



الإمارات العربية المتحدة  
وزارة الإقتصاد

# **Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations**

Guidelines for Designated Non-Financial  
Businesses and Professions

Supplemental Guidance for Trust & Company  
Service Providers

## 11.6 Supplemental Guidance for Trust & Company Service Providers (TCSPs)

### 11.6.1 Introduction

Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* (the “AML-CFT Decision”) identifies providers of corporate services and trusts as Designated Non-Financial Business and Professions (DNFBPs), and subjects them to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates, when they are engaged in certain covered activities on behalf of their customers. Namely, when performing or executing a transaction on behalf of their customers in respect of the following activities:<sup>1</sup>

- Acting as an agent in the creation or establishment of legal persons;
- Acting (or arranging for another person to act) as a director or secretary of a company, or as a partner (or in a similar position) in a legal person;
- Providing a registered office, work address, residence, correspondence address or administrative address for a legal person or legal arrangement;
- Performing work (or equipping another person to act) as a trustee for a direct trust or to perform a similar function in favour of another form of legal arrangement;
- Acting (or arranging for another person to act as a nominee shareholder in favour of another person.<sup>2</sup>

Recent studies<sup>3</sup> have concluded that professionals engaged in the establishment and/or administration of legal entities and legal arrangements may be particularly vulnerable to misuse, exploitation, and even targeted recruitment by both individual criminals and organised criminal networks engaged in money laundering and the financing of terrorism. Among the reasons noted for this vulnerability are the facts that: in some instances such professionals are required in order to establish or register companies or legal arrangements, and they may also play a key gatekeeping role with regard to access to

---

<sup>1</sup> Throughout the remainder of this supplemental guidance, these activities are referred to as “covered activities.” This is solely a term of convenience, and it in no way limits the types of activities under which TCSPs are subject to the relevant AML/CFT obligations imposed by the AML-CFT Law and the AML-CFT Decision, or international standards and best practices.

<sup>2</sup> AML-CFT Decision Article 3.4.

<sup>3</sup> See, for example, *Money Laundering Using Trust and Company Service Providers*, Financial Action Task Force/OECD/Caribbean Financial Action Task Force, October 2010; *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, FATF, June 2013; and *Professional Money Laundering*, FATF, July 2018.

financial institutions and the financial services sector in general; trust and company service professionals can be used, even unwittingly, to assist in or facilitate the misuse of corporate vehicles for the purposes of ML/FT, or to lend an appearance of respectability to a legal person or legal arrangement; and, in some cases, TCSPs and their employees either do not properly perform the required customer due diligence, or they lack the knowledge or experience concerning the nature of the activities of the company or legal arrangement structures which they establish and administer, or the appropriate level of awareness or understanding of the ML/FT vulnerabilities to which they are exposed and/or of the red flag indicators, which should alert them to potentially suspicious transactions or activities. Further complicating the picture is the fact that many of the services sought from TCSPs by those engaged in ML/FT activities are the same types of services used regularly by law-abiding customers for legitimate purposes, making it difficult to distinguish between the two situations.

The UAE's ML/FT National Risk Assessment (NRA) has identified professional money laundering (PML) as being one of the highest crimes/threats in relation to ML in the State. PML has been shown to have a high correlation with the misuse and exploitation of the legal, accounting, and trust and company service professions.<sup>4</sup> Accordingly, the NRA also identified TCSPs operating in the UAE, both onshore and in free zones, as having a medium-high inherent vulnerability to ML/FT. Additionally, in some foreign jurisdictions with less stringent AML/CFT regulations, or in which identification of beneficial owners is not obligatory, TCSPs may be used, and in some cases may even knowingly collaborate with, professional money launderers (PMLs), posing heightened risks for TCSPs within the UAE when they cooperate with foreign counterparts.

Given the above, it is of critical importance that trust and company service professionals are well acquainted with their CDD obligations under the UAE's AML/CFT legislative and regulatory framework, as well as with the various risk factors and indicators that can help them to identify and report suspicious transactions. While the former have already been covered in depth in the *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions*, it is the intent of this supplemental guidance to cover the latter in greater detail with respect to the TCSPs.

It should be noted that, at times, certain legal professionals such as lawyers, notaries, and other independent legal professionals may engage in the provision of trust and company services. Specific considerations for such professionals acting as TCSPs are covered

---

<sup>4</sup> See, for example, *Professional Money Laundering*, op. cit. Also see the separate *Supplemental Guidance for Trust and Company Service Providers*.

further below (see Section 11.6.6, Notes on Suspicious Transaction Reporting (STR) and “Tipping Off” for Legal Professionals Engaged as TCSPs).

### 11.6.2 Summary of TCSPs’ AML/CFT Obligations

Trust and Company Service Providers who engage in covered activities are required by the AML-CFT Law and the AML-CFT Decision to fulfil certain obligations which constitute the basis of an effective risk-based AML/CFT programme. These include:

- Identifying and assessing ML/FT risks (see Guidelines [Section 4](#));
- Establishing, documenting, and updating policies and procedures to mitigate the identified ML/FT risks (see Guidelines [Section 5](#));
- Maintaining adequate risk-based customer due-diligence (CDD) and ongoing monitoring procedures (see Guidelines [Section 6](#));
- Identifying and reporting suspicious transactions (see Guidelines [Section 7](#));
- Putting in place an adequate governance framework for AML/CFT, including appointing an AML/CFT Compliance Officer, and ensuring adequate staff screening and training (see Guidelines [Section 8](#));
- Maintaining adequate records related to all of the above (see Guidelines [Section 9](#)); and
- Complying with the directives of the Competent Authorities of the State in relation to the United Nations Security Council resolutions under Chapter VII of the Charter of the United Nations, as well as in relation to *Cabinet Decision No. (20) of 2019 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* (see Guidelines [Section 10](#)).

The ultimate purpose of these measures is to establish a reliable paper trail of business relationships and transactions, and to trace the true beneficial ownership and movement of assets, in order to prevent TCSPs from being exploited for the purposes of money laundering and/or the financing of terrorism, and to aid the Competent Authorities of the State by reporting suspicious transactions.

The sections below provide additional guidance specific to trust and company service providers, in regard to the identification of risk, customer due diligence, and the identification and reporting of suspicious transactions.

### 11.6.3 Risk Factors of Specific Concern to TCSPs

The AML-CFT Decision specifies certain risk factors that should be taken into consideration by DNFBPs when identifying and assessing ML/FT risk at both the enterprise and the

customer levels. General guidance on these risk factors is provided in [Section 4.4](#) of the Guidelines.

In addition to these generalised risk factors, there are a number of additional risk factors which TCSPs should be aware of and should take into consideration in identifying and assessing the ML/FT risks to which they are exposed. Some of these risk factors depend on the specific role of the trust and company service providers in the business relationship. Other risk factors relate to the nature and type of customer, and the type of legal entity or arrangement involved.

### **Role of TCSPs**

Trust and company service professionals may perform a wide variety of roles or functions relating to covered activities. For the sake of convenience, these roles may be summarised into the following categories:

- Acting in an advisory, consulting or executive capacity with regard to the organisation, establishment, registration, administration, and/or disposition of legal entities, legal arrangements or business structures;
- Acting in a representative or executive capacity (such as a director, secretary, partner, trustee, or nominee shareholder) of a legal entity or legal arrangement;
- Providing facilities or services to legal entities or legal arrangements, such as registered offices, business addresses or domiciles, correspondence or administrative addresses, introductions or referrals to financial institutions, or other similar services.

Generally speaking, TCSPs acting in any of the roles mentioned above, whether singly or in combination, must carefully consider factors such as the customer risk, geographic risk, channel risk, and product and services risk (see Guidelines Sections [4.4.1](#), [4.4.2](#), [4.4.3](#) and [4.4.4](#)). In particular, consideration should be given to such factors as:

- Customer type, complexity and transparency (e.g. whether the customer is a physical person, a legal person or a legal arrangement; and if a legal person or arrangement, whether the customer is part of a larger, more complex group);
- Customer's country of origin (whether a UAE national or a foreign customer, and in the case of the latter, whether the customer is associated with a High Risk Country—see Guidelines [Section 6.4.3](#));
- Channel by which the customer is introduced (e.g. referrals versus walk-in customers, international referrals versus domestic referrals, or customers sourced via the internet or other media) and communicates (e.g. remote or personal contact, direct contact versus contact via a legal representative or proxy, etc.);

- Type, size, complexity, transparency, and geographic origins of financial arrangements associated with the legal entities, legal arrangements, or transactions for which they provide covered activities (see Guidelines [Section 4.4.3](#), among others);
- Novelty or unusual nature of the financial arrangements, structures, or circumstances associated with the customer's transactions or activities, particularly compared with what is normal practice in the local market (see Guidelines Sections [4.4.5](#) and [4.5.4](#), among others).

### **Nature and Type of Customer, Transaction or Activity**

In addition to the factors mentioned above, when identifying and assessing ML/FT risk, TCSPs should also consider such factors as:

- Customer's residence status (whether a UAE National, a foreign resident, or an offshore/non-resident person or legal entity);
- Type and location of services provided (for example, the creation, liquidation, raising of capital, distribution of dividends, registration, deregistration, transfer or jurisdiction, purchase, sale, or other act involving legal entities or arrangements);
- Speed, frequency, and consistency of transactions (e.g. whether there is a requirement to expedite the transaction beyond what is considered usual, or a customer engages in multiple transactions or activities in a relatively short time span, especially when such transactions or activities appear to be inconsistent or in conflict with each other or with the customer's stated business purpose or socio-economic profile).

Thus, for example, a customer who is a UAE national seeking, in person, to engage a TCSP to create a company within the State for domestic commercial purposes may have a very different ML/FT risk profile from that of a foreign national seeking, via remote communication (such as telephone or email), to create a legal entity or legal arrangement in a Financial or Commercial Free Zone in order to engage in international activities. The types of risk profiles identified and assessed, and the resultant risk ratings applied to the customers (see Guidelines [Section 4.5.1](#)), should be used in determining the efficient allocation of AML/CFT resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures (discussed below).

In assessing ML/FT risk and assigning risk ratings to their customers, TCSPs may utilise a variety of methods, depending on the nature and size of their businesses. These may include more sophisticated models, such as the application of risk weightings to the various risk factors identified, and the calculation of an overall risk score for each customer; or simpler methods such as the development of indicative customer ML/FT risk profiles based on their business models, standard market practices, and target customer segments,

against which customers may be filtered and risk-rated. Whatever methods they choose, TCSPs should clearly document them (including the rationale for their use), and apply them consistently across their business activities.

#### 11.6.4 Customer Due Diligence (CDD) Guidance for TCSPs

Together with the accurate identification and assessment of ML/FT risks and the ongoing monitoring of customer relationships and transactions, the implementation of reasonable and proportionate customer due-diligence measures is one of the key components of an effective risk-based AML/CFT programme. It has also been identified by numerous jurisdictions around the world as one of the greatest ML/FT vulnerabilities of TCSPs. Developing and consistently applying robust CDD measures is therefore a critical step for TCSPs, in order to strengthen and enhance the effectiveness of their AML/CFT programmes.

The *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions*, of which this supplemental guidance is a part, discusses customer due diligence (including enhanced and simplified customer due diligence measures) in detail, and DNFBPs should study the related sections of the Guidelines carefully. Nevertheless, there are some additional points that are of particular relevance to TCSPs.

First, TCSPs should ensure that they have in place a process for screening customers and prospective customers against Sanctions Lists (see Guidelines [Section 10, International Financial Sanctions](#)), and for performing background checks to identify any potentially adverse information (including associations with financial or other crime, or with politically exposed persons) about their customers, prospective customers, or third-party intermediaries seeking to introduce new business relationships. In this regard, TCSPs should become familiar with the various tools available for these purposes, including but not limited to: publicly accessible government and intergovernmental Sanctions Lists; commercially available or subscription-based customer intelligence databases and due-diligence investigation services; and the use of internet search techniques.

Second, a characteristic technique used in a variety of ML/FT typologies is the attempt to conceal beneficial ownership through the use of third-party intermediaries, proxies, or legal structures or arrangements, which can help to create distance between the source of the illicit funds and the transaction or activity in question. Such third-party intermediaries may include family members, friends, business associates, other legal representatives, or other third persons. In this regard, TCSPs should be particularly attentive to establishing and verifying the identity of the true beneficial owner and, whenever possible, corroborating their source of funds through reliable independent sources.

Typically, the starting point in determining beneficial ownership of a legal entity or legal arrangement is to ask pertinent questions and to obtain information directly from the client.



The information thus obtained should be analysed for reasonableness and consistency, and should be appropriately confirmed or corroborated with reference to reliable independent sources, whenever possible. This verification process may raise additional questions that require further scrutiny by the TCSP and clarifying explanations from client, with the goal of ensuring reasonable satisfaction that the TCSP knows the identity of the true beneficial owner.

Generally speaking, in the context of this corroboration process, reliable independent sources may include (but are not limited to) such things as bank references or bank account information provided by financial institutions; the use of public registries and/or tax information, such as commercial registries or federal/national tax identification numbers to verify the ownership of legal entities; land registries and/or municipal or local tax rolls to corroborate real estate holdings or transactions; vehicle, maritime, or aircraft registries to corroborate the ownership of other assets. TCSPs should be alert to situations in which customers or prospective customers appear unwilling or refuse to divulge relevant ownership information or to grant any required permissions to third parties to divulge such information about them for corroboration or verification purposes.

They should also be alert to customer due-diligence factors such as:

- Compatibility of the customer's profile (including their economic or financial resources, and their personal or professional circumstances) with the specifics (including nature, size, location, frequency) of transaction or activities involved;
- Utilisation of complex or opaque legal structures or arrangements (such as trusts, foundations, personal investment companies, investment funds, or offshore companies), which may tend to conceal the identity of the true beneficial owner or source of funds;
- Possible association with politically exposed persons (PEPs), especially in regard to foreign customers;
- Possible prior association between the parties to a transaction (buyer and seller), or other indications that the transaction is not being conducted on an arm's length basis;
- Attempts to influence (including through bribery or other means of coercion) the transparency or accuracy with which TCSPs carry out their duties.

Finally, another technique often employed in various ML/FT typologies is the use of fraudulent and/or forged documents. In cases in which TCSPs act in a representative capacity with regard to the acquisition, disposition, transfer, or financing of legal entities or legal arrangements, they should pay particular attention to the authenticity of documents or financial instruments (including securities, bonds, title deeds, loan or mortgage documents, promissory notes, or other documents and information) involved.



### 11.6.5 Ongoing Monitoring

Depending on the nature of the business relationship and the frequency and type of services provided, it may not always be possible for TCSPs to perform detailed ongoing monitoring of the entirety of their customers' activity. Nevertheless, it is important that TCSPs take reasonable steps to protect themselves from misuse by criminals and terrorists (which also includes steps to ensure they do not become unwitting accomplices to ML/FT via the sources and methods by which they are compensated for the services they provide). Particularly in circumstances in which high-risk customers have been identified, trust and company service professionals should make reasonable efforts to monitor activity related to the transactions, services, or customer activities with which they are involved. Some example of ways in which they may do so include, but are not limited to:

- In the case of organising contributions for the establishment, operation, or management of companies, as well as creating or administering legal persons or legal arrangements, and selling and buying commercial entities: periodically monitoring information contained in commercial registries or held by registered agents, to detect any unexpected changes, amendments, or transfers; and monitoring changes in ownership, dividend payments, additional capital contributions, lending and borrowing activity, powers-of-attorney, and similar indicators of true beneficial ownership and/or control, to detect any inconsistencies, unusual patterns or unexpected changes;
- In cases of handling customer funds, financial instruments, documents, or accounts in a fiduciary capacity (such as in a director, corporate secretary, trustee or signatory role): monitoring the status throughout the course of the transaction or account life cycle, in order to detect any unusual changes or substitutions; and furthermore, monitoring the frequency and size of customer transactions or funds transfers through those accounts or legal entities or arrangements, to detect turnover which is out of line with the customer's declared profile;
- When collecting fees for their services, or when being reimbursed for out-of-pocket expenses: ensuring that the funds received come from known sources on which they have performed CDD, and not from third-parties, foreign accounts, or other unknown sources; and also ensuring that the methods of payment and/or the financial instruments used are consistent with the customer's profile, and are not methods which could disguise the origin of the funds (such as cash, cashier's cheques, postal money orders, prepaid cards, third-party endorsed cheques, cryptocurrencies, or other difficult-to-trace payment methods).

### 11.6.6 Notes on Suspicious Transaction Reporting (STR) and “Tipping Off” for Legal Professionals Engaged as TCSPs

Apart from the exception from certain AML/CFT reporting requirements provided to lawyers, notaries, other independent legal professionals and accountants under the specified circumstances (see Guidelines Section 7.6 Specific Exemption from the Reporting Requirement), both the AML-CFT Law and the AML-CFT Decision require supervised institutions to report their suspicions of ML/FT-related transactions or activity to the FIU (see Guidelines Section 7, Suspicious Transaction Reporting). Under penalty of legal and administrative sanctions, the AML-CFT Law and Decision also prohibit reporting persons from disclosing or “tipping off”, to the customer or any other person, the fact that a STR has been, or is intended to be, filed, or that an investigation may be, or is being, conducted (see Guidelines Section 3.9, Sanctions against Persons Violating Reporting Obligations), or from discussing the content thereof.

In some cases, legal professionals may act as TCSPs in providing trust and company services. It should be noted that under the provisions of the AML-CFT Decision, it is not considered to be “tipping off” when legal professionals or independent legal auditors attempt to discourage customers from committing a ML/FT violation, including through the misuse of a legal entity or legal arrangement. However, in such cases, even if they succeed, in the course of carrying out covered activities, in dissuading customers from undertaking a suspected ML/FT crime, legal professionals providing trust and company services must nevertheless file a STR in regard to the attempted transaction and should follow the other steps indicated in the Guidelines (see Section 7.11, Handling of Transactions and Business Relationships after Filing of STRs), including immediately designating the customer as a high-risk customer (if not already so designated), conducting an event-triggered customer due-diligence review, and considering whether (in the absence of FIU instructions to the contrary) to terminate the business relationship.

It should be noted that the AML-CFT Law and the AML-CFT Decision make no provisions for the above-referenced exemptions in relation to TCSPs who are not lawyers, notaries, other independent legal professionals and accountants. Such TCSPs are subject to the referenced reporting and non-disclosure obligations without exception.

### 11.6.7 ML/FT Typologies

As mentioned in the Guidelines (see [Section 4.3 ML/FT Typologies](#)), the methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organisations are continually evolving and becoming more sophisticated. Moreover, the variety of transaction and activity types in which TCSPs are involved is often very wide. It is therefore impossible to provide an exhaustive list of ML/FT typologies for TCSPs, as new typologies and techniques are constantly being developed and attempted.

Nevertheless, research on the subject and analysis of case studies from around the world have identified some common methods used by criminals to launder money and/or to finance terrorist and illegal organisations, involving the types of services provided by TCSPs. These methods broadly align with the classical stages of the ML/FT process (i.e. placement, layering, and integration; see Guidelines [Section 4.2, The Standard ML Model and Generic ML/FT Risks](#)), and can be organised into three major categories, according to their primary purpose. Specifically:

- Concealing or disguising the identity of the beneficial owner or owners;
- Concealing or disguising the illicit origin of the funds involved;
- Transferring or extracting value or utility from the assets involved for the benefit of the criminal perpetrators.

TCSPs should recognise that, often, multiple ML/FT typologies and techniques are used in a single transaction or in a series of related transactions. They should therefore be alert to indicators of potentially suspicious transactions from all categories. Furthermore, they should be sure to incorporate the regular review of ML/FT trends and typologies into their employment screening and compliance training programmes (see Guidelines [Section 8.2, Staff Screening and Training](#)), as well as into their risk identification and assessment procedures.

The following have been identified as being amongst the common typologies used for exploiting TCSPs for the purpose of ML/FT, according to the Financial Action Task Force (FATF):<sup>5</sup>

- Formation of trusts and companies (including shell companies). While there are numerous legitimate reasons for the creation of legal entities and legal arrangements (such as trusts or foundations, and even shell companies under certain circumstances), these vehicles may also be exploited by criminals for the purpose of ML/FT. Examples of some of the ways in which this may be done include but are not limited to:
  - Use of companies, trusts and/or bearer shares to obscure beneficial ownership;
  - Use of shell companies\* for the placement and/or layering of the proceeds of crime;
  - Use of professional intermediaries, trustees or nominee shareholders in order to provide the appearance of legitimacy and/or to obscure beneficial ownership.

---

<sup>5</sup> *Money Laundering Using Trust and Company Service Providers*, FATF/OECD/CFATF, October 2010.

An important variation of this typology is the creation of multi-jurisdictional structures of legal entities and legal arrangements. Specifically, a complex web of legal persons (whether corporations, partnerships, investment funds, limited liability companies) and/or legal arrangements (such as trusts or foundations), and their subsidiaries or affiliated entities, spanning multiple countries, can be used to disguise beneficial ownership, as well as to divert and/or obscure the trail of financial flows, thereby facilitating ML/FT and/or the predicate offences on which they are based.

Examples of cases illustrating these techniques are offered further below, as well as in separate Supplemental Guidance for Legal and Accounting Professionals.

**\* Use of Shell Companies to Place or Layer**

A shell company is a business or corporate entity that does not have any business activities or recognisable assets itself. Shell companies may be used of legitimate purposes such as serving as a transaction vehicle (e.g., an acquiring company sets up a shell company subsidiary that is then merged with a target company, thus making the target company the subsidiary of the acquiring company) or protecting the corporate name from being used by a third party because the incorporation of the shell company under that name blocks any other company from being incorporated with the same name. But criminals often seek to set up shell companies to help obscure beneficial ownership.

Shell companies should be distinguished from *shelf companies* that are often set up for the purpose of facilitating legitimate transactions. Such companies will be used when it becomes apparent during a transaction that there is a need for a corporate vehicle to be used and there is a legitimate need for speed in the transaction. They will usually be created with a legal professional or trust and company service provider (TCSP) or their employees as the directors and/or shareholders, and are held “on the shelf” until they are needed in the course of a transaction. In many cases they will only be in existence for a short amount of time before they are sold to the clients in full, with the TCSP having no further involvement in the management of the company after it is taken down off the shelf. Criminals may seek to misuse shelf companies by seeking access to companies which have been ‘sitting on the shelf’ for a long time in an attempt to create the impression that the company is reputable and trading well because it has been in existence for many years.

In terms of professional obligations, if a client fails to provide adequate information about the purpose for which the company was set up, this may give rise to concerns as to whether the TCSP would be able to adequately provide services in the best interests of the client. The failure to ask such questions may be an indicator that the legal professional is complicit in the scheme.

**Management of Companies and Trusts**

While the creation of companies and trusts is a key area of vulnerability for TCSPs, criminals will also often seek to have them involved in the management of those companies and trusts in order to provide greater respectability and legitimacy to the entity and its activities.

In some countries professional rules preclude a TCSP from acting as a trustee or as a company director. In countries where this is permitted, there are differing rules as to whether that TCSP can also provide other services, such as discretionary management or fiduciary services, for the company or trust. This will affect whether any funds relating to activities by the company or trust can go through accounts controlled by the TCSP.

Where a settlor creates a trust using the proceeds of crime or deposits further assets into the trust which are the proceeds of crime, a TCSP acting as trustee will be facilitating the laundering of those proceeds by managing the trust. Under common law there is an obligation on the trustee to acquaint themselves with all trust property and the FATF standards require that those providing trust services in a business capacity undertake CDD, including ascertaining the source of funds. Such enquiries would assist in minimising the risks of TCSPs who are acting as trustees inadvertently becoming involved in money laundering.

Source: Adapted from the Financial Action Task Force's, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, June 2013.

- Management (including discretionary management) of companies and trusts. In some situations, TCSPs may act as representatives of customers with regard to a variety of activities, including service as company directors, company secretaries, trustees, nominee shareholders, or account signatories. Trust and company services professionals who engage in such services must exercise due caution to ensure they do not perform activities which benefit criminals by establishing distance between, or concealing the identity of, the beneficial owner/illegitimate source of funds and the ML/FT transactions those persons seek to undertake. Some of the purposes for which TCSPs can be exploited by criminals include but are not limited to:
  - Opening of financial accounts (including bank, brokerage, and other accounts) for legal entities or legal arrangements whose beneficial owners or beneficiaries would otherwise raise concerns or suspicions on the part of a financial institution;
  - Providing access to other professional service providers for parts of a transaction or business relationship, especially when the other service providers operate or are domiciled in a different legal jurisdiction;
  - Execution of transactions for their customers' benefit, either on the customers' explicit instructions or on a discretionary basis.

Examples of cases illustrating the techniques referenced above are provided further below.

- Misuse of client accounts. The provision and use of client accounts is a service commonly offered by many TCSPs for legitimate purposes. These accounts, however, may also be exploited by criminals insofar as they may be misused:
  - As a first step in converting the cash proceeds of crime into other less suspicious assets;
  - As an intermediate link between different ML/FT techniques, such as the formation, capitalisation and/or acquisition of legal entities (including shell companies) or legal arrangements, and the transfer funds/proceeds of crime;
  - To help disguise the ownership or illicit source of funds or other assets;



- To obtain access to the financial system when the criminal might otherwise arouse suspicions or prove to be an undesirable customer for a financial institution.

Criminals may utilise a number of different techniques in exploiting client accounts, especially where weaknesses in operational controls or a lack of recognition of red flag indicators could render TCSPs vulnerable to misuse for the purposes of ML/FT. Some of the methods which TCSPs should be aware of include but are not limited to:

- Transfer of funds to/from third parties on the basis of fraudulent contracts, invoices, loans, or other payments, either with or without the use of the customer's own company or legal arrangement account as an intermediate step;
- Structuring of transactions, or the use of third-party names and/or involvement in transactions unrelated to the business relationship with the TCSP;
- Cancellation of transactions before completion, including those in which funds are instructed to be returned to third parties unrelated to the underlying transaction.

Examples of cases illustrating the techniques referenced above are provided further below.

- **Other.** In addition to the typologies referenced above, TCSPs may be called upon to perform a variety of other services which can be exploited for the purposes of ML/FT. Examples of other activities which may expose TCSPs to such risks include but are not limited to:
  - Advising on and/or creating tax structures or tax shelters;
  - Referring or introducing clients to banks, financial institutions, or other TCSPs;
  - Establishing, managing, registering, or performing services for charities.

Examples of cases involving some of the methods referenced above are given further below.

### 11.6.8 Examples of ML/FT Cases

#### **Concealment of the Identity of the Beneficial Owner(s)**

Criminals often go to great lengths to distance themselves from the transactions through which they attempt to launder money or finance terrorist or illegal organisations. Some of the techniques they may use include, but are not limited to, entering into various types of transactions, or seeking to obtain financing for such transactions, through the use of:

- Third-party intermediaries or proxies, including family members, friends, business associates, other legal representatives or third persons;
- Legal structures, including corporate entities or groups, limited partnerships, investment vehicles or funds, or non-profit organisations;

- Legal arrangements, such as trusts or foundations, clubs, or similar organisations of a legal character.

In this regard, TCSPs should give special attention to the identification of the true beneficial owner of the funds involved. This includes assessing whether the nature, type, and size of the transaction is consistent with the profile of the customer. In situations in which TCSPs handle financial instruments and/or documents on behalf of customers, they should also be particularly alert to the involvement of any third parties—including other unknown TCSPs, or legal and accounting professionals—in the transfer or delivery process. TCSPs should also be alert to attempts by persons from foreign jurisdictions (including persons associated with foreign TCSPs) to establish legal entities or arrangements for the beneficial interest of other legal persons or third parties.

**Example 1: Use of corporate vehicles to conceal beneficial ownership and launder the proceeds of official corruption<sup>6</sup>**

James Ibori, who was governor of Nigeria's Delta State from 1997 to 2007, inflated government contracts, accepted kickbacks and also directly embezzled state funds. His official salary was GBP 4,000 per annum, and his formal asset declaration stated that he had no cash or bank accounts outside of Nigeria. Despite this, he bought several houses and luxury assets around the world, including one property in the UK valued at approximately GBP 2.2 million.

The purchase of this house was hidden through the use of a company called 'Haleway Properties Ltd,' which was a previously-formed company incorporated in Gibraltar that had been arranged by Ibori's wife, Theresa, through a UK based TCSP. The beneficial owners of Haleway were James and Theresa Ibori.

Ibori also arranged for his mistress to transfer funds out of Nigeria and invest them on his behalf, acting as a conduit for the purchase of properties in the UK. By the end of 2003, she had deposited more than GBP 3 million into a Guernsey trust fund for the benefit of the Ibori family. The administrators of the trust fund expected that money would be deposited into the account from UK banks, consistent with the stated purpose for which it was established. When they received transfers from an unknown Nigerian company called 'Sagicon,' they requested further information. Ibori's mistress obtained forged company accounts and incorporation documents, certified by a corrupt solicitor in Nigeria, to falsely show Ibori as a major shareholder of Sagicon. These false documents satisfied the Guernsey authorities.

---

<sup>6</sup> Adapted from *Specific Risk Factors in the Laundering of Proceeds of Corruption*, Financial Action Task Force/OECD, June 2012, p. 14.

Ibori and his associates also used multiple UK bank accounts to launder funds. In 2005, Ibori utilised the services of a corrupt London-based solicitor, Bhadresh Gohil, to launder his funds. Money had been transferred from Nigeria to a UK corporate bank account, which was beneficially owned by Ibori but controlled by his former special assistant. The special assistant transferred some USD 4.7 million from the UK account into a Swiss company account called 'Stanhope Investments,' which was also beneficially owned by Ibori. Once the funds were held in the Stanhope account, they were then transferred to yet another Swiss company bank account, which was beneficially owned by another client of the corrupt solicitor. The solicitor then transferred the USD 4.7 million back to one of his client accounts in London, and later deposited it into a Texas bank account, where it was used as a deposit for the purchase of a private jet for Ibori.

As a result of these schemes, Ibori pled guilty in 2012 to ten counts of money laundering and fraud in relation to an estimated USD 250 million of stolen state assets. He was sentenced to 13 years imprisonment, and his wife was also convicted of money laundering.

**Example 2: Use of shell companies to launder the proceeds of official corruption and bid rigging<sup>7</sup>**

The government of Trinidad and Tobago followed a competitive bidding process to ensure a fair price in the construction of the Piarco International Airport. However, the project manager they hired to oversee the construction corruptly arranged for certain companies to rig the bidding in exchange for kickbacks.

The contractors, who operated a construction company and architectural firm in the United States, submitted a bid for work in the construction of the airport. A Trinidadian government assessor believed the bid was too high and requested that a second bid be conducted. Based on this, the targets of the investigation utilised a shell company to submit a second, much higher bid for the work. As a result of this much higher second bid, the contract was awarded to the targets of the investigation on the basis of their original bid. The winning bid was twice the cost of original estimates and the government overpaid approximately USD 25 million for two subcontracts alone. It is estimated that the total fraud involved more than USD 100 million. Once the corrupt contractors were paid by the Trinidadian Government, they laundered the proceeds by layering them through a series of shell companies in the Bahamas, Liechtenstein and the United States, and kicked back money to officials in the Trinidadian government as well as to the corrupt project manager.

Source: United States v. Gutierrez, No. 05-20859 CR-HUCK (November 17, 2005) superseding indictment; US Committee on Homeland Security and Governmental Affairs (2009).

<sup>7</sup> Ibid., p. 22.

**Example 3: Use of shelf companies and multi-jurisdictional shell companies to launder the proceeds of official corruption<sup>8</sup>**

Public officials in Ecuador, along with relatives and individuals connected to law firms, created a series of shelf companies in several countries for the purpose of receiving bribe payments. The bribe payments were effected through individuals with links to companies that provide goods and services to a public institution in the oil sector. To send the payments, and to hide the real beneficiaries of the transfers, the suppliers created companies in Panama, Hong Kong, British Virgin Islands, Bahamas, Uruguay, and the US.

**Example 4: Creation of complex company structures in multiple countries and use of bearer shares to launder proceeds of drug trafficking<sup>9</sup>**

A legal professional in Country A was approached to assist in setting up companies for a client. The legal professional approached a management company in Country B, who in turn approached a trust and company service provider in Country C to incorporate a number of bearer share companies. Only the details of the trust and company service provider were included in the incorporation documents as nominee directors and administrators.

The articles of incorporation and the bearer shares were forwarded to the lawyer, via the management company, who provided them to the client. The client was involved in drug importation. The use of bearer-share companies and professional intermediaries in this investigation almost offered absolute anonymity to the person in possession of the bearer shares. If investigators had not seized the bearer shares in the possession of the suspect, it would have been impossible to determine the owner of these companies and ultimately to identify and restrain their assets as proceeds of crime.

In this case, the offshore companies held significant assets alleged to be the proceeds of crime, including bank accounts in Country C, and residential property in Country B and Country D. Approximately USD 1.73 million in combined assets from residential property and bank accounts was seized in relation to those companies.

---

<sup>8</sup> *Concealment of Beneficial Ownership*, FATF/Egmont Group, July 2018, p. 30.

<sup>9</sup> Adapted from *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, FATF/OECD, June 2013, pp. 57-58 (as extracted from the website of the Jersey Financial Services Commission).

**Example 5: Exploitation of an unwitting TCSP to engage laundering the proceeds of fraud through shell companies<sup>10</sup>**

Person 1 was a chartered accountant in the business of providing corporate secretarial services to small and medium-sized enterprises in Singapore. As part of these services, he incorporated companies on behalf of his clients and acted as the resident director of companies whose directors were not ordinarily residents in Singapore.

Persons 2 and 3, members of a foreign syndicate, approached Person 1 to set up three companies, Company A, Company B and Company C, and to apply for their corporate bank accounts in Singapore. Once the accounts were set up, Persons 2 and 3 left Singapore and never returned. Person 1 was appointed the co-director of the three companies; although, he was neither a shareholder, nor the authorised bank signatory of these companies.

These companies received criminal proceeds into their bank accounts, derived from various frauds amounting to over SGD 650,000. The funds were quickly transferred by Person 3 to overseas bank accounts.

The companies had committed the offence of transferring the proceeds of crime, which was attributable to Person 1's neglect. There was a lack of supervision by Person 1 over the companies' affairs, which allowed the foreign syndicate to have unfettered control over the companies and to carry out their ML activities unimpeded. In January 2016, Person 1 was convicted of ML offences and for failing to exercise reasonable diligence in discharging his duties as a director. He was sentenced to a total jail term of 12 months, fined SGD 50,000 and disqualified from acting as a company director for the five years following his sentence.

**Example 6: Facilitation of ML by a TCSP<sup>11</sup>**

A Company Formation Agent involved in the financial services sector in the UK was prosecuted for money laundering offences, for laundering funds on behalf of organised crime groups. He carried out a complex process of funnelling criminal proceeds through a system of trusts and front and shell companies, linked to a complex matrix of inter-account bank transfers. As administrator of all the trusts used in the scheme he exercised full control of the funds flowing through them. Trusts, as well as front and shell companies were used deliberately to disguise the source of the money, and to provide a veil of legitimacy to the financial transactions.

---

<sup>10</sup> *Professional Money Laundering*, FATF, July 2018, p. 43.

<sup>11</sup> *Money Laundering Using Trust and Company Service Providers*, Financial Action Task Force, October 2010, p. 37.

**Example 7: Use of complex structures to facilitate ML of the proceeds of fraud**<sup>12</sup>

Seven International Business Companies (IBCs) were incorporated in Anguilla by a foreign national, Mr. D, using a local TCSP. The seven IBCs were then used to open bank accounts in Anguilla at two local private banks; these accounts were then utilised as the flow through points for money obtained from elaborate investment wire fraud scheme targeting persons from across the Americas, Asia and Europe. The monies would flow through bank accounts in Anguilla and another jurisdiction, then onwards to accounts in Europe. Over USD 4 million was defrauded from investors. Mr. D was arrested by the authorities in the other jurisdiction and extradited to the USA for prosecution for fraud and money laundering.

**Example 8: Use of TCSPs to obscure beneficial ownership by a foreign PEP**<sup>13</sup>

Mr. X, a foreign lawyer, utilised the services of several TCSPs to set up several offshore entities in various offshore financial services centres, including Countries A, B and C. The offshore entities included a private growth fund, which was registered in Country B. The subscriptions paid into the fund were routed through the various offshore entities in order to obscure the true source of the funds. At least two of the offshore entities were known to have bank accounts at a financial institution in Country B, where significant funds were located.

A joint investigation was subsequently initiated by authorities in Countries A and B, following allegations that the structures were set up to disguise the true source of the funds which allegedly came from a PEP in an Eastern European country, and that these funds were the proceeds of corruption. Information regarding the true ownership and purpose of the offshore entities was requested from TCSPs in the respective jurisdictions. The resultant information was incomplete. Though the foreign Lawyer claimed ultimate beneficial ownership of the entities, the authorities believed he was acting on behalf of the PEP.

Investigation indicated that the private growth fund was established on behalf of a prominent government minister in the Eastern European country, who used the fund and the other offshore entities to create a number of fictitious consultancy agreement entities, the purpose of which was to conceal millions of dollars he made as a result of investments in the sector which fell under his ministerial portfolio.

---

<sup>12</sup> Ibid., p. 39.

<sup>13</sup> Ibid., pp. 40-41.



The investigation ultimately resulted in criminal charges being brought against several offshore entities registered in Country A. These charges led to the successful prosecution and confiscation of USD 47 million.

**Example 9: Use of trust and company services to facilitate fraud and ML**<sup>14</sup>

Mr. L, a citizen of country A with prior criminal convictions, set up two medical liability insurance companies in third countries and offered fraudulent malpractice insurance coverage to medical practitioners in Country A. Mr. L also opened two bank accounts in Bermuda in the name of two of the insurance companies controlled by him, along with a mailing drop box account with a local mailbox service, thereby establishing a nominal office in Bermuda for each of these insurance companies. Both the drop box and the bank accounts were managed by a Bermuda TCSP. Mr. L also had similar drop box/bank account schemes in Country A and other countries. Premiums collected under the fraudulent insurance contracts were paid through the network of drop box accounts into related bank accounts.

Through ongoing due diligence, the Bermuda TCSP became unhappy with responses from Mr. L arising from questions/complaints from customers of the insurance companies. The TCSP therefore filed a STR, triggering a local investigation. This tied in with suspicions originating from a potential customer in Country A, who was also approached and offered insurance coverage, thereby resulting in investigations by local authorities in Country A. Cooperation between law enforcement authorities in Country A and Bermuda resulted in accounts in excess of USD 5 million belonging to Mr. L's Bermuda insurance companies being seized. This amount was eventually repatriated to Country A to assist in making restitution to the victims, and Mr. L was prosecuted for fraud and money laundering.

**Example 10: Use of a TCSP, shell companies and nominees to facilitate crime and ML**<sup>15</sup>

Companies registered in New Zealand by a Vanuatu-based TCSP operated by New Zealand citizens were suspected of acting as shell companies that facilitated crime in foreign jurisdictions. The TCSP acted as nominee shareholders and provided nominee directors who resided in jurisdictions such as Vanuatu, Panama and the Seychelles. The TCSP also provided a New Zealand-based nominee director to satisfy the legal requirement to have a New Zealand resident director and address. In the case of Company A, the employee recruited to act as a director likely had no knowledge of the activities taking place, as they had no previous involvement in any of the TCSP activities.

---

<sup>14</sup> Ibid., p. 43.

<sup>15</sup> *Concealment of Beneficial Ownership*, op. cit., p. 38.

By 2010, the TCSP had registered approximately 2,000 companies in New Zealand on behalf of clients in foreign jurisdictions. The address, in Auckland, was used as the registered office for most of the companies. Authorities suspect that at least 73 of these companies facilitated crimes in foreign jurisdictions, included the smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering.

### **Concealment of the Illicit Origin of the Funds Involved**

A key goal of criminals involved in ML/FT operations is to conceal the illicit source of the funds they are attempting to launder, in order to be able to place those funds into the financial system. As with the concealment of the identity of the beneficial owners, some of the techniques used in concealing the illicit source of funds include, but are not limited to the use of third-party intermediaries, legal structures, and legal arrangements. Furthermore, a variety of techniques, including but not limited to the use of bearer financial instruments (such as cash, bank drafts, cashier's cheques, etc.), real estate transactions, and the purchase and resale of other high-value assets, are often used to "layer" and conceal the illegal proceeds of crime. Some indicative examples are provided below.

#### **Example 11: Use of a trust to conceal the source of funds and facilitate a predicate offence and related ML activities**<sup>16</sup>

Mr. A established a Cayman revocable trust in 2004, with himself as settlor and a local Trust Company B as service provider acting as trustee. Mr. A also arranged for the incorporation of a Cayman company known as company C, with the Trust Company B also acting as registered office.

In 2008, Trust Company B, in conducting its risk assessment of its clients, became aware of allegations relating to Mr. A and his involvement in an oil and gas contract scam which also involved members of a foreign jurisdiction's government. Mr. A was the representative of the oil and gas company and was allegedly involved in a kickback scandal in which his company was awarded a contract by the foreign jurisdiction's government.

According to allegations in media reports, Mr. A was the money source who provided several officials from the foreign jurisdiction's government with the means to buy the support of other government officials, in order for them to participate in the scam. Trust company B reported in its suspicious activity report that, between 2004 and late 2005, Mr. A's trust and underlying company had received numerous transfers of funds and property from what was now deemed to be questionable sources.

---

<sup>16</sup> Ibid., pp. 42-43.

The FIU's analysis of the trust accounts uncovered outgoing funds to individuals named in numerous media reports who allegedly took part in the kickback scandal. Cooperation between the Cayman FIU and the FIU of the foreign jurisdiction revealed that Mr. A was being investigated for money laundering and corruption of government officials. The Cayman FIU was able to construct a timeline of events which demonstrated that funds and other assets had been added to the trust during the same time period in which the alleged criminal activity took place. The information disclosed by the Cayman FIU was used to further the foreign jurisdiction's investigations and related judicial proceedings.

**Example 12: Use of TCSP to conceal the illicit source of funds and proceeds of criminal activity**<sup>17</sup>

'ABC' was a company established for the provision of accounting, fiduciary and bank signatory services to others. In a regular review of its customers, 'ABC' found that the bank accounts of two of its customers, who were the beneficial owners of a number of connected companies, had frequent deposits and transfers of large amounts. Open-source research was conducted by the TCSP, revealing that the clients might be related to money laundering activities in three overseas jurisdictions. A suspicious transaction report was subsequently filed and the matter was pursued both in Hong Kong and the concerned overseas jurisdictions.

**Example 13: Exploitation of a TCSP to conceal the illicit source of funds and proceeds of crime**<sup>18</sup>

Two individuals, A and B, visited a country in Europe where they used a company formation agent to establish a registered company to receive profits from their ownership of 300 fairgrounds sites around the world. The TCSP, who also provided company and account management services, was suspicious of the underlying story and made a disclosure to the national FIU. Huge sums of money were received into the account in a brief period of time, and A and B instructed the TCSP to invest a large sum in a Unit trust on their behalf. The account continued to receive large USD transfers over the course of 2 years and a large amount was transferred into the account of a Mrs. X., who had earlier that year visited the same TCSP with an introduction from A and B.

Mrs. X explained that she would be receiving this money for a large amount of soya beans that she would supply to A and B's fairgrounds, and that she needed the TCSP's help to set up an account to receive the funds. The TCSP assisted her and then made a further

---

<sup>17</sup> Ibid., p. 72.

<sup>18</sup> Ibid., p. 72.

disclosure to the FIU, detailing the full transaction. When the large transfer to Mrs. X's account was made, a further disclosure to the FIU was again submitted by the TCSP.

The FIU's enquiries to their home country revealed that A and B were convicted drug traffickers and that Mrs. X was the wife of another convicted drug trafficker. Mrs. X later requested the TCSP to transfer a huge sum to her personal account in her home country. When notified of this development by the TCSP, law enforcement agents in both countries agreed that the transaction should be executed in order to gain further intelligence. However, when the money arrived in her account, the Customs agency in Mrs. X's country froze the funds, which were ultimately confiscated after a judicial determination was made that they were drug proceeds. The TCSP also notified law enforcement authorities of Mrs. X's efforts to liquidate her remaining funds held by the TCSP, which was prevented from taking place.

**Example 14: Attempted use of a TCSP to conceal and launder the proceeds of serious fraud<sup>19</sup>**

Bermuda Police received two suspicious activity reports, one from a bank and the other from a Corporate Service Provider, both in relation to a Country A individual, who was attempting to urgently establish a local business and open bank accounts. Unhappy with the results of due diligence, both the bank and the TCSP simultaneously made the reports, indicating that the individual was trying to wire in excess of USD 1 million into accounts in Bermuda the following day. Upon investigating, Bermuda Police discovered that fraudulent documents had been used to open the accounts and to start the business. They quickly arrested the individual, and found evidence in the individual's hotel room of serious fraud, which had been perpetrated in Country A and Country B. They also found documents that showed the route through Countries A, B and C of the laundered proceeds of that fraud. The end result was that the individual was charged and convicted in Bermuda for minor fraud offences, and was then repatriated to Country A to face criminal charges. The Bermuda Police provided significant evidence for the ensuing market manipulation trials in Country A that saw two persons convicted on numerous counts for a multi-million dollar stock market fraud scheme.

**Transfer of Value for the Benefit of the Perpetrators of ML/FT**

In addition to the placement and layering of funds for the purposes of money laundering or the financing of terrorism, criminals must also eventually integrate the proceeds of crime into the legitimate economy. In this regard, a variety of transaction types utilising the

---

<sup>19</sup> Ibid., p. 73.

services of TCSPs may be exploited as part of the ML/FT process itself, and may also be used to facilitate ongoing criminal activity. Some indicative examples are provided below.

As with the previous typologies, a number of different techniques may be used, including:

- Third-party intermediaries or proxies, including family members, friends, business associates, other legal representatives or third persons;
- Legal structures, including corporate entities or groups, limited partnerships, investment vehicles or funds, or non-profit organisations;
- Legal arrangements, such as trusts or foundations, clubs, or similar organisations of a legal character.

In order to take measures to protect themselves from being exploited by criminals and terrorists in this regard, TCSPs should give special attention to the plausibility and reasonableness of the business rationale for the types of products, services, and structures requested by their clients or prospective clients. They should also be particularly wary of requests for the use of unnecessarily complex structures, especially when multiple legal jurisdictions are involved; requests for products and services that appear to be targeted for their ability to provide anonymity or to obscure the trail of transactions and financial flows; and situations in which multiple professional intermediaries (including other TCSPs) are involved in different aspects of the same transaction or business relationship.

Examples of cases illustrating these techniques are offered further below, as well as in separate Supplemental Guidance for Legal and Accounting Professionals.

**Example 15: Involvement of a TCSP in professional money laundering**<sup>20</sup>

Mr. [C] was an accountant who started his own accounting and financial services business [N] in Panama. He advertised his services primarily on the internet and through mass mailings. [N] provided a variety of services, including the following:

- Formation of offshore entities to disguise ownership of assets;
- Passports and dual citizenship, mostly using new nominee names;
- Movement of cash and other assets offshore and back onshore using various methods;
- Issuance of debit cards for the purpose of anonymously repatriating and spending offshore funds;
- Use of correspondent bank accounts to skim profits of legitimate businesses and repatriate funds through the purchase of assets and use of debit cards;

---

<sup>20</sup> *The Misuse of Corporate Vehicles, including Trust and Company Service Providers*, FATF, October 2006, pp. 5-6.

- Anonymous trading of securities through accounts with two major brokerage houses;
- False invoicing/re-invoicing schemes to support fraudulent deductions on tax returns;
- False investment losses to disguise transfer of funds overseas.

[C] was identified pursuant to an Internal Revenue Service investigation of one of his clients for illegal importation and sale of goods. The targets of this investigation were using a re-invoicing scheme devised by [C] to illegally import chemicals into the US for sale. [C] assisted the targets in the re-invoicing scheme by preparing the invoices, receiving the proceeds of the scheme and hiding the proceeds in a myriad of Panamanian corporations for later use by the perpetrators.

As a result of this investigation, [C] became a subject of investigation for the formation of illegal trusts to facilitate money laundering and other crimes. The investigation disclosed that [C]'s company [N] had about 300-400 active clients/investors. The investigation also disclosed that it created between 5,000-10,000 entities for these clients, including the layering of foreign trusts, foundations and underlying business corporations, which were formed in offshore countries. The primary package purchased by the client was referred to as the Basic Offshore Structure, which included a foreign corporation, a foreign trust and a foundation.

In 2003, [C] was found guilty of money laundering and other criminal violations. He was sentenced to 204 months' imprisonment, fined USD 20,324,560, and ordered to pay restitution to the Internal Revenue Service in the amount of USD 6,588,949.

**Example 16: Use of trusts, companies and nominees to perpetrate fraud and ML**<sup>21</sup>

Mr [B] and his associate bought insurance companies. The assets of these companies were drained and used for personal benefits. The draining of the assets was concealed by transferring them into accounts in and out the US via wire transfers. The first step in the scheme was establishing a trust in the US. [B] concealed his involvement and the control of the trust through the use of nominees as grantors and trustee. [B] then used the trust to purchase the insurance companies.

Immediately after the acquisition, [B] would transfer millions of dollars of reserve assets to a corporation he set up in the US. The funds were then wire-transferred to an offshore bank account in the name of another corporation that he controlled. Once these funds were deposited into the offshore bank account, [B] used them to pay for his personal expenses.

---

<sup>21</sup> Ibid., p. 6.



**Example 17: Misuse of corporate vehicles, trusts and nominee services to help clients evade income taxes and launder the proceeds<sup>22</sup>**

Beginning in 1997, Mr. [D] assisted his clients with various schemes to hide income and assets from the IRS, including the use of trusts to conceal ownership, control of assets, and income, and the use of offshore trusts with related bank accounts in which the assets would be repatriated through the use of a debit card. [D] also set up international business corporations (IBC) that had no economic reality and did not represent actual ongoing business concerns, to conceal his clients' assets and income from the IRS. Concerning his own liabilities, [D] opened and maintained nominee bank accounts both in the US and abroad to conceal his income from the IRS.

**Example 18: Use of multi-jurisdictional companies and fraudulent loan for suspected ML<sup>23</sup>**

Company C was incorporated in the Netherlands. Its shareholder was Company D, in Curacao. A local carpenter acted as director in the Dutch limited liability company C. Another company, E, in Curacao provided a loan to Company D in the Netherlands, in several tranches. The loan, in favour of E, was not secured and interest was accrued rather than being paid. The terms of the loan did not appear to make business sense. A TCSP in the Antilles acted as director in both companies D and E. C invested the money in real estate in Amsterdam. The UBO is only known by the TCSP in the Antilles. It is suspected by investigators that the funds were the result of the proceeds of crime in Russia.

**Example 19: Use of multi-jurisdictional companies and charities to launder the proceeds of official corruption<sup>24</sup>**

International company A, headquartered in the Netherlands, paid corruption funds to a government employee via letter box companies. An international company was registered in an international jurisdiction, with a government employee listed as the beneficial owner but with nominee shareholders and directors. Payments were made via a Dutch bank account of a subsidiary of the international company to an account of the international company in Estonia and via an enterprise registered in Hong Kong, after which these funds were paid into bank accounts in a foreign jurisdiction and from there to a Luxembourg bank account of the international company. Bribes were also paid to charities that were directly associated with government employees. In order to account for the bribes, false invoices were entered in the accounting records.

---

<sup>22</sup> Ibid., p. 6.

<sup>23</sup> Ibid., p. 43.

<sup>24</sup> *Concealment of Beneficial Ownership*, op. cit., p. 33.

**Example 20: Use of TCSP, shell companies, nominees, fake documents for laundering the proceeds of drug trafficking<sup>25</sup>**

A New Zealand shell company was set up by a New Zealand TCSP based in Vanuatu. The shell company was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The actual business of the shell company was not apparent and was not indicated by the company name. The address listed on the companies' register was the same virtual office in Auckland as the TCSP. The nominee director resided in Seychelles, and the nominee shareholder was a nominee

shareholding company owned by the TCSP. The nominee shareholding company was itself substantially a shell company and had been used as the nominee shareholder for hundreds of other shell companies registered by the TCSP.

News reports indicated that a power of attorney document transferred the directorship to a Russian national who had sold his passport details, with a bank account opened in Latvia. When journalists from the Organised Crime and Corruption Reporting Project (OCCRP) made contact with the Russian national, the man revealed he was unaware of the New Zealand company or its bank accounts. His identity, which he had sold, had been used without his knowledge. Furthermore, a former officer of the Russian tax police told journalists that hundreds of law firms specialise in establishing ready-made shell companies for their clients, who want to remain anonymous. Usually, these law firms rely on disadvantaged individuals who sell them passport details for approximately USD 100–300.

Trade transactions were conducted with several Ukrainian companies including a state-owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third-party international companies. Transactions were also made with three other New Zealand shell companies registered by the same TCSP, using the same nominee director, nominee shareholder and virtual office address as the shell company. News reports indicated that all four shell companies had been involved in laundering USD 40 million for the Sinaloa drug cartel based in Mexico.

**Example 21: TCSP exploited to launder the proceeds of corruption by a PEP via real estate investment trust<sup>26</sup>**

The purported legitimate purpose of the scheme was the development and construction of real estate, based on small investors who injected capital. The funds provided by the settlor or third-party adherents were derived from illegal activities (corruption of public servants

---

<sup>25</sup> Ibid., p. 40.

<sup>26</sup> Ibid., p. 69-70.

and illicit enrichment). The scheme involved a BVI company with nominee directors, ultimately controlled by a PEP, who was a client of a bank that had a relationship with the TCSP. The TCSP set up a real estate trust to receive money and assets that come from the business of the settlor and “investors.” The assets received were invested in a real estate project, with the same assets given as a warranty to the bank that was financing 60% of the real estate project. The ultimate beneficial owner of the real estate project was the son of the PEP. The trustee did not conduct extensive CDD, but instead relied on the due diligence performed by the bank that referred the client, since both the client and the trustee maintained a business relationship with the bank.

**Example 22: TCSP investigated for failure to report suspicious transactions**<sup>27</sup>

A criminal investigation into a Dutch TCSP was instigated on account of the systematic failure to notify unusual transactions and money laundering. This was presumed to involve the facilitation of fake transactions on behalf of foreign clients to ensure, for example, the assets or property of those clients were scarcely taxed, or funds parked were transferred by means of fake transactions to another jurisdiction. This was carried out by means of complicated well-considered structures with companies and trusts in various countries for which instructions were given by a financial service provider and were also discussed in this way by the suspect with a Dutch civil-law notary. Dutch entities were part of these complicated structures. The same applied for the Dutch foundations registered at an international address. The structure sometimes consisted of eight different entities, in various countries. The suspect reportedly did not know in several cases the identity of the actual beneficiaries of the companies that he incorporated.

**Example 23: TCSP-registered/operated shell companies used for tax evasion & ML**<sup>28</sup>

This case involved a fraudulent tax scheme designed to evade paying tax generated from international trade and a ML infrastructure that was used to hide the illegally gained funds. The suspects used a TCSP to register and operate two international shell companies (Company A and Company B) to create the false appearance that the revenues from their international trading did not belong to the local Israeli company which they controlled, to avoid tax. The two companies traded with each other exclusively and did not have any other source of income. Company A (foreign shell company) transferred significant funds to company C (local company) using the cover of a "consulting fee" or "service commission." Only this commission, which was less than half of the real income, was reported to the

---

<sup>27</sup> Ibid., p. 73.

<sup>28</sup> Ibid., p. 79.

tax authority in Israel. Thus the suspects ultimately paid taxes only on a small part of their income.

**Example 24: Use of complex multi-jurisdictional company/trust structure for tax evasion and ML<sup>29</sup>**

A trust structure was setup for the son of Mr. X, a client of a UK law firm. The trust structure was set up to hold funds illegally diverted from an Italian company run by Mr. X. The scheme consisted of a BVI company owned by an Irish company. The BVI company, in turn, owned 100% of a Luxembourg company. The Luxembourg company would receive money from the Italian company from fictitious sales. The director of the Irish company was a partner of the same UK law firm. The director of the BVI company was another partner of the same UK Law Firm. A close associate of Mr. X had a power of attorney in the BVI company. The shares of the Irish company were held in trust for Mr. X's son (beneficial owner of the trust) by a TCSP in Jersey connected to the same UK law firm. Using such scheme there was no apparent link between the funds diverted from the Italian company and the beneficial owner of such funds. The only link was the trust.

**Example 25: Use of complicit TCSP and fraudulent loans to facilitate suspected ML<sup>30</sup>**

A Dutch target company received loans from a Swiss TCSP with a bank account in Montenegro, under the description of "repayment loan". This Swiss TCSP is also the sole shareholder of the Dutch target company. The received money was subsequently re-loaned again via a subsidiary of the Swiss TCSP in Moldova to the ultimate beneficial owner (UBO) in the Netherlands. The Dutch target company was also used by other clients of the Swiss TCSP. The Dutch target company received loans from the Swiss TCSP and subsequently re-loaned these funds to operational companies in Italy and England, which were managed by the UBOs. The account in Montenegro of the Swiss TCSP was topped up by a Swiss bank account in the name of the UBO of the Dutch target company. The FIU suspects that this manner of re-loaning one's own money via this Swiss TCSP is also used by other persons.

---

<sup>29</sup> Ibid., p. 134.

<sup>30</sup> Ibid., p. 145.

### 11.6.9 Indicators of Suspicious Transactions for TCSPs

From the examples provided above, it can be seen that criminals' methods are constantly evolving, and in many cases are specific to the particularities of a given market or a given type of trust and company services. The following list of red-flag indicators of potentially suspicious transactions is therefore by no means exhaustive.

TCSPs are also reminded that the presence of one or more of the indicators below does not necessarily mean that a transaction involves ML/FT; however, it is an indication that enhanced due diligence or further investigation may be required, so that an appropriate determination can be made by the DNFBP's appointed compliance officer as to whether the transaction is suspicious or not.

#### *The Physical Person Customer:*

- Is reluctant or refuses to provide personal information, or the TCSP has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
  - their business activities and corporate history;
  - the identity of the beneficial owner;
  - their source of wealth/funds;
  - why they are conducting their activities in a certain manner;
  - who they are transacting with;
  - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Does not maintain contact or communication after initial establishment of a legal entity or arrangement, when this would normally be expected.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for seeking a relationship with a TCSP in the country.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.

- Makes unusual requests (including those related to secrecy) of the TCSP or its employees.
- Appears very concerned about, or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is a politically exposed person, or has familial or professional associations with a person who is politically exposed.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Is the signatory to company accounts (especially multiple companies) without sufficient explanation.
- Is interested in foreign company formation, particularly in jurisdictions known to offer low-tax or secrecy incentives, without sufficient commercial explanation.
- Expresses interest in establishing or acquiring a legal entity or legal arrangement without a logical explanation or description of the purpose (especially when the type of entity or its activities does not appear to be related to the client's normal professional or personal activities).
- Requests the use of legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services that improperly conceal beneficial ownership from competent authorities, or that have the effect of improperly concealing beneficial ownership without any clear legitimate purpose.
- Requests services that deliberately provide or depend upon more anonymity than is normal under the circumstances and experience of the TCSP.
- Requests the use of nominee agreements to hide the beneficial ownership of companies or legal arrangements.
- Has previously been prohibited from holding a directorship role in a company or operating a Trust and company service provider (TCSP).
- Seeks to open multiple trusts or accounts with the same beneficiary.
- Seeks to open multiple trust accounts, each with a different business declared as the source of funds.



- Seeks to open trust accounts with high amounts, which are inconsistent with customer's profile.
- Takes an unusual interest in assisting or helping to facilitate the business arrangements of another party to the transaction.
- Requests the use of shelf companies, or pre-constituted shell companies, in jurisdictions that allow their use but do not require updating of ownership information.

*The Legal Person or Legal Arrangement Customer:*

- Cannot demonstrate a history or provide evidence of real activity.
- Sudden becomes active after a long period of dormancy, without a logical explanation (especially when the entity has otherwise been dormant since being established).
- Cannot be found on the internet or social business network platforms (such as LinkedIn or others).
- Is registered under a name that does not indicate the activity of the company, or that indicates activities different from those it claims to perform.
- Is registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations.
- Uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised the transaction.
- Has directors or controlling shareholder(s) and/or beneficial owner(s) who are also found to be representatives of other legal persons or arrangements, indicating the possible use of professional nominees.
- Has an unusually large number of beneficiaries and other controlling interests, or has authorised numerous signatories for the transaction without sufficient explanation or business justification.

- Uses informal representation arrangements (such as family or close associates acting as nominee shareholders or directors) without any apparent legal or legitimate tax, business, economic or other reason.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk.
- Is incorporated/established in a jurisdiction that does not require companies to report beneficial owners to a central registry.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Has management that appears to be acting according to instructions of unknown or inappropriate person(s).
- Has inexplicable changes in ownership, especially when the TCSP is not notified in a timely fashion.

*The Physical or Legal Person/Arrangement Customer:*

- Frequently, or without adequate explanation, changes legal structures or character (including name, ownership, beneficiaries) and/or managers, partners, directors or officers if legal entity, or trustees, protectors, or beneficiaries if a legal arrangement.
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Requests power-of-attorney for the administration or disposal of assets under conditions which are unusual, without a logical explanation.
- Requires introduction to financial institutions to help secure banking facilities.
- Makes deposits or other payments from multiple accounts or sources.
- Requests details of the TCSP's client or escrow account before the customer due diligence process or client agreement are completed, or before the details of a transaction are finalised.
- Uses the TCSP's client account or escrow account to receive funds without notification, or without sufficient justification.
- Requests the use of pooled client accounts or safe custody of client money or assets (or bearer shares, where allowed), either unnecessarily or without a reasonable explanation.

- Appears to engage multiple professionals in the same country to facilitate the same (or closely related) aspects of a transaction without a clear reason for doing so.
- Provides falsified records or counterfeit documentation.
- Is a designated person or organisation (i.e. is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Is referred by a TCSP in a jurisdiction that does not require TCSPs to record, retain or submit to competent authorities information on the beneficial ownership of corporate structures formed by them.
- Requests the use of legal persons or legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs.
- Requests the transfer of its registration or domicile to another jurisdiction without any genuine economic activity in the country of destination.

*The requested product, service, or transaction:*

- Involves the use of a large sum of cash (especially when being used as collateral rather than being used directly), without an adequate explanation as to its source or purpose.
- Appears to involve parties with a questionable connection, or generates doubts that cannot be sufficiently explained by the customer.
- Is a business transaction that involves family members of one or more of the parties without a legitimate business rationale.
- Involves multiple appearances of the same parties in different transactions over a short period of time, or involves transactions or financial transfers (e.g. disbursements or repayments) between the parties over an unusually long contractual time period.
- Is financed by a non-financial institution third party, whether a natural or a legal person, with no logical explanation or commercial justification.
- Involves loans or other financing from private third parties without adequate supporting agreements, collateral, or regular interest payments or principal repayments.
- Involves funds received from a legal entity which subsequently goes into liquidation or receivership, or is struck off the register (either voluntarily or compulsorily).
- Involves the acquisition of a legal entity in bankruptcy, liquidation or receivership, without a logical legal, tax, business, economic or other legitimate reason.

- Is executed from a business account but appears to involve personal purchases or sales, or public finances.
- Involves complicated transaction routings or multi-jurisdictional corporate structures without sufficient explanation or trade records.
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves frequent or high-value transactions between a small number of related natural or legal persons.
- Involves funds that are sent to, or received from, a foreign country when there is no apparent connection between the country and the client, and/or which are sent to, or received from, high-risk jurisdictions.
- Involves requests for payments to/from third parties without a substantiating reason or corresponding transaction.
- Involves assets purchased with cash, which is then used as collateral for a loan within a short period of time.
- Involves the unexplained use of powers-of-attorney or other delegation processes (for example, the use of representative offices).
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other authorised representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries, when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Is a legal arrangement (such as a trust or foundation) whose beneficiaries or class of beneficiaries have no apparent association with the settlor or founder.
- Involves persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities, or who are associated with such persons.
- Involves several transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties,

business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).

- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves contributions to the share capital of a company which has no registered address or permanent establishment in the country.
- Shows signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real beneficial owner.
- Involves unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction (such as the amount or terms) and/or the details of the financing or the payment instrument/procedures (e.g., a mortgage is arranged for a property purchase, but cash is substituted as the final payment method).
- Involves a significant increase in capital, or successive capital contributions over a short period of time, for a recently incorporated company with no logical explanation.
- Involves capital contributions that appear to be disproportionate to the size and requirements of the entity or its financial profile, or unusual for the type of business or industry in which it operates.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the assets being transferred, without a logical explanation.
- Involves large amounts, especially if requested by recently created companies, where the transaction does not appear to be justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs, or other justifiable reasons.
- Involves circumstances in which the parties:
  - Do not show particular interest in the details of the transaction;
  - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms;
  - Insist on an unusually quick completion, without a reasonable explanation.

**Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations  
Guidelines for Designated Non-Financial Businesses and Professions**

- Is performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, persons with similar last names, etc.).
- Is carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Takes place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.
- Involves persons or entities dealing in goods or services governed by a highly technical or regulatory regime that imposes criminal sanctions for breaches (increasing the risk of a predicate offence being committed).
- Involves the use of shell or shelf companies, front company, legal entities with ownership through nominee shares or bearer shares; control through nominee and corporate directors, legal persons or legal arrangements; or the splitting of company incorporation and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.
- Involves frequent intercompany loan transactions (especially when the conditions, such as amount or term, are changed or the agreement is assigned to a third party) or their repayment, and/or multijurisdictional wire transfers, especially when there is no apparent legal or commercial purpose.
- Involves a trust account being opened, which then receives multiple cash deposits (especially when these are from different sources or the funds originate from foreign financial institutions).
- Involves the payment of “consultancy fees” to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies.
- Involves unusual sophistication or complexity in control or ownership structures, governance arrangements, or the use of multiple TCSPs, without a clear explanation (especially when certain transactions, structures, geographical locations, international activities or other factors are not consistent with the TCSP’s understanding of the client’s business or the economic purpose behind the establishment or administration of the relevant trust, company or other legal entity).



- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves a legal entity whose characteristics (e.g. structure, number of employees, size of capital base or balance sheet, turnover, level of expenses, etc.) is unusual for its industry.
- Involves a business with an unexpected profile or unusual business cycle, especially when it is incompatible with the professional or personal experience of the principals.
- Involves indications that the client does not have or does not wish to obtain necessary governmental approvals, filings, licences, or other official requirements.
- Requires that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity, without adequate and reasonable explanation.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to: over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g. false entries on bills of lading); or multiple trading of the same goods and services).

*The Means of Payment:*

- Involves cash or negotiable instruments which do not state the true payer (for example, bank drafts, cashier's cheques, or the endorsement of a third-party cheque), especially where the amount of such instruments is significant in relation to the total value of the transaction.
- Is divided in to smaller parts with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves a loan granted, or an attempt to obtain a loan, using cash collateral, especially when this collateral is deposited abroad.
- Involves third-party funding (either for the transaction or for fees/taxes) with no apparent connection or legitimate explanation.

*Choice of TCSP:*

- Is unreasonable and without a clear explanation, given the size, location or specialisation of the TCSP.

**Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations  
Guidelines for Designated Non-Financial Businesses and Professions**

---

- Has changed a number of times in a short space of time (i.e. the client has changed or engaged multiple TCSPs) without legitimate reason.
- Is due to the fact that the required service was refused by another TCSP or the relationship with another TCSP was terminated without an adequate explanation.
- Involves a business relationship exclusively related to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services.

*Other:*

- The client is prepared to pay substantially higher fees than usual, without legitimate reason.
- The client's requested or preferred means of payment is unusual (e.g. precious metals or stones, virtual currencies, or other unconventional payment methods).