation	The prospective settlor/founder for whom the Trust or Foundation is formed	For a one-off service this will normally be an Occasional transaction
Acting as a trustee or board member of a Trust company, or board/council member of a Foundation or arranging for another person to act as such	The trustee of the Trust or the Foundation to which such services are offered	Business relationship
OTHER SERVICES		
Provision of mandataire services under Law 1381	The company or a non-transparent Société Civile to which such services are offered	Business relationship
Provision of services of the responsible person for the UBO register under article 22 of Law 1.362	The Société Civile to which such services are offered	Business relationship

3.3.5.4 **Distinguishing between the concepts of Introducer, Intermediary and Agent**

The person requesting the TCSP's services will normally be the customer itself. However, there may be circumstances in which the customer would be introduced or represented by another person or entity. In the TCSP context, customers may be introduced or represented by:

3.3.5.5 **The Introducer**

An Introducer is defined as a person who typically (though not necessarily) would have a business relationship with a third party (who, in this case, would be the Introducer's customer) and who introduces that third party to a TCSP. The intention would be that the third party would form a business relationship or conduct a one-off transaction directly with the TCSP. In this way the Introducer's customer or third party becomes a customer of the TCSP directly.

The Introducer's role is solely to make the introduction, and he would have no further involvement in the business relationship or the occasional transaction that would be established or carried out. It is the identity of the introduced customer that must then be established and verified, and no AML/CFT obligations arise in relation to the Introducer.

With that said, the integrity and type of clientele brought forward by an introducer implicated in criminality may be compromised and TCSPs may wish to carry out periodic checks on open sources to ensure there is no significant adverse media on the introducer.

3.3.5.6 **The Intermediary**

An Intermediary introduces the customer to the TCSP and remains involved in the business relationship between the customer and the TCSP, by giving instructions to the TCSP on the customer's operations or by coordinating work for the customer;

There are situations when an Introducer introduces a third party to a TCSP, but then proceeds to remain actively involved in carrying out the occasional transaction or in the business relationship established with the TCSP. This could be, for instance, by being responsible for communicating customer instructions to the TCSP (both at the initial stages when carrying out an occasional transaction or setting up a business relationship, or throughout that business relationship, as the case may be) without necessarily being legally authorised to bind the customer in the same way as an Agent would.

In such a scenario, the person making the introduction does not remain an introducer but becomes an Intermediary.

An Intermediary may, therefore, be an individual who enjoys the customer's trust and communicates the customer's intentions, instructions and decisions in relation to a particular transaction or matter to the TCSP, and/or undertakes specific tasks or activities (such as project management, vetting of documents, general co-ordination of the project, and giving legal or other advice to the customer), without having any powers to bind the customer.

In this scenario, while the TCSP is always, naturally, obliged to carry out CDD measures on the customer, the TCSP must also carry out further due diligence measures on the Intermediary.

3.3.5.7 **The Agent ("Mandataire")**

The Agent acts on behalf of a customer and can bind the underlying customer, for example by signing letters of engagement (thereby creating an indirect relationship between the TCSP and the customer and a direct relationship with the Agent). When the customer is a company or commercial partnership, its directors and partners, who are legally empowered to represent and bind the company or commercial partnership, are likewise considered to be agents when they exercise these legal representation powers to bind the company or commercial partnership. These individuals are typically involved in the carrying out of an occasional transaction or business relationship by giving instructions to the TCSP that bind the company or partnership, or by taking actions that likewise bind the company or commercial partnership (e.g., signing contracts on the company's behalf).

In order to better understand these types of relationships, the concepts of Agent and Intermediary must first be examined.

3.3.5.8 **The role of company directors and partners as agents**

Those company directors who are vested with the legal and judicial representation of a Company, or Société Civile or Commercial Partnerships who, within the context of an occasional transaction or a business relationship, act on behalf of the Company (e.g., signing contracts, agreements or letters of engagement), are likewise considered to be agents who purport to act on behalf of the respective company or commercial partnership.

These would therefore be required to be identified and verified, and the TCSP is expected to ensure that they are authorised in writing to act on the customer's behalf. As is explained in further detail below under Section 4.1.4, not all directors and partners need to have their identity and authorisation verified; this applies only to those who exercise the legal powers to bind the company or commercial partnerships within the context of an occasional transaction or business relationship carried out or established with the TCSP.

3.3.5.9 **Application of the distinction in real-life scenarios**

Intermediary relationships typically involve another local or foreign TCSP, trustee and/or wealth management firm, family office (or multi-family office), estate agent, law firm, accountancy/audit firm or other professional firm. The Intermediary, in this case, does not stop at merely *introducing* the customer, as explained above, but remains involved as the point of reference to carry out that occasional transaction or business relationship, without necessarily having the capacity to actually *bind* the customer.

The fact that all correspondence takes place between the TCSP and the introducing law firm or other professional firm as the Intermediary (and irrespective of whether the customer is always or mostly copied in, never copied in or copied in only rarely), is in itself indicative of the law firm or other professional firm actually acting as an Intermediary and not merely as an Introducer.

While each case must necessarily be assessed on its own merits, there may be circumstances that would indicate that the purported introducer is not simply an Introducer, but is actually acting as an Intermediary, for instance:

- instructions are always or mostly provided by a person purporting to be merely an Introducer;
- the letter of engagement is entered into with the purported Introducer, who then ends up coordinating the

project; or

- the letter of engagement is entered into with the customer directly, but interaction between the TCSP and the customer takes place through the purported Introducer.

When it comes to determining whether a person is an Intermediary or a mere Introducer, it is irrelevant whether it is the Intermediary or the underlying customer who ultimately pays the fees or is taking the risk of non-payment of fees. It is also irrelevant who ultimately decides issues; that is, whether the underlying customer has given the Intermediary some formal authority to take decisions on certain matters or whether the Intermediary is required to refer all matters to the underlying customer for a decision.

In other words, any situation in which an individual or entity carries out additional activities beyond merely introducing the customer to the TCSP and stopping there, renders that individual or entity an Intermediary, thereby necessitating the application of due diligence measures on that Intermediary.

It might transpire while (or even after) setting up a business relationship that a presumed customer or company UBO is acting on behalf of another person, i.e., a *prete nom*, fiduciary mandatory or front man. A TCSP may become aware of these situations through various behavioral indicators, such as when:

a) the presumed customer/UBO is not able to provide outright instructions on the company's operations since he/ she has to refer decisions to someone else;
b) correspondence between the TCSP and the customer/UBO might involve a third party, which is unknown to the TCSP;
c) the TCSP's professional fees are being paid up by someone else other than the presumed customer/UBO; or
d) the presumed customer/UBO shows a lack of detailed understanding about the company's business.

In these instances, and unless there exists a legitimate explanation, TCSPs should consider submitting an STR to SICCFIN/AMSF and desist from providing further services to this customer.

3.3.5.10 **Distinction between intermediation and reliance**

It is important to distinguish an Intermediary or Agent relationship from a situation where reliance is being placed in AML Law 1.362. The two should not be confused since they are completely distinct, and one does not necessarily involve the other. That is, a TCSP can be dealing with an Agent or an Intermediary without placing reliance on that Agent/Intermediary, just as a TCSP can rely on another TCSP or a third party without that other subject person/third party being an Agent or an Intermediary with regard to the TCSP.

In certain circumstances an Introducer, Intermediary or Agent could be another TCSP or third party subject to AML/CFT obligations in another jurisdiction on whom the TCSP is permitted at law to place reliance to carry out some aspects of CDD. In this case, it is up to the TCSP to determine whether to place reliance or, alternatively, to conduct its own CDD on the underlying customer (besides also on the Intermediary or Agent).

For further guidance on implementation of the reliance provisions, see Section 4 below on Customer due diligence obligations.

3.3.6 **Country and geographical zone risks -Geographical Risk**

This refers to the risk that arises from connections with one or more geographical areas. The jurisdictions to be taken into consideration for this purpose are those (a) where the customer or its beneficial owners are based, have their main place of business or where the activity generating their wealth is carried out, and the jurisdictions with which the customer has especially strong trading or financial connections; or (b) with which the customer or its beneficial owner have relevant personal links (e.g., the individual's residence in a given jurisdiction). If these jurisdictions pose a higher risk of ML/TF-C or their AML/CFT frameworks are deemed to be non-reputable, there is a higher risk that funds connected to the relationship are tainted.

Note:

- Manage the risks faced by the TCSP by selecting customers and services based on a thorough assessment of their profile.
- Mitigate the risks based on the assessed profile.
- A TCSP which controls all activities in a customer's structure, and manages the entire chain of ownership will be in a better position to reduce risks.

4. CUSTOMER DUE DILIGENCE

4.1 Common circumstances

The Generic Guidelines provide details of the means of identification and verification of customers and related parties. The section below provides additional specific guidance in respect of some common circumstances which may be encountered by TCSPs:

4.1.1 A person acting solely as Introducer

When a person acts solely as an Introducer, having no further involvement other than introducing the customer, by, for instance, providing instructions or otherwise representing the customer, the TCSP would not be required to carry out any CDD on the Introducer.

4.1.2 A person acting as an Intermediary

TCSPs should have internal processes to review and approve Intermediaries before the TCSP starts servicing customers who are introduced and represented by these Intermediaries. These internal processes are necessary for TCSPs to ensure that they deal with Intermediaries who are reputable and of good standing, which will itself reflect on the quality, standing and intention of customers who are introduced to them. These internal processes should require senior management approval before any working relationships with intermediaries are initiated. These processes should also require scrutiny and due diligence to be carried out on the Intermediary for the senior management's determination to be well informed. This scrutiny and due diligence should include the following:

<u>Basic checks for all Intermediaries:</u>

a) determine whether the Intermediary would be representing end customers to whom/which company services will be provided, or whether the Intermediary will be passing on instructions from another intermediary/other intermediaries, one of which would ultimately represent the end customer (i.e., "Intermediary Chains");
b) establish the existence of the Intermediary through public sources;
c) assess, and be satisfied with, the Intermediary's reputability and integrity. This would involve carrying out public searches (e.g., using online search engines, meta search engines or commercial databases) to assess whether any adverse information exists on the Intermediary, which would raise doubts about the Intermediary's integrity, such as involvement in any wrongdoing (e.g., criminal offences or breaches of AML/CFT, prudential or other professional obligations). Moreover, given that these Intermediaries are typically professional law, accountancy or tax advisory firms or other TCSPs, the TCSP would also be expected to confirm that these Intermediaries are licensed, regulated or are accredited professionals, as the case may be; and,
d) when the relationship with the Intermediary is ongoing, TCSPs are to carry out regular checks to ensure that the information obtained at the point of establishing the working relationship with the Intermediary remains current and to be aware of any new information that might concern the Intermediary's reputability and integrity. These ongoing checks are expected to be carried out at least on an annual basis.

Additional checks for higher risk Intermediaries

Higher risk Intermediaries would include Intermediaries who are:

- not subject to any licensing, regulation or professional accreditation;
- situated in high-risk or non-reputable jurisdictions; or
- less renowned and on whom it is difficult to find information through public sources.

Before establishing working relationships with higher risk Intermediaries, TCSPs should be more cautious and should carry out additional and more in-depth checks on these Intermediaries. These additional checks may include:

a) identifying and verifying the Intermediary's identity by collecting the necessary identification details and verifying those identification details on the basis of data, documents or other information. In the case of Intermediaries that are firms or entities, TCSPs should also identify the directors, partners or administrators of these Intermediaries and also identify and verify the identity of their ultimate BOs.

b) in the case of Intermediaries that are entities or firms, extending the reputability and integrity checks envisaged under paragraph (c) above of the list of basic checks for Intermediaries to cover not only the Intermediary, but also its directors, partners or administrators, and its ultimate BOs;

c) gathering further information on their internal AML/CFT procedures (where applicable) to formulate an understanding of the Intermediary's compliance culture;

d) holding introductory meetings (physical or virtual meetings using a video-conferencing facility);

e) in the case of Intermediary Chains, carrying out the above procedures on each and every Intermediary in the chain; and

f) where the relationship with the Intermediary is ongoing, TCSPs are to carry out regular checks to ensure that the information obtained at the point of establishing the working relationship with the Intermediary remains current and to be aware of any new information that might concern the Intermediary's reputability and integrity. These ongoing checks are expected to be carried out at least on an annual basis.

This section is intended to provide guidance on the due diligence checks that are to be carried out by TCSPs when they seek to establish a working relationship with an Intermediary. When TCSPs would, in addition, be placing reliance on the CDD measures carried out by Intermediaries on the end customers, TCSPs refer to section 4.3.4.

4.1.3 **A person acting as an Agent**

Where a customer is represented by an Agent, who acts on his/her behalf to carry out an occasional transaction or to set up a business relationship, or else is empowered to act on behalf of and bind the customer throughout the business relationship, the TCSP must not only identify and verify the customer but must also carry out specific CDD measures on that Agent, who is purporting to act on the customer's behalf.

The following persons or entities would be considered to be acting for and on behalf of the customer:

a) directors or partners who are authorised to legally represent the corporate customer and who take actions that formally bind the company or legal entity within the context of an occasional transaction or business relationship, such as by signing letters of engagement with the TCSP or by signing off any operations and agreements that bind the company or commercial partnership throughout the business relationship; and

b) other persons who are empowered to act on the customer's behalf, such as by carrying out transactions on behalf of the corporate customer being serviced by the TCSP (e.g., bank signatories), or persons who, by means of a power of attorney or resolution, are authorised to take any action that binds the corporate customer.

In these cases, the TCSP is expected to identify and verify the identity of any person purporting to act on the customer's behalf, and to also ensure that this person is authorised in writing to act on the customer's behalf.

4.1.4 Treatment of directors and partners

While TCSPs are expected to identify all directors or partners of corporate or fiduciary entity customers (including directors of Trustee Corporations, or board/council members of Foundations) TCSPs are not expected to verify the identity of all these directors, but only those who are authorised to legally represent the corporate customer and who exercise that power of representation within the context of an occasional transaction or a business relationship.

In this regard, TCSPs must also ascertain that these directors are actually vested with the power to legally represent the corporate customer.

In order to ascertain that directors and partners are duly authorised to represent the respective company or commercial partnership, reference may be made to the constitutive document of that respective legal entity, such as the Memorandum and Articles of Associations or other statutory document, or to any power of attorney or resolution authorizing the person concerned.

4.1.5 Provision of instructions by staff members of corporate entities

There may also be instances when the TCSP is approached by an individual (such as a CEO or CFO), acting on behalf of the company or entity, to establish a business relationship with the TCSP. As explained above, the TCSP is expected to identify and verify this individual's identity, and also to ascertain that he/she is duly authorised to represent the company.

However, as the business relationship progresses, the TCSP starts receiving instructions from members of staff working within that CEO or CFO's team. The requirement to ensure that the actual person sending instructions binding the entity is so vested with that authority is not to be interpreted to mean that the TCSP should require documentation to ascertain that each staff member giving instructions is so authorised. In these cases the TCSP should verify the link between this member of staff and the entity. This can be done by, for example, ensuring that the relevant individual (the CEO or CFO, in this case) is copied in on the relevant emails sent by the staff member in question, which would enable the TCSP to assume that the CEO or CFO is aware that this staff member is giving binding instructions.

Alternatively, the TCSP could also be considered as having verified the link between the member of staff and the respective entity if that member of staff have been originally copied in, or introduced in earlier correspondence sent by, or including, the CEO or CFO who originally requested the provision of services, or any other such situation indicating that they have been given authority by the CEO or CFO to continue providing instructions.

4.2 Trusts, Foundations and other entities - verification

The obligations of businesses when establishing or administering or dealing with trusts and foundations and other entities are outlined below. They summarise the requirements for identifying and verifying the identity of various individuals and entities associated with the trust or foundation, including settlors, founders, trustees, councilors, foundation board members, guardians, protectors, beneficiaries, and persons exercising ultimate effective control. The text also provides examples of suitable documents for verifying the identity of a trust or foundation. It also mentions the importance of understanding the ownership and control structure of the trust and the purpose of the business relationship or occasional transaction.

The text also discusses the verification of the identity of the beneficial owners of foundations and trusts, providing guidelines and definitions for determining control and ownership. It emphasizes the importance of verifying the identity of natural persons likely to benefit from the foundation or trust and obtaining relevant documents to support the verification process.

The details obtained on the trust or foundation must be verified by referring to appropriate independent, reliable sources. Verification should be undertaken by either requesting a copy of the trust instrument from the trustee or an extract of the relevant parts of the trust instrument or the equivalent for a foundation. In exceptional circumstances, such as when a trust is created verbally and thus no trust deed or similar instrument exists in writing, verification can be carried out by obtaining a signed declaration by the trustee containing the information listed in paragraphs 4.2.1.1. (a) to (d) below.

When trusts or foundations are registered in an official registry, another alternative available to the TCSP is to refer to these registers, though particular attention has to be paid to any limitations on registration therein, which may limit the quality and reliability of the information reported.

It is up to the TCSP to ensure, in accordance with its CRA (and bearing in mind, among other matters, the risk posed by the particular relationship to be established, the governing law of the trust, or the law of the foundation, the country of residence of the trustee and also the complexity of the structure) that appropriate measures be adopted to verify the existence of the trust or foundation. TCSPs should bear in mind that documents and sources vary in their degree of reliability. In particular, when the verification documentation and/or information is obtained directly from the trustee or from the foundation or when one relies on a declaration made by the trustee, or the board of the foundation, the TCSP should keep in mind the status of the trustee (e.g. whether the trustee or the authorised person representing the foundation is subject to any registration, authorisation or licensing requirements for it to carry out its activities, and whether they are subject to the same or equivalent provisions of AML Law 1362 in the jurisdiction from which their business is conducted and where it is supervised for compliance with those provisions) and their reliability (e.g., whether there is any adverse information on the trustee, or foundation representative).

When copies of documents are obtained, TCSPs should consider, based on the risk assessment carried out by the TCSP, whether additional checks and safeguards should be applied to ensure it is satisfied with the robustness of its verification measures. This may include obtaining documents duly certified by the trustee, the foundation representative or other reliable persons.

Where the *customer* is a trust, *foundation* or other *legal arrangement*, there may be a situation where a charity or NPO is identified as a "long-stop" beneficiary, for example, under a calamity/disaster clause (or equivalent). In such cases the TCSP would not be expected to consider the factors identified above when carrying out a *relationship risk assessment*, except where all other intended beneficiary arrangements have failed, or if the TCSP considers it appropriate in the circumstances.

4.2.1 Trusts and Foundations (or Equivalent)

4.2.1.1 Obligations of Businesses Establishing or Administering Trusts

During the course of establishing a trust relationship for which it is to act as trustee, the TCSP must, in order to identify and verify the identity of the *customer* and *beneficial owners*, identify:

(a) the *settlor*(s) or founder, including the initial *settlor(s) or founders* and any persons or *legal arrangements* subsequently settling *funds* into the trust;

(b) any *protector*(s), enforcer(s) and co-trustee(s);

(c) any beneficiary (whether his or her interest under the trust is vested, contingent or discretionary and whether that interest is held directly by that person or as the *beneficial owner* of a *legal person* or a *legal arrangement* that is a beneficiary of the trust), any class of beneficiaries and any other person who is likely to benefit from the trust; and

(d) any other natural person who exercises ultimate effective control over the trust.

Where the TCSP is establishing a *legal arrangement* other than a trust for which it is to act in a position equivalent to that of a trustee, the TCSP must identify those persons fulfilling positions equivalent to those set out above.

In identifying any person who is likely to benefit from the trust, the TCSP should seek to establish whether any documentation other than the trust deed, for example, a letter of wishes, identifies persons other than beneficiaries who are likely to benefit from the trust.

The information collected by the TCSP on the identity of these persons above must at a minimum include their full name and date of birth. The extent to which the other information is obtained by the TCSP will depend on the likelihood of that person benefiting from the trust, with such an assessment documented. All information on the identity of that natural person must be collected and the identity of that person verified by the TCSP prior to any distribution of trust or foundation assets. For the avoidance of doubt where a *legal person* or a *legal arrangement* has been identified as "any other person" the TCSP must apply this rule to its *beneficial owner/s*.

4.2.1.2 **Obligations when Dealing with Trusts or Other Legal Arrangements**

Where a trust is a *key principal* to a *business relationship* or *occasional transaction*, the TCSP must:

(a) identify and verify the identity of the trust (or take reasonable measures to do so, including without limitation:
- (i) the full name;
- (ii) any official identification number (for example, a tax identification number or registered charity or NPO number, where relevant); and
- (iii) the date and place of establishment of the trust;

(b) identify and take reasonable measures to verify the identity of the trustees of the trust;
(c) require the trustees (or equivalent) of the trust or other legal arrangement to provide the TCSP with details of the identities of the beneficial owners of the trust, including:
- (i) the settlor(s), including the initial settlor(s) and any persons or legal arrangements subsequently settling funds into the trust;
- (ii) any protector(s), enforcer(s) and co-trustee(s);
- (iii) any beneficiary (whether his or her interest under the trust is vested, contingent or discretionary and whether that interest is held directly by that person or as the beneficial owner of a legal person or a legal arrangement that is a beneficiary of the trust), any class of beneficiaries and any other person who to the best of the trustee's knowledge, is likely to benefit from the trust; and
- (iv) any other natural person who exercises ultimate effective control over the trust; and

(d) understand the ownership and control structure of the trust or other legal arrangement and the purpose and intended nature of the business relationship or occasional transaction.

When verifying the identity of the trust the TCSP does not need to obtain copies of the entire trust instrument (for example, trust deed or declaration of trust); obtaining copies of relevant extracts of such an instrument may suffice or, provided that the criteria set out in 4.2 above are met, by requesting the Trustee to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

Where the *business relationship* or *occasional transaction* has been assessed as high *risk*, the TCSP should obtain relevant extracts of the trust deed, deeds of amendments and letter(s) of wishes (as applicable).

4.2.1.3 **Verifying the Identity of the Beneficial Owners of Trusts or Other Legal Arrangements**

In relation to a trust the TCSP shall take measures to understand the ownership and control structure of the trust and identify and take reasonable measures to verify the identity of the *beneficial owner.*

In relation to a trust *beneficial owner* means:

(a) any beneficiary who is a natural person, whether his or her interest under the trust is vested, contingent or discretionary, and whether that interest is held directly by that person or as the beneficial owner of a legal person or legal arrangement that is a beneficiary of the trust;
(b) any trustee, settlor, protector or enforcer of the trust who is a natural person;
(c) if any trustee, settlor, protector or enforcer of the trust is a legal person or a legal arrangement, any natural person who is the beneficial owner of that legal person or legal arrangement;
(d) any natural person (other than a beneficiary, trustee, settlor, protector or enforcer of the trust), who has, under the trust deed of the trust or any similar document, power to:
- (i) appoint or remove any of the trust's trustees;
- (ii) direct the distribution of funds or assets of the trust;
- (iii) direct investment decisions of the trust;
- (iv) amend the trust deed; or
- (v) revoke the trust;

(e) where a legal person or legal arrangement holds any of the powers within subparagraph (d) (other than a trustee, settlor, protector or enforcer of the trust), any natural person who is a beneficial owner of that legal person or legal arrangement; and
(f) any other natural person who exercises ultimate effective control over the trust.

In the case of a *legal arrangement* other than a trust, *beneficial owner* means any natural person who is in a position in relation to that *legal arrangement* that is equivalent to the position of any natural person as set out above.

Other than where a *business relationship* or *occasional transaction* has been assessed as being high *risk*, the TCSP should take reasonable measures to verify the identity of any natural person who is a beneficiary of, or any other natural person who benefits from, the trust prior to any distribution of trust assets to (or on behalf of) that natural person.

Where a *business relationship* or *occasional transaction* has been assessed as being high *risk*, the TCSP should, where possible, take reasonable measures to verify the identity of all beneficiaries and other persons who are likely to benefit from the trust at the time that the assessment of *risk* is made. Where it is not possible to do so (for example, because the beneficiaries have not yet been born or are excluded) the reasons must be documented and retained on the relevant *customer's* file.

Many trusts established and administered are discretionary trusts.

Under a discretionary trust the beneficiaries have no right to any ascertainable part of the income or capital of the trust property. Rather, the trustees are vested with a power, which they are obliged to consider exercising, to pay the beneficiaries, or apply for their benefit, such part of the income or capital of the trust as the trustees think fit. Consequently, a beneficiary's interest in trust property is merely discretionary except to the extent that the trustee has decided to appoint a benefit to him or her.

*T*here are differences between the interests of beneficiaries under discretionary trusts, as well as those under *fixed trusts* whose interests have not yet arisen and who contingent beneficiaries are, therefore,. In this respect, other than in relation to high risk relationships mentioned above, the verification of the identity of a beneficiary will take place at the time that a distribution of trust assets or property occurs to, or on behalf of, that beneficiary.

Where the beneficiaries of a trust are designated by characteristics or by class, the TCSP must obtain sufficient information concerning the beneficiaries to *satisfy* itself that it will be able to identify, and verify the identity of, a beneficiary at the time of a distribution or when the beneficiary gains vested rights, for example, a beneficiary who is unaware of their beneficiary status until a point in time or a minor who reaches the age of majority.

The TCSP must take reasonable measures to verify the identity of those *beneficial owners* exercising control over the affairs of the trust, i.e. any *settlor(s)*, trustee(s), *protector(s)* and enforcer(s), including the *beneficial owners* of such entities where they are *legal persons* or *legal arrangements*, before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction*.

Verification of the *beneficial owners* of a trust must be undertaken either by the TCSP itself or, provided that the criteria set out in 4.2 above are met, by requesting the trustee to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

In taking measures to identify and reasonable measures to verify the identity of a *beneficial owner* of a corporate trustee, consideration should be given to the *ML* and *FT risk* associated with the ownership of the corporate trustee, whether it is appropriately regulated and the influence and/or control a particular *beneficial owner* of the corporate trustee has over the business and affairs of that corporate trustee in respect of the assets of the applicable trust.

Where the trustee or its parent is subject to the same or equivalent provisions of AML Law 1.362 in the jurisdiction from which its business is conducted and where it is supervised for compliance with those provisions, it may be possible to rely on information in the public domain or provided by the trustee regarding the identity of its *beneficial owners* and its directors or other controlling persons by way of a summary sheet and/or structure chart, without the need to gather *identification data* on those individuals. Such an approach would be consistent with the following guidance from the FATF's guidance paper on applying a risk-based approach for TCSPs detailed below:

"Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, the TCSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A TCSP can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body which regulates the trustee and of the regulated trustee itself)."

In making this determination, the TCSP should take note of reports and assessments by the FATF and/or FATF-style regional bodies, in particular of findings, recommendations and ratings of compliance with FATF Recommendation 28 or precursor recommendation which assesses the adequacy of supervision of trustees and document the conclusions of its assessment.

Where neither the trustee nor its parent is based in a jurisdiction with equivalent provisions of *AML Law 1362* in the jurisdiction from which its business is conducted and where it is supervised for compliance with those provisions, reasonable measures to verify the identity of the *beneficial owners* of the corporate trustee will be required. This will involve the collection of *identification data* on those *beneficial owners*, together with evidence of their ownership, for example, via *copies of the share register of the corporate trustee or regulatory returns.*

4.2.1.4 **Obligations of Businesses Establishing or Administering Foundations**

During the course of establishing or administering a *foundation* relationship, the TCSP must, in order to identify and verify the identity of the *customer* and *beneficial owners*, identify:

(a) the *founder*(s), including the initial *founder(s)* and any persons or *legal arrangements* subsequently endowing the *foundation*;
(b) all councillors;
(c) any guardian(s);
(d) any *beneficial owner*, including any default recipient; and
(e) any other natural person who exercises ultimate effective control over the *foundation*.

4.2.1.5 **Obligations when Dealing with Foundations**

Where a *foundation* is a *key principal* to a *business relationship* or *occasional transaction*, the TCSP must:

(a) identify and verify the identity of the foundation (or take reasonable measures to do so), including without limitation:
- (i) the full name;
- (ii) the legal status of the foundation;
- (iii) any official identification number (for example, a registered number, tax identification number or registered charity or NPO number, where relevant);
- (iv) the date and country or territory of establishment/registration; and
- (v) the registered office address and principal place of operation/administration (where different from the registered office);

(b) identify and verify the identity of any registered agent of the foundation, other than where the agent is a transparent legal person;
(c) identify the following:
(i) the founder(s), including the initial founder(s) and any persons or legal arrangements subsequently endowing the foundation;
- (ii) all councillors;
- (iii) any guardian(s);
- (iv) any beneficial owner, including any default recipient; and
- (v) any other natural person who exercises ultimate effective control over the foundation; and

(d) understand the ownership and control structure of the foundation and the purpose and intended nature of the business relationship or occasional transaction.

The following non-exhaustive list provides examples of *documents* considered suitable to verify one or more aspect of the identity of a *foundation*:

(a) a copy of the Certificate of Registration;
(b) a registry search, if applicable, including confirmation that the foundation has not been, and is not in the process of being, dissolved, struck off, wound up or terminated;
(c) a copy of the latest audited financial statements;
(d) a copy of the Charter; and/or
(e) a copy of the Council Resolution authorising the opening of the account and recording account signatories.

Verification of the identity of the *beneficial owners* of a *foundation* must be undertaken either by the TCSP itself or, provided that the criteria set out in 4.2 above are met, by requesting the registered agent, where one has been appointed, to provide the relevant information on the identity of such parties by way of a certificate or summary sheet.

4.2.1.6 **Verifying the Identity of the Beneficial Owners of Foundations**

A person has control of a *foundation* through ownership if that person holds, directly or indirectly, any of the following:

(a) an interest equivalent to a shareholding of more than 25% including but not limited to an entitlement to more than 25% of the assets of the foundation in the event of its winding up or dissolution;
(b) more than 25% of the voting rights in the conduct or management of the foundation;
(c) the right to appoint or remove a majority of the managing officials of the foundation holding a majority of voting rights on all or substantially all matters at meetings of the foundation that are equivalent to board meetings;
(d) a vested beneficial interest or future entitlement to benefit from more than 25% of the assets of the foundation.

Other than where a *business relationship* or *occasional transaction* has been assessed as high *risk*, the TCSP must take reasonable measures to verify the identity of any natural person above prior to any distribution of *foundation* assets to (or on behalf of) that natural person.

Where a *business relationship* has been assessed as being high *risk*, the TCSP must, where possible, take reasonable measures to verify the identity of any natural person falling within above at the time that the assessment of *risk* is made. Where it is not possible to do so (for example, because that person has not been born or is disenfranchised) the reasons must be documented and retained on the relevant *customer's* file.

The TCSP must take reasonable measures to verify the identity of those parties identified other than the *beneficial owners* (for example, the *founder*(s), *foundation official*(s), councillors, guardian(s) and any other person(s) with ultimate effective control over the *foundation* (including the *beneficial owners* of such entities where they are *legal persons* or *legal arrangements*)) before or during the course of establishing a *business relationship* or before carrying out an *occasional transaction*.

Regardless of form, where the TCSP identifies that a *founder* is acting on behalf of another person, i.e. as a nominee *founder*, the TCSP must identify and take reasonable measures to verify the identity of the true economic *founder*.

The persons falling within 4.2.1.6. (d) above will depend on the specific circumstances of the *foundation*. However, this will generally include individuals who under the terms of the official documents of the *foundation* have a future entitlement to a substantial benefit from the *foundation*. As a matter of practice and policy, this will generally mean an entitlement to a benefit which in the hands of an individual recipient equates to more than 25% of the total assets of the *foundation*. In other words, it is not intended that, where a *foundation's* official documents anticipate the provision of benefits to a potentially large group, (for example, by providing *funds* to supply food to the inhabitants of a flooded village) members of that group should be treated as *beneficial owners*.

4.2.2 **Protected Cell Companies**

A protected cell company ("PCC") is a single legal entity with one board of directors and one set of memorandum and articles of incorporation. A PCC can create an unlimited number of protected cells ("PCs"), the assets and liabilities of which are separate from those of the PCC (with the assets of the latter referred to as "non-cellular" or "core"). Importantly, the PCs are not separate legal entities and therefore cannot transact as such.

A PCC can be a newly incorporated entity or alternatively an existing company can be converted to a PCC. A PCC may create any number of PCs, the assets and liabilities of which are segregated from the non-cellular assets of the PCC and from the assets and liabilities of other PCs. However, a PC may not own shares in its own PCC or another PC of the same PCC.

Where a PCC is a *key principal* to a *business relationship* or *occasional transaction*, the TCSP must apply *CDD* measures to both the core and the relevant PC(s), including the *beneficial* owners of such, in accordance with the requirements for legal persons.

4.2.3 Limited Partnerships and Limited Liability Partnerships

An LP is a form of partnership with or without legal personality at the election of the General Partner (GP). Its members include one or more GP, who has actual authority over the LP, for example to bind the LP in contracts with third parties, and is liable for all debts of the LP, and one or more limited partner who contributes (or agrees to contribute) to the capital of the LP and who (subject to certain provisions) is not liable for the debts of the LP.

A Limited Liability Partnership ("LLP") is a body corporate with legal personality separate from that of its members and is therefore liable for its own debts. As a consequence of this legal personality, LLPs established must usually be registered and therefore public records exist similar to those for *legal persons*. With regard to the members of an LLP, there must be at least two who, unless otherwise stipulated within the members' agreement, may take part in the conduct and management of the LLP and are entitled to share equally in the profits of the LLP.

Where an LP or LLP is a key principal to a business relationship or occasional transaction, the TCSP must identify, and verify the identity of, that LP/LLP or take reasonable measures to do so.

4.3 Reliance

4.3.1 Scope

TCSPs are allowed to rely on the CDD measures carried out by other subject persons or certain third parties subject to a number of conditions stipulating which elements of due diligence may be relied on, which entities may and may not be relied on, the circumstances under which a TCSP may not place reliance, and the requirement to enter into a reliance agreement.

TCSPs are authorised to have certain obligations of AML Law 1362 carried out by a third party, being:

Article 4-1
(1°) to identify the customer, the authorised representative and, if applicable, the beneficial owner;
(2°) to check these identification details by means of a supporting document bearing their photograph)

Article 4-3
to obtain the customer's socio-economic background and the following characteristics of the business relationship:
- regularity or duration;
- purpose;
- nature of the business relationship;
- foreseeable volume of transactions conducted).

The third party concerned must satisfy the following conditions:

- the third party must have fulfilled his own duty of due diligence;
- the third party must be a person or organisation specified in points 1°) to 3°), 6°), 12°), 13°) or 20°) of Article 1, or in 3°) of Article 2, operating in the Principality or in the territory of a State whose legislation includes provisions considered equivalent to those of this Act and having their compliance with these obligations supervised, and which does not appear on the list of high-risk States and territories specified in Article 14-1;
- the person or organisation relying on a third party must have access to information, a copy of the identification details, and other due diligence documents gathered by the third party in the manner provided for by Sovereign Ordinance.
Ultimate responsibility for compliance with the obligations laid down in Articles 4-1 and 4-3 remains with the organisations and persons relying on third parties.

4.3.2 Carrying Out Reliance

When placing reliance, a TCSP must immediately obtain the information required by the above Articles, before carrying out the occasional transaction or entering into a business relationship.

For the application of these provisions, the third party who implements the due diligence obligations, shall immediately make available to the TCSP the identification details relating to the identity of the customer and, where applicable, the beneficial owner, and to the purpose and nature of the business relationship.

Upon first request, the third party shall send them a copy of the customer's identification documents and, where applicable, those of the beneficial owner, as well as any document relevant to the due diligence, including adequate copies of identification and verification data obtained through the use of remote identification means.

4.3.3 The Reliance Agreement

TCSPs are at all times expected to be able to respond to any requests for information from SICCFIN/AMSF, regardless of whether the TCSP has placed reliance or otherwise. This means that the TCSP needs to be able to retrieve documents in a timely manner so as to comply with such requests. In fact, rules on reliance require TCSPs to take adequate steps to ensure that the entity relied upon immediately forwards relevant information and copies of documents. To this effect, TCSPs must enter into a written formal agreement with the entity being relied upon, to regulate the procedures and conditions on such requests.

The procedures for transmitting the above-mentioned information and documents, as well as the procedures for monitoring the due diligence measures implemented by the third party, are specified in a written contract between the TCSP and the third party.

The intervention of a third party is subject to the following conditions:

- the TCSP verifies in advance that the third party meets the conditions set out in the Law, and keeps the documentation on which he has based his decision;

- the third party undertakes in writing, prior to entering into a relationship, to provide the TCSP with information identifying the customers or beneficial owners he will identify, as well as a copy of the documents by means of which he will have verified their identity; including, where applicable, data obtained through the use of remote identification means;

- the TCSP must be able to make the declarations provided for in Chapter V of the AML law no. 1.362, and to respond to requests from SICCFIN/AMSF;

- there must be no contractual outsourcing or agency relationship between the TCSP and the third party; otherwise, the outsourced service provider or agent is considered part of the TCSP.

It is the TCSP's responsibility to check that the identification of the customer or the beneficial owner and the verification of their identity have been fully and correctly carried out by the third party in accordance with the legislation applicable to them.

It is the TCSP's responsibility to carry out, if necessary, any additional identification and verification, and where appropriate to re-identify and re-verify the identity of the customer or beneficial owner.

TCSPs should also consider testing the reliance agreement to ensure that the entity can be relied upon consistently. This can be done by requesting information and documents from time-to-time from the entity being relied upon. Through such testing, the TCSP can ensure that the entity does indeed provide information and documentation in a timely manner and provides insight on the whether the due diligence measures conducted by it are satisfactory (e.g.: whether the entity is collecting the right documents and whether CDD updated through ongoing monitoring). This is important as TCSPs remain ultimately responsible for compliance with their AML/CFT obligations.

4.4 Purpose and intended nature, and establishing the customer's business and risk profile

This section provides further guidance and explanation to assist TCSPs to adhere to their obligations under AML Law 1362, which are further explained in the *Generic Guidelines*. In terms of the AML Law 1362 and related Ordinances TCSPs are required to:

- assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship; and
- establish their customer's business and risk profile.

When TCSPs are requested to incorporate a company or establish a commercial partnership, they are typically approached by the prospective shareholders, partners or UBOs of that prospective company or commercial partnership, or by Intermediaries. In addition to formation services, TCSPs may also be requested to provide additional services once that company, trust, foundation or partnership is established. These could include providing (or arranging for the provision of), a registered office or a directorship/s, trustee services, corporate secretarial and or accounting services, among others.

Initially, therefore, the TCSP's customer would typically be the prospective shareholder/s or UBO/s of that prospective company or entity (who may or may not be represented by Intermediaries or other persons) and the TCSP ought to identify and verify the identity of that individual or entity and, in the case of a legal entity or arrangement, its UBO/s, and also adhere to the other obligations envisaged by AML Law 1362, as further explained in the *Generic Guidelines*.

TCSPs who are requested to provide the above services to entities which the TCSP itself incorporates or which are already incorporated, would be establishing a business relationship (see the Table above under Section 3.3.4 – 'The Customer'), since these services are offered over a span of time and hence denote an element of duration. Accordingly, these TCSPs are required to assess, and, as appropriate, obtain information on the purpose and intended nature of the business relationship being established.

Information that would be relevant in this context would include the following:

4.4.1 Information on the rationale

The rationale for the setting up of entity in the particular jurisdiction, and the reason for using a Monaco based TCSP and/or for the provision of the requested service/s. Is there a legitimate and economic/business rationale for the company, trust, foundation or partnership being set up or serviced? When, for example, such an entity forms part of a larger group of companies, it is important for the TCSP to understand the entity's purpose within the larger group (e.g., a conglomerate business in which the different business streams are set out under different companies). This would also involve gathering information on the commercial/trading activities pursued by the larger group or sub-group that owns the relevant entity.

When the entity is set up to hold shares in another company, the TCSP should also seek to understand the rationale for that set-up. This approach is important to ensure that multi-tier and/or complex structures are not being purposely set up to conceal ill-gotten gains and to create obstacles to the tracing of these gains.

Assessing the purpose behind the setting up of the company, partnership, trust, foundation or other legal entity is especially relevant when non-residents are UBOs of companies or partnerships set up or being set up by the TCSP in Monaco. TCSPs should also be particularly vigilant when they assist Monaco residents to set up companies or legal entities outside Monaco, or when they provide other services to these companies or legal entities. The TCSP should consider whether the structure is being used by a Monaco resident to avoid the obligation to obtain a Monaco business licence when the commercial activity continues to be undertaken from Monaco. When providing this assistance or these services, either directly through, for example, the drafting of incorporation documents (e.g., Memoranda & Articles of Association or other constitutive documents), or indirectly through liaising and representing the customer with foreign TCSPs, the Monaco TCSP should question and understand the rationale behind the setting up of that company or other legal entity outside of Monaco;

4.4.2 Information on the activity or purpose

Information on the activity or purpose that the company, trust, foundation, partnership or other legal entity will be carrying out or serving would involve understanding the trading/commercial activity that is to be carried out by the company. When the entity is not set up to carry out a commercial/trading activity but rather to hold assets (e.g., a shareholding in another entity, or real estate ownership), it would not suffice to simply determine the purpose of that entity, which may be quite self-evident from the nature of the company itself (i.e., to hold shares in a subsidiary company or companies).

The TCSP providing services to that company would be expected to understand and gather information on the trading/

commercial activity carried out directly by the holding company's subsidiary or subsidiaries (where these are trading companies), or indirectly by subsidiaries of these subsidiaries in the ownership chain. It is only by doing so that the TCSP would be able to get a holistic understanding of what purpose or activity the holding company will be linked to;

4.4.3 **The profile of the shareholders or beneficial owners**

The TCSP is expected to assess whether this profile tallies with the company, trust, foundation or partnership or other legal entity activity or purpose. Do these individuals have experience in the area of business that the company will be trading or involved in? For example, in the case of a company that will be providing consultancy services, do any of the parties involved have technical expertise in the area in relation to which the company will be providing consultancy?

4.4.4 **The value of share capital or assets of that company or entity**

TCSPs are expected to obtain information on the value of the share capital or assets, and, depending on the ML/FT-C risks identified, obtain documentation evidencing the source of funds and/or assets forming the capital of the company or partnership. These checks would entail gathering information on the source of wealth of the shareholder or UBO who contributes to the company's capital.

This would be, for instance, information on employment or business activity, including information on salary in the case of individuals in employment, or business income in case of corporate shareholders or individuals whose wealth is derived from business or commercial activities. Private companies in many jurisdictions can be incorporated with a very low minimum share capital. In these cases, TCSPs are not expected to obtain extensive information or to obtain documentation to substantiate the source of that minimum share capital, and it would suffice for the TCSP to simply identify the employment or business activity of the shareholder/UBO contributing to that share capital.

TCSPs should, however, seek to establish how the company will continue to be financed, including whether any other capital injections are projected once the company is incorporated. Together, these measures would allow the TCSP to place more focus on effective monitoring of the company's activities once it starts to operate.

4.4.5 **Ongoing monitoring of transactions**

TCSPs who provide (or arrange for the ongoing provision of) directorship, trustee, foundation services or act as partners in commercial partnerships, and who would be empowered to legally represent and bind the company or entity, are expected to carry out ongoing monitoring of the transactions that the entity undertakes, as is explained in the Generic Guidelines. When providing these services, TCSPs should obtain information on the anticipated level of the activity that is to be undertaken through the relationship (e.g., expected volume of transactional activity, projected turnover, proposed suppliers and customers) in order to understand the eventual source of funds flowing through the company.

This information is necessary for the TCSP to be able to formulate an understanding of the typical transactional activity that is expected from that entity. This understanding is crucial to enable it to carry out effective ongoing monitoring of the companies' or entities' activities and transactions.

Naturally, the extent of the scrutiny as well as information and documentation to be gathered will vary according to the ML/FT-C risks connected with that particular business relationship.

4.5 Providing Company, Trust, Foundation and other legal entity formation services

When the TCSP would be providing solely company, partnership, trust, foundation or other legal entity formation services, without any additional ongoing services, the TCSP would be carrying out an occasional transaction and not establishing a business relationship, since the TCSP's services will end with the setting up of the company.

This notwithstanding, TCSPs are still expected to understand and, as appropriate, obtain information on the intended purpose of the company or other legal entity being set up. TCSPs are expected to ensure that their services are not misused for the setting up of an entity intended to facilitate the laundering of proceeds of crime or the financing of terrorism. This not only exposes them to reputational risks and the risk of being involved in criminal acts, but undermines the reputability of Monaco and its financial and business sectors.

TCSPs should, therefore, carry out the risk assessment and obtain information relating to the rationale for the entity, its intended activity/purpose, and the coherence of the UBO profile with the nature of the entity envisaged since this is the only way in which the risk of being involved in an ML/FT-C set-up could be mitigated. As explained earlier, when private companies are incorporated with low value share capital, the due diligence to be carried out with respect to the source of the funds of that capital would be simplified, and TCSPs should seek to understand how the company will continue to be financed and whether any other capital injections are projected.

TCSPs who would only be forming the company, partnership, trust, foundation or other legal entity and providing no additional services that will lead to the establishment of a business relationship, would not be required to monitor the company's activities once it starts to operate. Apart from gathering information on the employment or business activity of the shareholder/UBO as explained above, it is important for these TCSPs to carry out open source checks on the individuals involved in the company or partnership (i.e., directors, partners, shareholders and UBOs) or make use of commercial databases to ascertain that there is no adverse information that might link these individuals to criminal activities or participation in criminal organisations.

4.6 Network firms and Groups

4.6.1 Network firms

TCSPs may be part of an international member network or group of correspondent firms. These networks aim to facilitate cross-border transactions for the customers of network firms.

The level of due diligence required by a TCSP depends on whether they directly communicate with and provide services to the customers of the network firm or if they continue to correspond through or provide services to the network firm. If a foreign network firm simply refers a customer to a local correspondent firm without remaining involved in the relationship, the foreign network firm is considered an introducer, and no due diligence is required on them. However, the TCSP may still wish to assess the reputation of the foreign network firm for any potential links to money laundering, terrorist financing, or proceeds of crime.

If the foreign network firm remains involved in the provision of the service by assisting or liaising in communication, they are considered an intermediary. In such cases, TCSPs need to apply due diligence measures for foreign network firms.

In situations where the TCSP provides a service to a foreign network firm but the engagement with the customer remains with the foreign network firm, the TCSP is considered to have a business relationship/occasional transaction with the foreign network firm, not the firm's customer. The TCSP is expected to report directly to the foreign network firm and provide services accordingly.

If a firm belongs to a network that shares common standards and quality-control policies with other network firms, the customer due diligence can be limited to identifying the network firm, obtaining its official name, registration number, date

of incorporation/registration, and registered office or principal place of business address. Additionally, identifying the Chief Executive Officer, managing partner, or equivalent position in the network firm is necessary. The TCSP can gather this information from the network firm or through their portal, and they need to retain evidence of conducting this check.

However, the TCSP still has an obligation to request and consider necessary information and documentation to understand the purpose of the transaction and mitigate associated risks. If necessary, they should file an STR.

4.6.2 Groups and subsidiaries

TCSPs established on the territory of the Principality and belonging to a group whose parent company is established in the Principality or in a State whose legislation includes provisions deemed equivalent to Monegasque law, in particular with regard to professional secrecy and the protection of personal information, and which are subject to supervision for compliance with these obligations, shall transmit to the companies in the same group the information necessary for the organization of the fight against money laundering and the financing of terrorism, in accordance with the procedures laid down by Sovereign Order.

The TCSP's internal procedures define how information required to combat money laundering and the financing of terrorism is circulated within the Group.

The TCSP shall require its branches and subsidiaries established abroad, in which they hold a majority shareholding, to apply measures equivalent to those provided for in Monaco AML Law with regard to customer due diligence, the sharing and retention of information and the protection of personal information.

Where the law of the State in whose territory their branches or subsidiaries are located does not allow them to implement measures equivalent to those provided for in the present law, they shall ensure that their branches and subsidiaries apply specific due diligence measures.

4.7 Establishing the Source of Wealth and Source of Funds

Part of the information required to understand the purpose and intended nature of the business relationship or of an occasional transaction is information on the source of the customer's wealth and the source of funds to be used throughout the relationship or to fund an occasional transaction. In addition to helping with the establishment of the business and risk profile of the customer, information on the source of wealth and/or funds, supported by documentation where necessary, is also essential to ensure that the customer's wealth and any funds to be used have been generated legitimately, and will also allow the TCSP to conduct meaningful ongoing monitoring and detect unusual or suspicious transactions.

The source of wealth is the economic activity or activities that generate the customer's wealth. By way of example, the source of wealth may be comprised of income through employment, business, or inheritance in the case of a natural person, revenue or share capital in the case of a company, and donations or endowments in the case of a foundation. The term 'source of funds' is then defined as '*the activity, event, business, occupation or employment generating the funds used in a particular transaction, or to be used in future transactions*'. The Generic Guidelines provide more guidance on establishing the source of wealth and source of funds, and are to be read in conjunction with the following sections which provide sector-specific guidance and examples on the application of this requirement.

4.7.1 Source of Wealth

The overarching principle when understanding the source of wealth of a customer is to form a reasonable conclusion that the customer's wealth has been accumulated legally. In this regard, the measures taken may be varied depending on the level of ML/FT-C risk posed by the relationship and by the nature of the risks.

When establishing the source of wealth of customers that are legal entities, TCSPs may request and refer to recent financial statements prepared by the customer, paying particular attention to the statement of financial position, statement of cash flows and related notes. Legal entities may be financed through various means, including equity, retained earnings, other reserves, third party debt, shareholders and related party debt, and working capital. TCSPs should seek to understand these elements and their contribution to the source of wealth of the company. When doing so, TCSPs may request the customer to provide additional information such as financial statements from previous years and details on any shareholders' loans.

Where the entity has only recently been established and is not able to provide such information, the TCSP's role is to understand how the legal person will be financed, and then determine the source of such funds and the source of wealth of any persons making any significant capital injections or financial contributions.

4.7.2 Source of Funds

The purpose behind the requirement to establish the source of funds is to ensure that funds used throughout the duration of the relationship are legitimate and that transactions are conducted in line with the customer's profile. In requesting information and, where necessary, documentation on the expected source of funds, TCSPs may, on a risk-sensitive basis, consider the following:

a) volume and frequency of expected cash inflow and outflows; geographical distribution of main money flows;
b) details of major customers and suppliers;
c) details on expected funding through borrowings (related party or third party);
d) source of initial equity funding and related entity debt financing (where applicable).

Throughout the duration of the business relationship, TCSPs are not expected to understand or request the source of funds of every transaction. However, when activities or transactions appear to be unusual, or not in line with what is known about the customer, or represent a new source of funding, when assessed on both materiality and risk, information and any supporting documentation on the actual source of funds used to finance the unusual activity or transaction should be collected. This will lead the TCSP to determine whether the funds were derived from a legitimate source.

The following are examples of sources of funds which attract higher ML/FT-C risks:

a) the use of crowdfunding to raise capital;
b) assets denominated in virtual currencies;
c) funds raised through initial coin offerings or security token offerings;
d) debt with related entities, if they are incorporated in high-risk or non-reputable jurisdictions, especially without a legitimate reason;
e) debt from parties which are not related to the customer, and that are not licensed credit/financial institutions.

Within certain business activities, it may be normal for customers to conduct high and very high value transactions, and the customer's risk profile would indicate that such values of transactions are indeed in line with their business. In these cases, TCSPs should still request substantiating documentation from time to time so that they may continue ensuring that the transactions are indeed related to the business activity.

4.7.3 Source of Wealth of Beneficial Owners

The requirement to understand the source of wealth of the customer should not always be interpreted as requiring the TCSP to obtain information on the source of wealth of the beneficial owner(s).

For example the TSCP would not be expected to verify the Source of Wealth of UBOs of Trusts or Foundations who do

not introduce funds into the relevant entity. This would for example concern Protectors/Enforcers, Trustees and Beneficiaries.

Information on the wealth of the beneficial owner(s) would be relevant when, while obtaining information on the purpose and intended nature of the business relationship, or at any time during the provision of the service or prior to conducting an occasional transaction, it is noted that the customer's funds or wealth have been or will be provided or contributed by the beneficial owner(s). In these cases, TCSPs will need to obtain information on their source of wealth/funds to establish that they have been derived legitimately.

Examples of such instances include:

a) Where the capital is provided by the beneficial owner and the amount is substantial;
b) Where the capital or funding of the company does not appear to be sufficient (e.g.: in the cases where the company has been set up with minimal or very low share capital). In such cases the TCSP should ask and understand how the company will be operating and whether there will be capital increases. It should also establish how these funds will be provided by the beneficial owner, as well as the source of said funds;
c) With respect to trusts and foundations, if these are being serviced at a stage where assets are still to be placed or the foundation is not yet generating the funds needed to support its activities, TCSPs should establish where the assets will come from and establish the source of funds of persons making any significant settlements or endowments;
d) On an ongoing basis whenever significant assets or funds are placed or settled.

A contribution is significant when the value is high compared to that person's salary or income.

The above also applies in the case of shareholders, settlors (when the customer is a trust), founders (when the customer is a foundation) and other persons with a similar role. TCSPs should obtain information and, where applicable, documentation on the source of the funds and the source of wealth of the third parties.

This applies equally in the case of other non-related third parties providing or lending assets into the company or entity (unless these are licensed credit or financial institutions). In such cases, the TCSP must understand the connection between the third party and the company. Where the connection is not apparent or there does not appear to be any economic or business rationale behind the arrangement, TCSPs should request additional information and/or documents to understand the purpose and the source of the fund. In case of suspicion of ML/FT-C or proceeds of crime, TCSPs must report to SICCFIN/AMSF.

4.7.4 **Extent of Information and Documentation**

The extent and level of detail of the information required on the source of wealth and the expected source of funds, and whether and how much documentation should be requested to substantiate the information provided by the customer, would depend on the outcome of the CRA and the risks highlighted by it. In cases of lower risk, or where it emerges from the CRA that the ML/FT-C risk is not driven by the source of funds (e.g. the source would be a ML/FT-C risk if the value of funds to be used is significant, if there is PEP involvement, or there are connections with high-risk jurisdictions), it would suffice to obtain information by way of a declaration from the customer. In higher risk scenarios, enhanced measures would need to be taken, which would include substantiating the information with documentation provided by the customer and/or information from open sources.

Ultimately TCSPs need to reasonably conclude on the legitimacy of the source of wealth and funds. Measures undertaken should be commensurate with risk and TCSPs should be mindful of taking measures that are excessive, disproportionate, or irrelevant when considering the ML/FT-C risks involved.

4.8 Ongoing Monitoring

Effective ongoing monitoring is vital to understand customers' activities and is an integral part of effective AML/CFT systems and controls. It helps TCSPs to update their knowledge of their customers and detect unusual or suspicious transactions/activities.

The purpose of the first aspect of ongoing monitoring (i.e., monitoring of activities and, in some instances, the transactions being undertaken) enables the TCSP to:

a) identify transactions and/or activities that are not in keeping with the corporate customer's operations and business for further examination and scrutiny by the TCSP;
b) generate internal reports on unusual/dubious transactions or activities to be reviewed by the TCSP's MLRO; and
c) ensure that suspicions of ML/FT-C or proceeds of crime are reported to SICCFIN/AMSF in a timely manner, as required by law.

Business relationships are subject to customer due diligence procedures throughout their duration, in the form of ongoing monitoring obligations. The requirement to conduct ongoing monitoring is comprised of two key elements:

a) the scrutiny of transactions or activities being undertaken by the TCSP's customers (companies, trusts, foundations etc) to ensure that these transactions are in line with the TCSP's knowledge and understanding of that customer, in particular its business and operations; and
b) ensuring that the data, documents and information obtained as part of the CDD process (i.e., identification and verification information, as well as information gathered on the purpose and intended nature of the business relationship and the customer's business and risk profile) are kept up to date.

4.8.1 **Scrutiny of transactions**

The scrutiny of transactions through transaction monitoring during the relationship requires TCSPs to use their knowledge of the customer (including the information gathered on the purpose and intended nature of the business relationship and the business and risk profile) to identify transactions that are unusual or subject to sanctions (see Section 6 below). A transaction can be 'unusual' by its nature, because it is suspicious, illogical, unnecessarily complex, or unreasonable. A transaction may also be unusual when taking into consideration what one knows about a given customer, for instance because it is inconsistent with the customer's profile or is significantly different to the customer's usual activity or transactions.

Scrutiny of transactions should not only be restricted to the movement of funds, but should also include consideration of the movement of other value, such as the transfer of shares, rights or the assignment of debt.

AML Law 1362 imposes a specific requirement to examine the purpose and background of transactions that are complex, unusually large, conducted in an unusual pattern, or have no economic or lawful purpose, and to prepare an internal report to evidence this examination.

There is also a requirement to examine and prepare an internal report ("Examen Particulier") on all transactions that have a connection with jurisdictions considered by Monaco to be high risk and listed by Ministerial decision from to time.

An unusual transaction is not automatically deemed to be suspicious but should, however, serve as a red flag or trigger for TCSPs to assess the situation and undertake measures to establish whether that transaction is suspicious and ought to be reported, or whether there are legitimate explanations for the unusual transaction.

For the purpose of identifying unusual customer transactions or activities, TCSPs should take into consideration a number of aspects, including:

a) the nature and type of individual transactions or a series of transactions (i.e., the purpose of the transaction/s – e.g., a transaction linked to a sale of goods), and the manner in which the transaction is conducted (e.g., bank transfer or cash payment);
b) the value of the transactions, paying special attention to particularly substantial transactions;
c) unusual changes or increases in a customer's activities or turnover;
d) unusual changes in the nature of a customer's transactions or activities;
e) the detection of certain ML/FT-C typologies;
f) the geographical origin/destination of a payment; and
g) the customer's usual pattern of activities or turnover.

Measures that can be undertaken to assess an unusual transaction include:

a. Assessing the customer's profile to understand whether the flagged transaction makes sense in line with the known source of wealth, source of funds and business activities;
b. Conducting searches on open sources to verify aspects of a transaction, such as the existence of any parties mentioned in an invoice;
c. Asking the customer about any new operational activities that have given rise to changes in transactional behavior;
d. Requesting information on the transaction, such as the purpose of the transaction and/or the source of funds used or to be used to finance the transaction;
e. Requesting documentation to substantiate the transaction and/or the source of funds used or to be used to finance that transaction.

A non-exhaustive list of red flags which might indicate a suspicious transaction is included in Annex 2. In addition to these red flags, TCSPs should be wary of certain indicators within trade documents, such as invoices and contracts, provided by the customer. Such documents may contain certain defects, irregularities or features that should cause the TCSP to question further and assess whether there is cause for suspicion or knowledge of ML/FT-C:

a. invoices for large sums with generic descriptions (e.g.: € 200,000 for 'consultancy services' without additional information or without a breakdown of what the sum consists of);
b. recurring invoices for services without a contract or agreement regulating such services;
c. large value contracts for services without commencement dates or service periods;
d. inconsistencies between the name or address of the seller/exporter and the person or entity receiving the payment;
e. contracts that do not make business sense (e.g.: contract for tax, commercial and administrative support spanning only a few months);
f. contracts for goods or services the value of which appears to be highly inflated (or deflated) when compared to the expected market value or what is usually charged;
g. incorrect or missing details (e.g.: incorrect VAT and registration numbers).

TCSPs are not expected to scrutinise each and every invoice or contract of the customer. However, when such defective documents are provided to justify or substantiate a given transaction, particularly one flagged by the TCSP itself, close attention should be given that there is already a degree of doubt or concern at that stage. These documents may be indicative of false transactions either to layer or structure funds or as part of a wider trade-based money laundering scheme.

Ultimately, the purpose behind scrutinising transactions is to ensure that the transaction and the source of funds used are not connected to ML/FT-C or proceeds of crime. The type and extent of measures taken to scrutinise transactions should be risk-based and should provide the TCSP with a reasonable level of comfort that the transaction is legitimate. In cases of knowledge or suspicion of ML/FT-C or proceeds of crime, TCSPs must submit a report to SICCFIN/AMSF.

Not all unusual transactions will give rise to suspicions, as there may be legitimate reasons for the flagged activity. Sometimes, an assessment of an unusual transaction will lead the TCSP to identify important changes in the customer's profile, such as a significant change or expansion in the business activity. In this case, TCSPs should ensure that the customer due diligence and the customer profile are up to date and should also assess the existing CRA to determine whether it needs to be updated.

Note:

- Ongoing monitoring should be adapted for the risk profile of the customer.
- Verification of source of funds and counterparties should not only cover ingoing and outgoing flow of funds, but should also be undertaken on the movement of value, such as transfers of shares or other non-financial assets, loan assignments, additional settled funds for example.
- From time-to-time AMPA forwards to its members requests from the Sureté Publique for information "Commissions Rogatoires" which should be responded to promptly within the given timeframe.

4.8.2 Transactions falling outside the Scope of 'Relevant Activity'

TCSPs can provide a range of services to any one customer, some of which from time to time may fall outside the definition of the activity of TCSPs in Article 1(6) of AML Law 1.362 ('relevant activity') and hence would not require the application of AML/CFT measures if undertaken by another business (eg translation services, or CRS reporting). However, the knowledge gained on the customer through the provision of these services should not be excluded or ignored from the TCSP's overall knowledge of the customer. For instance, in cases where the TCSP comes across information that gives rise to suspicion of ML/FT-C while providing services falling outside the scope of 'relevant activity', the information cannot be ignored. TCSPs should seek to understand how this information impacts the relationship and the risk of ML/FT-C, and should they have suspicion or knowledge of ML/FT-C, they should still report this to SICCFIN/AMSF.

4.8.3 Ensuring that the Documents, Data, or Information held by the TCSP are kept up to date

The second aspect of a TCSP's ongoing monitoring requirement is to ensure that the documents, data, or information held on the customer are kept up to date. A TCSP's knowledge of the customer and its business activities continues to develop throughout the duration of the relationship. Through this requirement, customer information, including due diligence and the risk profile are reviewed and updated, so that they continue to reflect the current circumstances surrounding the customer and their activity. This requirement is also essential to ensure that the level and extent of due diligence being carried out continues to mitigate the actual risks posed by the relationship, since such measures would have been based on the information obtained on the customer prior to onboarding.

The ongoing monitoring process also allows TCSPs to determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the TCSP's risk appetite and, if so, understand whether the level of due diligence and mitigating measures in place need to be adjusted in view of any changes from the initial risk understanding.

The need to update CDD information should be considered at appropriate times, following a risk-based approach. Reviews may be conducted periodically, with the frequency depending on the ML/FT-C risk of the business relationship, based on trigger events, or a combination of both periodic and trigger events.

4.8.4 **Periodic reviews**

The AML Law 1362/Generic Guidelines and this document do not prescribe a specific frequency for carrying out ***periodic reviews***. However, these must be risk-based, with higher risk relationships being subjected to enhanced ongoing monitoring procedures which entail more frequent reviews.

4.8.5 **Trigger events**

Potential events that may trigger the need to review and update due diligence and risk profile information (**trigger events**) include:

a. At the start of and when planning for recurring engagements;
a. When requesting to provide a new service to the customer that would impact the risk of the relationship or which changes or presents a new risk factor in terms of the CRA;
b. When a previously suspended engagement starts again;
c. Whenever there is a change of control and/or ownership of the customer;
d. Whenever there is a significant change to key office holders;
e. When there is a material change in the level, type, or conduct of business (e.g. a change in the industry or jurisdictions in which the customer operates). The monitoring and assessment of transactions undertaken by the corporate customer may indicate a change in, or the venturing into new, business operations/activities of the corporate customer. In these cases the TCSP would be required to update the CDD records by obtaining information and/or documentation to understand the corporate customer's new business operations or activities;
f. Whenever a customer or its beneficial owner(s) is identified as being a PEP.
g. Changes in parties involved with a particular corporate customer;
h. The customer requests the setting up of new corporate structures;
i. The customer requests services that pose a higher risk;
j. Unexplainable frequent changes in the name of the customer entity; and/or
k. Whenever there is any cause for concern or suspicion, or the filing of an STR to SICCFIN/AMSF, which should lead the TCSP to assess whether CDD information is to be updated.

Ongoing monitoring procedures need not necessarily result in the collection of more documentation; this should only be necessary when information and documents held are no longer relevant, accurate or valid.

4.8.6 **General Principles applicable to ongoing monitoring**

It is crucial for proper ongoing monitoring to be carried out that the TCSP's customer-facing members of staff, as well as compliance officers or other staff members tasked with monitoring business relationships, are equipped with the necessary knowledge and expertise to identify and flag dubious or suspicious transactions or activities, or trigger events that should prompt a review of business relationships.

TCSPs are thus required to ensure that they, as well as senior management and all relevant members of staff are kept informed and receive training on ML/FT-C trends, methods and risks relevant to the services provided by the TCSP. Training should be undertaken on a regular basis, and in particular staff should be informed of changes in AML/CTF legislation on a timely basis. International bodies such as the FATF, MONEYVAL, EUROPOL, as well as the reports and documents published by SICCFIN/AMSF from time to time, provide information on the latest ML/FT-C trends and risks, including on the misuse of companies and other legal entities. Apart from attending and receiving training, TCSPs should also keep themselves informed about ML/FT-C developments generally.

It is also important that TCSPs review the monitoring methodologies and processes adopted on a regular basis to ensure they remain adequate since ML/FT-C risks and ML/FT-C trends and practices change. Moreover, the results of ongoing monitoring processes should always be documented, and records maintained.

Similarly, staff members responsible for drafting bank transfer instructions, constitutive documents or contracts or monitoring the receipt of assets for companies, partnerships, trusts, foundations and other legal entities should receive

more regular and focused training, as opposed to staff members who are responsible for the completion and submission of statutory forms. In view of the nature of their work, the former type of staff members would thus have a better overview of the corporate customer's dealings and activities, which would therefore enable them to identify anomalous activities or transactions.

Moreover, and especially for high risk customers, TCSP should adopt adequate procedures and mechanisms of information-sharing to ensure that relevant staff (e.g., the MLRO, designated employees, front-line staff, relationship managers and compliance staff) are provided with timely information about customer relationships, such as the result of Enhanced Due Diligence or other additional measures undertaken, any information about any connected accounts or relationships, and about any suspicious or dubious behaviours or activities identified.

4.8.7 Risk-based approach to ongoing monitoring

The extent of monitoring should be commensurate with the particular customer's risk profile, which is established through the customer risk assessment. For effective monitoring, resources should be targeted towards business relationships presenting a higher risk of ML/FT-C.

Some services (such as company formation) may be provided only on a one-off basis, without a continuing relationship with the customer, in which case no ongoing monitoring obligations would apply. Moreover, the TCSP's access to documentation and information about the customer, his/her operations and business activities will vary depending on what type of service that TCSP would be offering.

By way of example, a TCSP offering only bookkeeping, registered office, or Law 1381 mandataire services would not have access to, or visibility of, specific transactions or contracts being undertaken by the customer, or of bank records, to enable the TCSP to monitor the transactions being undertaken. On the other hand, TCSPs offering directorship, partnership, trustee or foundation management services and being vested with the legal representation of the company would have visibility of contracts or transactions that are to be executed by the corporate customer, enabling them to conduct appropriate ongoing transaction monitoring.

The corporate and fiduciary services provided by TCSPs enable them to gain access to information and documents relative to the customer, to enable them to conduct ongoing monitoring and to identify suspicious activities or transactions carried out using companies, partnerships, trusts, foundations or other legal entities. For example, their direct knowledge of, and access to, the records and management accounts of these structures, as well as through close working relationships with trustees, settlors, managers and UBOs involved in corporate and fiduciary entity customers, may help TCSPs to monitor the customer's activities in an appropriate manner. The continued administration and management of partnerships, trusts, foundations or other legal entities (e.g., asset disbursements, account reporting, and corporate filings) would also enable TCSPs to develop a better understanding of their customers' ongoing activities.

The list below identifies the type of ongoing monitoring that TCSPs are expected to undertake depending on the particular TCSP activities they provide. The list also provides examples of specific monitoring measures that may be undertaken. The TCSP should determine which measures to implement based on the ML/FT-C risk posed by the particular business relationship.

All TCSP ongoing services – TCSPs are expected to have processes in place to monitor and keep CDD documentation up to date. This is intended to ensure that identification data and documentation (e.g., the customer's details, such as its name, information on its structure and involved parties, such as beneficial ownership information) and information on the customer's business operations or activities (determined through the gathering of information and/or documentation), is reviewed to ensure that it is still relevant and up to date.

This could be achieved through measures such as the following:

a. reviewing financial statements to evaluate whether the customer activity disclosed at the outset remains unchanged;
b. reviewing corporate filings that may be processed by the TCSP or accessed through company registers. These may

shed light on changes in the customer's structure or involved parties;

c. carrying out media searches on an ongoing basis to be aware of any adverse or relevant information on the corporate customer and involved parties (such as shareholders and BOs), with the frequency of these checks being dependent on the customer risk classification;
d. making use of commercial databases to screen, on an ongoing basis, the corporate customer and involved parties; and
e. requesting information about any changes from the customer itself.

Directorship, trustee, foundation management services – TCSPs offering directorship services and who would be vested with the legal and judicial representation of the customer, or are otherwise empowered to bind the customer, are expected to carry out both types of ongoing monitoring, i.e., monitoring of transactions and monitoring and updating of CDD data, information and documentation. In these cases the TCSP's visibility of payments or transactions undertaken by the corporate customer will depend on a number of factors, such as:

- whether, as director, trustee, partnership or foundation manager one would have the legal representation (sole or joint) of the corporate or fiduciary customer, or whether this may be exercised by others without that director's, trustee's, or foundation manager's involvement, for example if legal representation is vested in any one of the directors acting individually; or
- whether, as director, trustee, partnership or foundation manager, one would have signatory rights (sole or joint) on the company's bank or payment account.

The level of accessibility to, and visibility of, transactions and payments undertaken by the corporate customer will ultimately determine the type of ongoing monitoring of the company's transactions and activities that the TCSP may carry out. Directors who are legal representatives of the corporate entity (solely or jointly) or are granted representation powers (e.g., through a Power of Attorney or Directors' Resolutions) and are responsible for approving payments or undertaking transactions (e.g., signing contracts) would have visibility of all prospective transactions to be undertaken by the corporate customer.

In these cases TCSPs are expected to monitor transactions or payments prior to their execution (pre-transaction monitoring) to ensure that they are in line with the customers' expected activities. Furthermore, the TCSP should request supporting documents and information when this is not clear and necessitates further scrutiny to ascertain the purpose and nature of the transaction or payment and, where appropriate, the source of funds.

TCSPs may act as directors, trustees, partnership or foundation managers in an entity when the legal representation or other powers to bind the customer are vested in different persons acting individually. In such a scenario, the legal representation or binding powers may be exercised by other directors or individuals without that TCSP's involvement, and thus the TCSP acting as director would not be able to carry out pre-transaction monitoring at all times.

In these cases, TCSPs should adopt post-transaction monitoring, whereby they periodically request information on transactions, contracts or payments undertaken by the corporate customer to determine whether these are in keeping with the corporate entity's known activity. TCSPs offering directorship services should also ensure that discussions and decisions at board level are minuted, and that they are in line with the customer's expected activities.

When TCSPs provide director, trustee, partnership or foundation management services, but are not vested with the customer's legal or judicial representation or any other power to bind the customer, they might not always have access to information and documents on transactions, contracts and payments. Nevertheless, they are still expected to carry out the checks envisaged under paragraph (a) to (e) above to monitor that the CDD data, information and documentation, including the information obtained on the corporate customer's activities, remain relevant and up to date.

This information and documentation should be scrutinised and, when doubts or concerns arise on any particular activity or transactions, TCSPs must question and request further information and/or documentation to understand the rationale and purpose of the transactions or the activity in question. TCSPs providing directorship, trustee, or foundation services would also have access to discussions and minutes of the meetings of the decision making body (eg board), and hence should also

use this information and power of representation to obtain information on, and scrutinise, the customers' activity to ensure that it remains in line with the customer's expected line of activity and purpose.

Company secretarial services – in addition to the ongoing monitoring obligations contemplated under paragraphs a) to e) above TCSPs offering company secretarial services should ensure that discussions at board level (which, as company secretary, they are necessarily privy to) are in line with the understanding of the customer's business activities. TCSPs offering these services are not expected to carry out ongoing monitoring of transactions;

Law 1381 mandataire services, and the provision (or arranging for the ongoing provision) of registered office – no ongoing monitoring of transactions is expected when these services are provided. In these instances, TCSPs are expected to carry out ongoing monitoring of CDD data, information and documents as explained under paragraphs a) to e) above. When providing (or arranging for the ongoing provision of) registered office services, TCSPs should also monitor the correspondence being received to ensure that this is in line, and tallies, with the TCSP's understanding of the activities being carried out by the corporate customer;

In addition to the above checks, which are led by the TCSP, it may be wise for the TCSP to hold the customer itself responsible for informing the TCSP of any changes in connection with the customer and the ownership structure that are relevant for the purpose of fulfilling the TCSP's ongoing monitoring obligations. This is especially helpful with respect to company services in relation to which the TCSP does not need to meet the customer on a regular basis or does not have ongoing visibility of the customer's business activities (for example, the provision of registered office services).
This undertaking can be obtained in the contractual agreement or letter of engagement, or should otherwise be agreed on by the customer in writing. Although this provides an additional safeguard to the TCSP, it does not in any way exonerate the TCSP from its ongoing monitoring obligations. In other words, the TCSP will always be held responsible for carrying out the necessary ongoing monitoring. This responsibility may not be shifted.

4.8.8 Complex and unusual types of transactions

When transactions are complex, unusually large in amount or conducted in an unusual pattern, or have no apparent economic or lawful purpose, TCSPs are expected to examine the background and purpose of those transactions as required by AML Law 1362 and the *Generic Guidelines*. Such transactions should include transactions between the TCSP and its customer, as well as the underlying transactions between the TCSP's customer and its own customers, where applicable.

This obligation is only applicable to those that offer TCSP services that require the carrying out of ongoing monitoring of transactions, as explained in this section. The purpose of these examinations is that of determining whether these complex or unusual transactions give rise to suspicions of ML or FT, which should be reported to SICCFIN/AMSF, and to determine whether the continuation of services is appropriate.

The findings and outcomes of these examinations should be properly documented in writing and be available for inspection by SICCFIN/AMSF. Proper records of the decisions taken and the reasons for the decisions will help a TCSP demonstrate that the manner in which it handles unusual or suspicious activities is appropriate.

Ongoing monitoring of the business relationship should be carried out on a risk-sensitive basis. This means that: the regularity of transaction/activity scrutiny or CDD reviews should be proportionate to the risks of ML/FT-C identified, though still in line with specific requirements on the type and timeliness of ongoing monitoring that is provided for in this document; and, moreover the extent of information or documentation being requested to understand the source of funds for particular transactions, the purpose of certain transactions or any changes in the customer's activity or business should also be proportionate to the ML/FT-C risks being posed by that customer.

Note:
Despite the private wealth nature of TCSP business in Monaco, the multinational and multicultural background of UBOs increases the potential risk of terrorist related activities. It is therefore essential to verify ownership for connections with terrorist organisations which may be obscured by complex ownership structures, and to monitor transactions which may relate to the financing of terrorist activities, and which may only involve small unitary values.

4.9 Timing of due diligence procedures

In determining the appropriate time to commence CDD procedures, TCSPs should be primarily guided by the AML Law 1362 and the Generic Guidelines. TCSPs are not expected to initiate CDD procedures on an enquiry being made by a prospective customer. When these enquiries are simply preliminary, it would be premature to commence CDD procedures. As a general rule, the TCSP is expected to initiate CDD procedures when the customer takes active steps to seek the services of the TCSP. CDD measures are then to be completed prior to the setting up of the business relationship or the carrying out of an occasional transaction.

AML Law 1362 requires the TCSP to complete verification procedures prior to the establishment of a business relationship or the carrying out of an occasional transaction. This notwithstanding, TCSPs may complete verification procedures and carry out other CDD measures during the establishment of this business relationship, or the carrying out of an occasional transaction, as long as it is demonstrated that the risk of ML/FT-C within that initial phase of establishment of the business relationship, or the conducting of the occasional transaction, and until CDD is completed, is low and remains low.

4.9.1 Completion of CDD – Company, Partnership, Trust, Foundation or other Legal Entity Formation

Where a TCSP has been engaged to incorporate a company, partnership, trust, foundation or other legal entity the TCSP need not obtain all the necessary CDD information in relation to the entity formation on the signature of the letter of engagement. The TCSP may for example commence drafting the Memorandum & Articles of Association and may accept the initial share capital (when the value of the initial share capital is low in value) prior to receiving all the documentation required to verify the identity and other information obtained on the prospective company, shareholders and UBOs.

It is, however, expected that, at this stage, the TCSP would have obtained the necessary identification information of the prospective company's involved parties and UBOs, as well as information about the prospective entity's structure and planned activities. The TCSP is then expected to ensure that all the necessary identification and other documentation to complete the CDD process is obtained prior to the actual formation of the entity.

If the customer is not forthcoming with documents, and CDD measures are not completed within a reasonable period of time as determined by the TCSP in its procedures manual and prior to the formation of the entity, the TCSP should return any funds received from this customer less any fees incurred, to their origin, and desist from carrying out the formation, and also consider whether to submit an STR.

It is also to be noted that the delay in carrying out verification procedures may not always be possible, notwithstanding the low risk of ML/FT-C within the initial period of setting up the relationship or carrying out the occasional transaction. By way of example, following the introduction of the Beneficial Ownership Register and the requirement to provide the Monaco Business Registry with details of the UBO(s)/senior managing official(s) prior to the company being incorporated, all the required due diligence documentation must be invariably obtained and verified prior to submitting the necessary forms.

4.10 Termination of Business Relationships for the purposes of AML/CFT Obligations

4.10.1 In the event of loss of contact

In certain cases, the relationship with the customer cannot be officially terminated. For example, TCSPs providing registered office or directorship services, who wish to cease the provision of this service to a corporate customer, would not be able to do so when contact with the customer is lost or the customer becomes unresponsive and the TCSP cannot obtain information on a new registered office.

In these cases, only once the TCSP has exhausted all possible means to contact the customer and has documented the actions taken to do so, the termination date of the business relationship would be considered to be the date when the TCSP would have lost contact with the customer.

The business relationship would be considered terminated as of that date, notwithstanding that the TCSP's address would still appear as the corporate customer's official registered office. Termination as set out in this section is to be understood as termination of the business relationship for AML/CFT purposes only; that is, for the purposes of ongoing monitoring and the requirement of record keeping.

4.10.2 In the event of TCSP activity termination

In the event of cessation of their activity in Monaco, TCSPs are required to arrange for customer data to be held by a custodian in Monaco for a period of 10 years.

5. EXTERNAL REPORTING REQUIREMENTS

5.1 Suspicious Transaction Reporting

The TCSP is obliged to report to SICCFIN/AMSF all sums registered in the books of customer entities and all operations that could be linked to money laundering, terrorist financing or corruption. The TCSP must implement appropriate procedures to analyse any internal reports (Examen Particulier) as soon as possible, under the coordination of the person responsible for the prevention of money laundering and terrorist financing, in order to determine whether these operations or facts should be reported to SICCFIN/AMSF.

These STR obligations are covered in the AML Law 1362, and the Generic Guidelines.

It is important to note that the TCSP should be proactive in examining customer activities and profiles, and should not just rely on media reporting to identify suspicious activity; as such reports are likely to be post-event.

This report, made on the basis of sufficient grounds for suspicion, must be made in writing, before the operation is carried out, and must specify the facts which constitute the indications on which TCSPs base their report. It should indicate, where appropriate, the time limit within which the transaction must be carried out. If the circumstances so require, the report may be made in advance by fax or other appropriate electronic means. See Annex 2 for broad examples of the indicia to be considered.

Any information obtained after the report has been made that may alter the scope of the report must be communicated without delay to SICCFIN/AMSF.

The internal report, its analysis and, where applicable, the declaration of suspicion to which this analysis has led are kept and made available to SICCFIN/AMSF.

If, due to the seriousness or urgency of the case, SICCFIN/AMSF deems it necessary, it may oppose the execution of any transaction on behalf of the customer concerned by the STR.

In the event that the TCSP knows or suspects that a transaction is related to money laundering, terrorist financing or corruption, but cannot make a report before executing that transaction, either because it is not possible to postpone it or because it would be likely to prevent the prosecution of the beneficiaries of suspected money laundering, terrorist financing or corruption offences, it must make the report immediately after executing the transaction.

The following measures and procedures should be adopted to ensure the application of the above principles:

a) Following KYT checks and procedures, the MLRO may receive a written report on the atypical transaction from an employee or the TCSP's management;
b) Similarly, the MLRO may receive an oral or written report from an employee or TCSP management on a transaction suspected of being related to funds derived from drug trafficking, organised criminal activity or terrorist activity;
c) The MLRO should then investigate these transactions and, if necessary, discuss them with the employee concerned or the TCSP's management. If these discussions eliminate the suspicion, no further action is taken. The MLRO should verify that the file documentation allows third parties to reach the same conclusions;
d) The MLRO should review the case and decide whether a report should be sent to SICCFIN/AMSF. If not, an explanatory note should be written and kept on file;
e) If the TCSP's employees are not satisfied with the MLRO's findings, the matter may be referred to the management. These persons may write a written report to SICCFIN/AMSF if they consider that a report is necessary;
f) Under no circumstances should the employee or the TCSP's management inform the Customer or the related counterpart that a report has been sent to SICCFIN/AMSF;
g) If necessary, the business relationship should be closed. If the business relationship continues, the transactions should be recorded and the TCSP should define how to report the ongoing transactions to SICCFIN/AMSF. The MLRO should continue to monitor the Business Relationship;
h) Any new information obtained or facts discovered after the suspicion has been reported that may change the scope and consequences of the report should be communicated to SICCFIN/AMSF as soon as possible;
i) The timing of reporting is important and reports should be made within the shortest practical time after the suspicion being identified.

5.2 Reporting of transactions with entities in specific identified jurisdictions

The reporting obligations outlined in 5.1 are extended to all transactions and facts concerning natural or legal persons domiciled, registered or established in a State or territory whose legislation is recognized as insufficient or whose practices are considered as hindering the fight against money laundering, terrorist financing or corruption.

A ministerial order determines the state or territory, the facts and the type of transactions concerned.

5.3 UBO Registers and reporting.

These obligations are covered in the AML Law 1362, and the Generic Guidelines and will not be repeated here. These registers are managed by the Directorate for Economic Development.

There are reporting obligations for:

- A commercial company or economic interest group (GIE) registered in the Trade and Industry Register (TIR);
- A civil company listed in the special register kept by the TIR;
- A trustee established or domiciled in the Principality who administers a trust set up or transferred to the Principality under Law 214
- Trusts established under Law 214
- A trustee or any person occupying an equivalent function in a legal structure similar to trusts, established or domiciled outside the European Union, when purchasing a property or establishing a business relationship in the Principality.

TSCPs should ensure that the relevant information is reported to the DDE in the form and timeframe set out in the relevant legislation.

5.4 Trusts with business relationships with obliged entities

Could be considered as a business relationship for example:

a) opening a bank account in Monaco or establishing any relationship with a banking institution;
b) asset management in the name of the trust;

c) a relationship with an insurance company or broker (for example, in the context of insurance contracted through a broker in Monaco for a work of art held by a Monegasque resident at his domicile in Monaco);
d) a mandate granted to the centre for the conservation of precious works (Fontvieille);
e) a mandate for the sale of a work of art entrusted to a major Monegasque house (even if the sale is made outside the Principality;
f) the fact of using, for a trust, a lawyer or counsel in Monaco, to be represented by a Monegasque lawyer before the courts of the Principality on an ongoing basis;
g) the fact of using a chartered accountant in Monaco to prepare its accounts,

The notion of business relationship is therefore broad. However, the fact that a settlor appoints a person in Monaco as trustee should not be considered a business relationship.

5.5 Obligation for annual reporting of accounts for Law 214 Trusts

Pursuant to article 10 of law no. 214 of February 27, 1936, as amended, trusts are required to draw up an annual balance sheet, showing the settled funds, as well as a profit and loss account, and, where applicable, a valuation of the portfolio of securities held.

These balance sheets and profit and loss accounts must be submitted within three months of the end of the financial year to the Service du Repertoire du Commerce et de l'Industrie.

5.6 Annual internal reports

Management reports on money laundering issues (such as the number of reports to the authorities, monitoring tools, changes in applicable laws and regulations, or the number and scope of training sessions offered to employees) should be produced regularly.

At least once a year, a progress report must be submitted to the TCSP's management body on the conditions in which the prevention of money laundering, terrorist financing and corruption is ensured.

This report must make it possible, in particular, to:

- assess the presumed attempts to commit the offences that have been detected;

- make an assessment of the adequacy of the administrative organisation, the internal controls implemented and the collaboration of the TCSP's departments in preventing these offences, taking into account the TCSP's activities, size and locations;

- know the main actions carried out in the area of internal control of the provisions for combating money laundering, terrorist financing and corruption and to present those that are planned;

- describe the significant changes made to the controls during the reference period, in particular to take account of changes in the business and risks.

A copy of this annual activity report is sent to SICCFIN/AMSF

5.7 Reporting to SICCFIN/AMSF – Strix Annual reports

Each year, professionals must complete a questionnaire drawn up by AMSF in accordance with Ministerial Order no. 2022-553 of October 20, 2022.

This questionnaire enables institutions to inform AMSF of the activities of the TCSP for the year ended on 31 December of the previous year. The deadline for the reporting is set by AMSF.

5.8 Obligation for an annual derogation for the automated systems

TCSPs are required to adopt a monitoring system enabling them to detect unusual transactions. This system must satisfy all of the criteria listed in Art. 28 of Sovereign Ordinance no. 2,318 (amended), and must also be automated.

TCSPs may, with permission from SICCFIN/AMSF, be exempted from the requirement to adopt an automated system. They must be able to show that the nature and volume of the transactions does not require an automated system. In this case, the TCSP concerned is required to submit a formal request to SICCFIN/AMSF in advance, accompanied by all documents and information needed to prove that the alternative system adopted exists, and is operational and effective. This request may be sent to SICCFIN/AMSF by standard post. SICCFIN/AMSF will reply by post, indicating whether the exemption has been granted. The request for exemption must be renewed every year.

In practice, due to the nature of TCSP business in Monaco involving multiple banks and non-cash wealth movements, it is unlikely that TCSPs will be able to put in place an automated system Partial automation for screening the customer base is however recommended for larger TCSPs.

6. SANCTIONS SCREENING

TCSPs are reminded that they are required to undertake sanctions screening, freezing of assets and have reporting obligations. In this regard, TCSPs are encouraged to continuously keep up to date with any sanctions that may be imposed and with any guidance, notices, decisions, recommendations or rulings adopted by the Principality of Monaco.

Under Sovereign Ordinance no. 8.664 of 26 May 2021 pertaining to the procedures for freezing funds and economic resources in accordance with international economic sanctions, asset freezing measures are adopted in the Principality by ministerial decisions and apply from the moment they are published on the Prince's Government website dedicated to the freezing of funds and economic resources: www.geldesfonds.gouv.mc

The Minister of State's Decision no. 2021-1 of 4 June 2021, taken on the basis of the abovementioned Sovereign Ordinance, implements all of the international sanctions that are in force and, to that effect, includes an updated list of the financial sanctions imposed by the United Nations, the European Union and France.

This Sovereign Ordinance also stipulates the creation of a national list featuring all individuals, legal persons, entities and organisations who are subject to the freezing of their funds and economic resources in the Principality.

All TCSPs are expected to subscribe to the freezing measures Newsletter, to ensure that they obtain timely updates to the Monaco's National Freezing List which includes the UN, EU and France consolidated lists. This service will help the TCSP to screen their customers against this list on a regular basis and to implement the freezing measures without delay.

The Sovereign Ordinance no. 8.664 of 26 May 2021 establishes the principle that asset freezing measures adopted by the United Nations Security Council or its competent committees shall be applied directly and immediately.

Consequently, the lists drawn up or updated by the United Nations Security Council are directly applicable in Monaco from the moment they are published on the United Nations Security Council website as such publication gives rise to an implicit decision on freezing by the Minister of State.

When the assets or economic resources of an individual or legal entity designated either by the United Nations Security Council or by a Ministerial Decision are frozen, the professional who implemented the freeze on assets or economic resources is required to promptly inform the Director of Budget and Treasury by email (dbt.geldefonds@gouv.mc) and to provide the Director with information about the assets and economic resources to which the freeze applies.

In accordance with Article 14.1 of Sovereign Ordinance no. 8.664, as amended, natural or legal persons, entities or bodies designated by the Minister of State in accordance with the restrictions adopted by the European Union with regard to actions that compromise or threaten the territorial integrity, sovereignty and independence of Ukraine must report the funds or economic resources belonging to them, or that they own, hold or control within the territory of the Principality, to the

Department of Budget and Treasury on the form which can be downloaded online, within six weeks following the date of designation, whichever is later.

A number of other countries, and the EU, have enacted sanctions regimes against specific countries, (eg Russia and Belarus).

TCSPs should consider whether they are also bound to comply with any of those regimes. That will turn on the territorial (and potentially extra-territorial) scope of each regime.

In most cases, the regime will bind on the basis of presence or conduct in the territory of that state or the EU, or on the basis of nationality. For example, the UK Russia sanctions regime effectively applies to any individual or entity in the UK, and to UK nationals or UK incorporated entities worldwide. However, in some cases the United States applies 'secondary sanctions' that do not require a nexus to the United States.

If a person is bound to comply with a given sanctions regime, of particular importance is to understand:

a) the prohibitions imposed by the regime in question;
b) whether the regime provides for any licences that would allow conduct that is otherwise prohibited; and
c) whether any reporting obligations apply.

To find out that information, the relevant legislation is the primary source, as explained by guidance, and legal advice.

Broadly speaking, the various sanctions regimes against states comprise of:

- targeted prohibitions against individuals or entities, in particular asset freezes; and
- general prohibitions in relation to whole economic sectors, such as import/export restrictions and restrictions on the provision of various services.

With respect to individual targeted measures, when an individual or entity is sanctioned (or technically 'designated') under a given sanctions regime, that person is usually made subject to an asset freeze.

What an asset freeze demands will depend on the sanctions regime in question. However, in general, an asset freeze will prohibit dealing with funds or economic resources of, or providing a financial benefit to:

a) the sanctioned person; and
b) entities owned or controlled by the sanctioned person.

It is usually straightforward to know if a person has been sanctioned as the information will typically be available online. Conversely, it can be hard to know how the test for ownership and control applies on the facts and this is often a key issue in practice. If in doubt, legal advice should be taken.

With respect to general measures, each one is specific to a given sector, so one should be particularly attentive to the prohibitions relevant to the sectors one works in or otherwise operates in. Further, if one is subject to overlapping regimes, it is important to understand key definitional differences in terms of the connection to Russia required – the UK's Russia sanctions regime, for example, does not rely on Russian nationality as a criterion to trigger any prohibitions; however, the EU's Russia sanctions regime does.

Licencing is not standardised across different sanctions regimes, with the result that it is easy to be caught out. For example, a licence issued by the UK's Office for Financial Sanctions Implementation (OFSI) will not ordinarily extend to activities in the Crown Dependencies (Jersey, Guernsey and the Isle of Man) or the Overseas Territories. It is therefore important, if relying on a licence, to be sure that it applies in all of the jurisdictions in which the licenced conduct is proposed to take place.

Reporting obligations vary across different regimes. It is important to know whether in a given regime, if there is a reporting requirement at all, it applies to anyone in the jurisdiction, or just a certain category of persons.

Further, even if there is no reporting requirement, the enforcement policy under certain regimes may take into account proactive disclosure in the event of a potential breach of sanctions.

6.1 Trade sanctions circumvention

TCSPs should be aware that sanctions regulations include financial, trade, aircraft, shipping, and immigration restrictions. Trade awareness and due diligence in preventing the displacement and diversion of goods to restricted jurisdictions reinforce the effectiveness of the sanctions. The true end-users of goods often conceal their activities through intermediary companies and this suggests closer scrutiny of these entities to uncover discrepancies. Actors may use complex procurement cycles involving different stages and entities involved in covertly acquiring goods. There is a need for strong due diligence and internal governance related to sanctions, even with established counterparties. Key risk indicators include involvement in the supply of restricted goods, connections with sanctioned entities, use of complicated structures to conceal involvement, non-specific or misleading documentation, and involvement with countries of concern.

Note:

- Regular consultation of the Government website is essential, with subscription to the freezing measures Newsletter.
- Information on frozen assets must be reported promptly to the Director of Budget and Treasury.
- Pay attention to rapidly evolving sanctions regimes, including those outside Monaco involving, especially, Ukraine.
- In addition AMPA forwards to its members regular updates on changes to sanctions regimes

ANNEX

Annex 1: Business Risk factors example model – (low risk categories not included)

Risk factor	Category	Sub-category	Risk level (1 – low, 5 – high)
Customers	Type of customer legal entity	Offshore wealth management companies	5
		Offshore commercial companies	5
		Trusts	5
		Foundations	5
		French and Monegasque SCI/SCP	4
		EU or regulated companies	4
		Not-for-profit associations	4
		Onshore commercial companies	3
	Types of shareholding structures of customer entities	Structures for which TCSP acts as nominee shareholder	4
		Structures with third-party nominee shareholders (other than TCSP itself)	5
		Structures with bearer shares	5
		Discretionary trusts with unnamed beneficiaries	5
		Unusual or complex holding structures	5
		Other (advice)	
	Political links (PEPs)	PPE or persons linked to PPE	5
	Sectors of activity of beneficial owners	Building/property development	5
		Pharmaceuticals and healthcare	5
		Armaments and defence industry	5
		Extractive industries	5
		Public procurement	5
		Casinos and gaming	5
		Trade in precious metals	5
		Cash-intensive commercial activities (retail outlets, supermarkets, restaurants, dry cleaners, petrol stations, etc.)	5
		Mobile telephony	5
		Top-level sport	5
		Art and antiques	5
		Currency and virtual assets	5
		Other (please specify)	4

	Behaviour	Percentage of high-risk customers for reasons other than PEP/industry/geography (e.g. difficulty in updating KYC, desire for anonymity, unclear origin of assets, amount of assets vs. level of income)	5
	Reputation	Customers who have been the subject of special scrutiny (for reasons other than transactional, e.g. bad press)	4
		Customers who have been the subject of a suspicious transaction report	5
		Customers who have been the subject of a funds freeze procedure	5
Country/geography	**Country of residence of beneficial owners**	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
	Country of nationality of beneficial owners	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
	Origin of beneficial owners' assets	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
	Origin of funds held by customer entities	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
	Location of principal operations or assets of customer entities	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
	Country of incorporation of customer entities / Country of residence of the trustee in the case of a trust	Very high risk jurisdictions	5
		High risk jurisdictions	4
		Medium risk jurisdictions	3
Products and services	**Products**	French and Monegasque SCI/SCP	4
		Other simple and regulated structures (e.g. EU companies)	4
		Other (trusts, foundations, complex structures)	5
	Services	Domiciliation without management of Monegasque SCI/SCP	4
		Customer relationship for a structure managed by third parties	4
		Management function and/or signatory on bank account	4

		Carrying out transactions on the basis of a power of attorney granted by a structure	4
		Acting as shareholder (nominee)	5
Distribution channels used	**Remote identification**	Customers not physically present at the start of the relationship	5
		Customers not physically present during the business relationship (less than once a year)	4
	Use of third parties	Customers introduced by third parties (business introducers/third-party managers/Group entities) and for whom part of the due diligence measures are delegated to these third parties (e.g. collection of information)	5
		Customers represented by or using other TCSPs involved in the business relationship	4
Transactions	**Amounts**	Transactions over €1M	5
		Transactions between €100K and €500K	4
		Transactions under €100K	3
	Types	Transactions carried out by bank transfer or bank card	2
		Bank cheques	3
		Cash transactions (>€10K)	5
		Other transactions	3
	Level of risk	Transactions having generated an alert	5

Annex 2: Red Flags (including tax)

The following section contains a list of activities or circumstances that may indicate a higher risk of ML/FT-C. Not all the below circumstances would be relevant to all practitioners and across all services, as these red flags depend on the customer's specific profile and the circumstances surrounding the transaction or activity.

The existence of one or multiple red flags should not automatically give rise to suspicion and/or a report but rather, should cause the practitioner to analyse the transaction and customer in further detail to determine whether the activity is justified or whether there is indeed a suspicion of ML/FT-C. The list is based on known information and typologies and on guidance issued by the FATF from time-to-time, including the FATF's Guidance for a Risk-Based Approach, and FATF/EGMONT reports on Concealment of Beneficial Ownership and on Trade-Based Money Laundering Risk Indicators.

As stipulated in article 36 of law 1.362 , practitioners are required to report to SICCFIN/AMSF any knowledge or suspicion of an offence under article 218 of the Criminal Code involving money laundering, terrorist financing or the proceeds of crime.

1. **Red flags relating to the Customer**
   - The customer's registered address does not make sense when compared against its operational activity. E.g.: the address relates to an office or residential building when the customer's operations are more industrial or commercial, or else, the address is likely to be a mass registration address such as a post-box or an office building.
   - Unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
   - Customers who appear to actively and inexplicably avoid face-to-face meetings or who provide instructions intermittently without legitimate reasons or are otherwise evasive or very difficult to reach, when this would not normally be expected.
   - Adverse results from screening procedures.
   - Customer starts or develops an enterprise with unexpected profile or abnormal business cycle or customer is entrant into new/emerging markets. Organised criminality generally does not have to raise capital/debt, often making them first into a new market, especially where this market may be retail/cash intensive.
   - Indicators that customer does not wish to obtain necessary governmental approvals/filings, or similar statutory documents.
   - Frequent or unexplained change of professional adviser(s) or members of management.
   - The customer is reluctant to provide all the relevant information or the TCSP has reasonable doubt that the provided information is correct or sufficient.
   - The irregularity or duration of the customer relationship. One-off engagements involving limited customer contact throughout the relationship may present higher risk.
   - Knowledge of previously undisclosed arrangements.
   - New directors or shareholders, whose profile of a director or shareholder is inconsistent with the activities of the company.
   - Multiple changes to a customer's accountants/auditors without a valid explanation.
   - Change in trading partners that is not in line with expectations/nature of business.

2. **Red Flags relating to Transactions**
   - Company transactions do not indicate ongoing business activity in line with its stated activity.
   - High volume of trading with high-risk jurisdictions which does not make immediate economic sense when compared with the customer's known trading activity.
   - Investment in or loans to entities that have no apparent legal or legitimate tax, business, economic or other reason or entities that may pose higher geographical risk.
   - Holding of substantial or excessive amounts of cash considering the nature of the business.
   - Injection of new funds into the business, from an unclear source or where the value appears to be disproportionate to beneficial owners' circumstances.
   - Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.
   - Suspicion of customers' use of false loans, false invoices, and misleading naming conventions.
   - Sudden activity from a previously dormant customer without clear explanation, or else the company is unusually dormant from time to time where this is not in line with what would normally be expected.
   - Unexplained (where explanation is warranted) use of pooled client accounts.

- Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- An unexplained and illogical change in the jurisdictions in which the customer trades, which does not make economic sense when compared to the customer's profile and known trading activity.
- Contributions or transfers of goods that are inherently difficult to value (e.g. jewels, precious stones, objects of art or antiques, virtual assets), where this is not common for the type of customers, transaction, or with the customer's normal course of business, such as a transfer to a corporate entity, or generally without any appropriate explanation.
- Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.
- Transactions involving closely connected persons and for which the customer and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- Commercial, private, or real property transactions or services to be carried out by the customer with no apparent legitimate business, economic, tax, family governance, or legal reasons.
- Existence of suspicions regarding fraudulent transactions, or which are improperly accounted for. These might include:
    - Over and under invoicing of goods/services.
    - Multiple invoicing of the same goods/services.
    - Falsely described goods/services - over and under shipments (e.g. false entries on bills of lading).
    - Multiple trading of goods/services.

3. Red Flags indicative of Tax Evasion

3.1 Customer's Identification Information

- Customer failed to disclose dual citizenship or tax residence.
- Individual's business is not located in the same jurisdiction as their residential jurisdiction and having no reasonable commercial justification for such.

3.2 Unusual or Suspicious Transactions

- A transaction which is not in line with the known customer profile.
- The use of shareholders' loans to finance corporate activities, especially where the amounts lent to the corporate entity are not in keeping with known customer profile and financial resources.
- Under or overvaluing goods and/or services where the declared value on the invoices for these goods and/or services does not reflect the market value.
- Transactions involving services such as consultancy, marketing or research when the service provider is located in a non-cooperative jurisdiction or does not have the necessary resources to provide such services or the company providing the services only has one or very few customers notwithstanding that it has a particularly high turnover.
- Circular transactions or round-tripping transactions where funds are reinvested into the original jurisdiction after being transferred to a foreign entity.
- Transactions for which there is no economic, commercial or logical explanation.
- Transactions where assets are transferred in circumstances where there is no clear legal and rational choice to account for such transfers, and/or the assets are transferred to non-cooperative jurisdictions.
- Amount of tax paid in the past, prior to the establishment of an occasional transaction or business relationship with the TCSP, is not justified or consistent with the circumstances, facts and documentation available.

3.3 Customer Interaction & Behaviour

- Customers may show an uncommon interest in tax-related issues such as whether income from a particular transaction or activity will be declared or reported.
- Customer provides information which might indicate that the service is being utilized in relation to undeclared funds.
- A customer requests to use a client account without a reasonable or commercial justification. A customer shows concerns about regulatory reporting by the TCSP.
- The TCSP realises that the customer did not file one or more tax returns or other prescribed documents and refuses to correct defaults.
- The TCSP identifies one or more transactions as having been undertaken to try and evade taxes, or communication with the customer gives rise to suspicion that the customer has undeclared funds or evades taxes.
- The customer insists that they should not be contacted by the TCSP directly. Similarly, the customer refuses any form of contact or communication with the TCSP.
- The customer requests to close the relationship upon the TCSP's request for additional information on tax-related matters.
- A discrepancy between the customer's organisation structure and/or transactions and the documentation recorded on file.
- Funds are transferred to/from non-cooperative jurisdictions or jurisdictions with recent material changes in their tax regime.
- The customer refuses to provide information required to comply with international tax obligations, including documentation regarding declared income in their country of origin.
- The TCSP has reason to suspect or believe that the customer is not complying with tax reporting obligations in other countries.
- The customer becomes uncooperative when due diligence is carried out (whether at onboarding stage or during the relationship).
- The customer requests or suggests not to disclose any pertinent information to the tax authorities where the disclosure of that information is required in terms of law.
- The incorporation of companies which are then abandoned shortly after their establishment.
- Adverse media, such as allegations of tax fraud or convictions on tax crimes, related to tax on the customer or any connected parties.
- False statements or documents relating to tax.
- The customer is unwilling to take advantage of tax mitigation opportunities available in certain specific circumstances with no reasonable explanation for such unwillingness.
- The customer requests advice in connection with the repatriation of income or capital from a foreign jurisdiction without a reasonable or commercial justification related to the origins of the wealth.

3.4 Entity Structure & Governance

- The setting up of two or more trading companies in different jurisdictions having the same company name without a commercial reason.
- The structure includes the use of bearer shares.
- The use of nominee shareholders within the entity structure with no clear and legitimate purpose or justification.

3.5 Source of Funds & Source of Wealth

- Customer is unable or is unwilling to provide information and/or documentation on the source of funds and source of wealth when so requested.
- Information and/or documents provided on the source of wealth or source of funds seem odd or not sufficiently clear as to their source.
- Indications that funds have not been properly declared to the tax authorities.

- Transactions being made or received are not in line with the source of wealth and expected source of funds information held on file.
- The source of funds information provided does not tally with the services being requested.
- Frequent amounts of deposits from unexplained sources.
- Sales and purchases are not backed by invoices or proper documentation, or there are doubts about the legitimacy of such documentation.

[i] Created partially with reference to other regulatory guidance for the TCSP sector including: Malta Implementing Procedures - Part 2 CSPs and Part 2 Accountants and Auditors, and its VFA guidance and Final Guidance on The funding of Terrorism, the Guernsey FSC Handbook on Countering Financial Crime and Terrorist Financing of 5th November 2021, HMRC UK TCSP Guidance.