الإمارات العربية المتحدة
وزارة الإقتصـــــاد

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

Guidelines for Designated Non-Financial Businesses and Professions

Supplemental Guidance for Auditors

June 4, 2019

11.7 Supplemental Guidance for Auditors

11.7.1 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") subjects Designated Non-Financial Business and Professions (DNFBPs) to specific AML/CFT obligations under the AML/CFT legislative and regulatory framework of the United Arab Emirates. Furthermore, the federal laws of the UAE and their implementing regulations, regulating the audit profession,[1] commercial companies and financial institutions,[2] impose specific obligations on auditors with regard to the nature and content of their duties in respect of the auditing of accounts, as well as in respect of the reporting of crimes detected during the course of carrying out those duties.

Numerous studies[3] have reported that legal entities and legal arrangements may be particularly vulnerable to misuse and exploitation by both individual criminals and organised criminal networks engaged in money laundering and the financing of terrorism. 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 legal entities and legal arragements.[4]

By virtue of their role in examining the accounts, books, records, papers, governance structures, and control processes and procedures of such entities, audit professionals are in a unique position to identify potential AML/CFT weaknesses and ML/FT vulnerabilities, as well as to detect potentially suspicious activity, involving them. Moreover, persons involved in illicit activities through legal entities or legal arrangements may attempt to exploit audit professionals to lend an appearance of respectability to such legal persons or arrangements.

Given the above, it is of critical importance that audit professionals are well acquainted with the obligations which both they and the legal entities they audit have under the UAE's

[1] See, for example, Federal Decree-Law (12) of 2014, *On the Regulation of the Auditing Profession*.
[2] See, for example, Federal Decree-Law (2) of 2015, *On Commercial Companies*, and Federal Decree-Law No. (14) of 2018, *Regarding the Central Bank & Organization of Financial Institutions and Activities*. It should be noted that the company laws of several of the financial free zones (FFZs) and commercial free zones (CFZs) include similar provisions with regard to the obligations and duties of professional auditors.
[3] 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.
[4] See, for example, *Professional Money Laundering*, op. cit. Also see the separate *Supplemental Guidance for Trust and Company Service Providers*.

AML/CFT legislative and regulatory framework, as well as with the various risk factors and red flag 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 audit profession.

It should be noted that the scope of this supplemental guidance is intended to cover audit professionals acting independently, whether as sole practitioners or as members or employees of firms or companies engaged primarily in the provision of audit-related services. It is not intended to cover internal auditors employed by companies, financial institutions, or other legal entities (e.g. non-profit organisations), which are already subject to the AML/CFT obligations. Furthermore, this supplemental guidance does not cover the limited circumstances of professional attorney-client privilege, under which the AML-CFT Law and the AML-CFT Decision provide for an exception to certain AML/CFT reporting requirements to certain legal audit professionals (see Guidelines Section 7.6 Specific Exemption from the Reporting Requirement).

11.7.2 Summary of AML/CFT Obligations

The AML-CFT Law and the AML-CFT Decision require both Financial Institutions and DNFBPs 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 Section10).

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 supervised institutions 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.

As DNFBPs, audit professionals are also under the obligations summarised above; however, given the nature of their activities and functions, auditors may place greater emphasis on certain of these obligations than on others. The sections below provide additional guidance specific to audit professionals, in regard to the identification of risk, the establishment of internal control and governance frameworks, customer due diligence, and the identification and reporting of suspicious transactions.

11.7.3 Risk Identification and Assessment for Auditors

The AML-CFT Decision specifies that supervised institutions should identify and assess the ML/FT risks to which they are exposed. As part of this process, certain risk factors are specified, which should be taken into consideration by supervised institutions 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.

Audit professionals are in the unique position of approaching the statutory risk identification and assessment requirements, as well as the specific risk factors to be considered, from two different perspectives. The first perspective is that of the identification and assessment of their own ML/FT risks. The second perspective is that of the auditor's responsibilities in regard to the client's ML/FT risk identification and assessment obligations. This latter responsibility will often depend on the specific role of the auditor in the business relationship with the client. Other risk factors relate to the nature and type of customer, and the type of legal entity or arrangement involved.

Auditor's Own ML/FT Risk Identification and Assessment

Auditors may perform a variety of roles or functions relating to their activities. For example:

- Financial audits related to a client's books, records, and annual and periodic accounts;
- Operational audits related to a client's internal controls, governance structures, and risk management processes and procedures;
- Compliance audits related to a client's adherence to legal and regulatory requirements.

Generally speaking, auditors acting in any of the roles mentioned above, whether singly or in combination, may be involved in examining and opining on a range of financial transactions or operations that could expose them to ML/FT risk. For example, their work may involve: the valuation of certain types of assets or liabilities; the approval of changes in a company's capital structure or the payout of dividends; the approval of a merger or acquisition; the approval of a write-off of an uncollected debt, or the use of a reserve account, or similar corporate actions. Furthermore, auditors receive payments from their clients, which could potentially represent the proceeds of crime. In this regard, when performing their own risk identification and assessment, they 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:

- Client type, size, complexity and transparency (e.g. whether the client is a single legal entity or is part of a larger, more complex group);
- Country of origin of persons associated with the client, including beneficial owners, senior managers, legal representatives or signatories, etc. (i.e. whether a UAE national or a foreign customer, and in the case of the latter, whether the person is associated with a High Risk Country—see Guidelines Section 6.4.3);
- Industry/sector of the client (i.e. whether it is associated with a higher risk of ML/FT, taking into consideration the results of the NRA and other relevant sectoral risk assessments);
- Channel by which the client is introduced and communicates (e.g. referral versus walk-in, in-person meeting versus remote communication via the internet or other media);
- Type, size, complexity, transparency, and geographic origins of financial arrangements associated with the client (see Guidelines Section 4.4.3, among others);
- Novelty or unusual nature of the financial arrangements, structures, or circumstances associated with the client, particularly compared with what is normal practice in the local market (see Guidelines Sections 4.4.5 and 4.5.4, among others).

Thus, for example, a client that is a mainland UAE public joint-stock company involved in producing goods for domestic consumption may have a very different ML/FT risk profile from that of a limited liability company in a CFZ, engaged in international trade in electronics, and whose ownership or control structure involve persons from a high-risk country. 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 the auditor's AML/CFT resources, as well as the appropriate application of reasonable and proportionate risk-mitigation measures, including customer due-diligence measures (discussed further below).

Client's ML/FT Risk Identification and Assessment

When performing audit functions related to the evaluation of a client's internal controls and/or AML/CFT programme, auditors should also consider such factors as the client's:

- Consideration of appropriate risk factors;
- Effective application of a risk-based approach;
- Formulation, documentation, and consistent application of an appropriate risk assessment methodology;
- Involvement of appropriate internal resources, including the AML/CFT compliance officer, senior management, risk managers, or others as appropriate to the nature and size of the client's business;
- Process for the periodic review/update of both the risk assessment and its methodology.

Audit professionals should note that, in assessing ML/FT risk and assigning risk ratings to their customers, both they and their clients 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 (in the case of their own risk identification and assessment) or their clients (in cases in which they are auditing their client's internal controls and/or AML/CFT programmes) choose, they should be clearly documented (including the rationale for their use), and applied consistently across the related business activities.

11.7.4 Auditing AML/CFT Internal Controls, Policies and Procedures, and Governance

When performing audit functions related to the evaluation of a client's internal controls and/or AML/CFT programme, auditors should pay particular attention to a careful examination of the client's AML/CFT internal controls, policies and procedures, and governance structures. The statutory requirements concerning these subjects has been discussed at length in the Guidelines. In this regard, auditors should consider testing for (among other things):

- Involvement of appropriate resources (including the AML/CFT compliance officer, senior management, risk managers, or others as appropriate to the nature and size of the client's business) in the formulation, approval and implementation of relevant internal controls, policies and procedures related to AML/CFT;

- Consistency of the relevant policies and procedures with the organisation's stated risk appetite;
- Completeness of the relevant internal controls, policies and procedures, and governance structures, and their compliance with the requirements of the AML-CFT Law, AML-CFT Decision, and other applicable laws and regulations;
- Application of a risk-based approach embodied in the internal controls, policies and procedures, and in the appropriateness and proportionality of ML/FT mitigation measures in regard to the inherent risks identified, in keeping with the nature and size of the organisation;
- Extent of awareness and training of employees with regard to the relevant internal controls, policies and procedures;
- Consistency of application and adherence to the relevant internal controls, policies and procedures;
- Effectiveness of the relevant internal controls, policies and procedures;
- Documentation, record-keeping, and application of periodic reviews/updates in respect of the relevant internal controls, policies and procedures.

11.7.5 Customer Due Diligence (CDD) Guidance for Auditors

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. In keeping with the nature of their work, the development and consistent application of robust CDD measures is therefore a critical step for auditors, whether in connection with their own AML/CFT obligations, or in connection with the AML/CFT obligations of their clients when they carry out financial/accounting-, operational, or compliance-related audit activities.

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 audit professionals should study the related sections of the Guidelines carefully. Nevertheless, there are some additional points that are of particular relevance to auditors.

First, auditors should ensure that they have in place a process for screening clients and prospective clients (including their beneficial owners and persons exercising management control) 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 clients, prospective clients, or third-party intermediaries seeking to introduce new business relationships. In this regard, auditors 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, auditors should be particularly attentive to the risk-based identification and verification of the true beneficial owner of their clients, as well as those of particularly significant business relationships or counterparties of their clients. In regard to the latter, auditors are not expected to investigate their clients' business relationships or counterparties as a routine part of their audit work; however, they should consider appropriate risk-based methods of examining and testing the accuracy and effectiveness of the customer due-diligence measures taken by their clients in regard to those business relationships or counterparties. In some cases, this may involve verification of supporting documentation concerning the beneficial ownership of their clients' business relationships or counterparties.

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 auditor and clarifying explanations from the client, with the goal of ensuring reasonable satisfaction that the auditor 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. Auditors should be alert to situations in which clients or prospective clients 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 client's and the beneficial owner's profile (including known economic or financial resources, and the relevant personal or professional circumstances of the owner) with the specifics (including nature, size, location, frequency) of the business activities or transactions 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 beneficial owners or controlling persons;
- 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 auditors 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 auditors act in a capacity related to the approval or opinion with regard to an 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.

11.7.6 Ongoing Monitoring

Depending on the nature of the audit activities and the frequency and type of services provided, it may not always be possible for auditors to perform detailed ongoing monitoring of the entirety of their clients' activity (for example, when auditing a specific aspect of a client's internal controls or AML/CFT programme). Nevertheless, it is important that auditors take reasonable steps to protect themselves and their clients from misuse by criminals and terrorists. This includes taking 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.

In this regard, auditors should make reasonable efforts to examine the nature, size, frequency, and consistency of the transactions in which the client is involved, with particular regard to the client's expected activities and with what is considered normal for

organisations in similar circumstances. Some example of ways in which they may do so include, but are not limited to:

- Examining information contained in commercial registries or held by registered agents, to detect any unexpected changes, amendments, or transfers;
- 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;
- Monitoring the frequency and size of client transactions or funds transfers through accounts held with financial institutions, or through affiliated legal entities or arrangements, to detect turnover which is out of line with the financial accounts or with the client's expected activity;
- When collecting fees for services, or when being reimbursed for out-of-pocket expenses: ensuring that the funds received come from known sources on which auditors 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 client'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).

11.7.7 Notes on Suspicious Transaction Reporting (STR) for Auditors

Apart from the exception from certain AML/CFT reporting requirements provided to lawyers, notaries, other independent legal professionals and legal auditors 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 client 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.

At the same time, it should be noted that certain federal statutes, as well as regulations in several FFZs and CFZs, regulating financial institutions and commercial companies oblige auditors to report to Supervisory Authorities either crimes detected in the course of performing their duties, or situations which may comprise contraventions of the relevant laws and regulations. For example, the first paragraph of Article 249 of *Federal Decree-Law (12) of 2014, On Commercial Companies*, states that:

> "The auditor shall notify the Authority in connection with any violations of the provisions of this Law or any contraventions that constitute a crime detected upon performance of his duties at the company, within 10 (ten) days from the date of detecting the contravention."

By way of clarification, it should be noted that in the case of the detection of suspicious transactions related to possible ML/FT, auditors are obliged to file STRs with the FIU in accordance with the provisions of the AML-CFT Law and AML-CFT Decision (see the Guidelines, Section 7, Suspicious Transaction Reporting). However, to the extent that auditors also detect an underlying predicate offence related to a suspicious transaction, they should separately report that crime to the relevant Competent Authority, without reference to the fact that the STR has been filed with the FIU.

11.7.8 ML/FT Threats and Typologies

Threats

Due to the nature of their work in terms of examining the accounts, books, records, transactions, and documents of their clients, audit professionals are in a unique position to detect potentially suspicious activity or transactions. For this reason, it is important for auditors to be aware of the key ML/FT threats faced by their clients in the UAE. In this regard, the UAE's National ML/FT Risk Assessment (NRA) is of primary significance.

Many of the top (high and medium-high) ML/FT threats identified by the NRA may involve legal entities, and should therefore be of concern to auditors. Among these are ML/FT threats related to the following predicate offences:

- Fraud
- Counterfeiting and Piracy of Product
- Professional third party Money Laundering
- Insider Trading and Market Manipulation
- Tax crimes (related to direct taxes and indirect taxes)

The sectors most vulnerable to the identified threats include:

- Banking
- Money Service Business/Exchange Houses
- Dealers in Precious Metals and Stones
- Lawyers, Notaries and other independent legal professionals

- Real Estate Agents
- Company Service Providers
- Financial Advisors/Consultancy, Investment Fund/Asset Management, Brokers and Agents
- Credit Providers (Finance Companies)

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. It is therefore impossible to provide an exhaustive list of ML/FT typologies for auditors, 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, which may be detected by auditors in the course of their examination of the accounts, books, records, and other documents of their clients. 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.

Auditors 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 the purpose of ML/FT, according to the Financial Action Task Force (FATF):[5]

- Formation and/or use of corporate vehicles, companies (including shell companies), and complex legal structures or arrangements (such as trusts). While there are numerous legitimate reasons for legal entities to create other legal entities or legal arrangements (such as trusts or foundations, special-purpose vehicles, and even shell companies under certain circumstances), these structures 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.

  An important variation of this typology is the creation and/or use 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.

- Management (including discretionary management) of companies and trusts by a professional intermediary. In some situations, legal professionals, accountants, or TCSPs may act as representatives of clients with regard to a variety of activities, including performing services as company directors, company secretaries, trustees, nominee shareholders, or account signatories. Such situations may provide opportunities for criminals to benefit from the services provided by these professional intermediaries (who may be unwitting or complicit participants) by establishing distance between, or concealing the identity of, the beneficial owner/illegitimate source of funds and the ML/FT transactions those criminals seek to undertake. Some of the purposes for which professional intermediaries 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;

[5] See, for example, *Money Laundering Using Trust and Company Service Providers*, FATF/OECD/CFATF, October 2010; *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, op. cit.; *Professional Money Laundering*, op.cit.; and *Concealment of Beneficial Ownership*, FATF – Egmont Group, July 2018.

- 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.

- Misuse of professional service providers' client accounts. The provision and use of client accounts is a service commonly offered by many legal professionals, accountants, and 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 legal, accounting, or trust and company service providers vulnerable to misuse for the purposes of ML/FT. Some of the methods which auditors 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 lawyer, accountant or TCSP;
  - Cancellation of transactions before completion, including those in which funds are instructed to be returned to third parties unrelated to the underlying transaction.

  In addition to the typologies referenced above, professional service providers may be called upon to perform a variety of other services which can be exploited for the purposes of ML/FT. Examples of other such professional service providers' activities which auditors should consider 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 professional service providers;

  - Establishing, managing, registering, or performing services for charities.

- Real estate-based ML. Transactions involving the sale, purchase, leasing, and financing of real estate—including by legal entities and legal arrangements—have long been established as a typology for money laundering and the financing of terrorism, both as a part of the money laundering process itself and as a mechanism for further facilitating criminal operations. Recent studies[6] indicate that in the MENA region, after the use of cash and cheques, real-estate based ML represents one of the top trends in ML/FT typologies each year. Some of the methods used in this regard include but are not limited to:

  - Use of complex loans or credit finance schemes;
  - Use of corporate vehicles;
  - Manipulation of the appraisal or valuation of a property;
  - Use of monetary instruments (including bearer negotiable instruments);
  - Use of mortgage schemes (including fraudulent mortgage schemes);
  - Use of investment schemes and financial institutions;
  - Use of properties to conceal money generated by illegal activities.

- Trade-based ML. Transactions involving international trade and trade finance instruments—including those carried out by legal entities and legal arrangements—are a known typology for money laundering and the financing of terrorism. Some of the most common methods used in this regard, which auditors should be aware of, include but are not limited to:

  - Manipulation of invoices (over-, under-, or fictitious invoicing);
  - Fraudulent shipments (misrepresented goods, false shipments, re-shipping or so-called round-tripping);
  - Customs, excise or value-added tax fraud.

- Other. Examples of other methods used by criminals for the purpose of ML/FT, often related to tax evasion, but also to other predicate offences, include but are not limited to:

  - Transactions related to licence or royalty payments;
  - Private loan/credit agreements;
  - Use of fraudulent consultancy agreements;
  - Use of fraudulent investment agreements.

[6] See, for example, *Money Laundering and Terrorist Financing Trends and Indicators in the Middle East and North Africa Region—Update*, Middle East and North Africa Financial Action Task Force (MENAFATF), 2013; Biennial Typologies Report, MENAFATF, 2014.

Examples illustrating some of the methods referenced above are provided in the next section, as well as in separate Supplemental Guidance for the Real Estate Sector, Legal and Accounting Professionals, and for TCSPs.

11.7.9 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, auditors should give special attention to the identification of the true beneficial owner of the entities they audit. This includes assessing whether the nature, type, and size of the client organisation is consistent with the profile of the beneficial owner. They should also be alert to the involvement of third parties—for example, independent legal, accounting, or trust and company service providers (especially when these are associated with foreign jurisdictions)—in the establishment or management of 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**[7]

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.

[7] Adapted from *Specific Risk Factors in the Laundering of Proceeds of Corruption*, Financial Action Task Force/OECD, June 2012, p. 14.

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.

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.

<u>Example 2</u>: Use of shell companies to launder the proceeds of official corruption and bid rigging[8]

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.

[8] Ibid., p. 22.

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).

Example 3: Use of shelf companies and multi-jurisdictional shell companies to launder the proceeds of official corruption[9]

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[10]

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.

[9] *Concealment of Beneficial Ownership*, FATF/Egmont Group, July 2018, p. 30.
[10] 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).

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.

<u>Example 5</u>: Exploitation of an unwitting TCSP to engage laundering the proceeds of fraud through shell companies[11]

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

[11] *Professional Money Laundering*, FATF, July 2018, p. 43.

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: Creation of complex company structures in multiple countries to launder proceeds of drug trafficking[12]

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. Approximately USD 1.73 million in combined assets from residential property and bank accounts was frozen in relation to those companies.

Example 7: Use of complex structures to facilitate ML of the proceeds of fraud[13]

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[14]

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

[12] *Money Laundering & Terrorist Financing through the Real Estate Sector*, FATF, June 2007, pp. 57-58.
[13] *Money Laundering Using Trust and Company Service Providers*, Financial Action Task Force, October 2010, p. 39.
[14] Ibid., pp. 40-41.

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.

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[15]

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

[15] Ibid., p. 43.

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[16]

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.

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[17]

[16] *Concealment of Beneficial Ownership*, op. cit., p. 38.

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.

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.

<u>Example 12</u>: Use of TCSP to conceal the illicit source of funds and proceeds of criminal activity[18]

'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.

[17] Ibid., pp. 42-43.
[18] Ibid., p. 72.

Example 13: PEP involved in financial wrongdoing purchases expensive properties in foreign country through a corporate vehicle[19]

A foreign client approached a legal professional to buy two properties, one in Alpes-Maritimes (South of France), and the other in Paris, for EUR 11 million. The purchase price was completely funded by the purchaser (there was no mortgage) and the funds were sent through a bank in an off-shore jurisdiction.

As the contract was about to be signed, there was a change in instructions, and a property investment company was replaced as the purchaser. The two minor children of the client were the shareholders of the company. The foreign client held an important political function in his country and there was publicly available information about his involvement in financial wrongdoing.

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 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;
- The buying, selling, and leasing of real estate (often with unusual financing arrangements, or involving successive transactions of increasing value).

When carrying out their work, auditors should give special attention to the plausibility and reasonableness of the business rationale for the types of products, services, and structures

[19] *Money Laundering & Terrorist Financing through the Real Estate Sector*, op. cit., p. 49.

utilised by their clients. They should also be particularly wary of the use of unnecessarily complex structures, especially when multiple legal jurisdictions are involved; 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 are involved in different aspects of the same transaction or business relationship.

Example 14: Legal professional convicted of money laundering through property purchase involving cash and significant funding from multiple parties[20]

Shadab Kahn, a solicitor, assisted in the purchase of a number of properties for a client using the proceeds of crime. The client owned a luxury car business, but was also involved in drug dealing.

The funds for the property purchases were generally provided in cash from the client or from third parties. Almost GBP 600,000 was provided by the client, which was a significant level of private funding despite the client's apparent legitimate business activities.

Mr Khan was convicted in 2009 of money laundering and failing to make an STR, jailed for four years, and struck off the roll by the Solicitors Disciplinary Tribunal in 2011. The court criticised Mr Khan for accepting explanations about the source of funds at face value and not looking behind the claimed cultural customs about the funding arrangements.

Example 15: Involvement of a TCSP in professional money laundering[21]

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;
- Anonymous trading of securities through accounts with two major brokerage houses;
- False invoicing/re-invoicing schemes to support fraudulent deductions on tax returns;

[20] Ibid., p. 45.
[21] *The Misuse of Corporate Vehicles, including Trust and Company Service Providers*, FATF, October 2006, pp. 5-6.

- 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[22]

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.

Example 17: Misuse of corporate vehicles, trusts and nominee services to help clients evade income taxes and launder the proceeds[23]

[22] Ibid., p. 6.

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[24]

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[25]

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.

Example 20: Use of TCSP, shell companies, nominees, fake documents for laundering the proceeds of drug trafficking[26]

[23] Ibid., p. 6.
[24] Ibid., p. 43.
[25] *Concealment of Beneficial Ownership*, op. cit., p. 33.

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.

<u>Example 21</u>: TCSP exploited to launder the proceeds of corruption by a PEP via real estate investment trust[27]

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 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

[26] Ibid., p. 40.
[27] Ibid., p. 69-70.

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[28]

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[29]

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

[28] Ibid., p. 73.
[29] Ibid., p. 79.

Example 24: Use of complex multi-jurisdictional company/trust structure for tax evasion and ML[30]

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[31]

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.

Example 26: Use of Successive Real Estate Transactions for ML Purposes[32]

A lawyer created several companies the same day (with ownership through bearer shares, thus hiding the identity of the true owners). One of these companies acquired a property

[30] Ibid., p. 134.
[31] Ibid., p. 145.
[32] *Money Laundering & Terrorist Financing through the Real Estate Sector*, FATF, June 2007, p. 18.

that was an area of undeveloped land. A few weeks later, the area was re-classified by the town hall where it is located so that it could be urbanised.

The lawyer came to the Property Registry and in successive operations, transferred the ownership of the property by means of the transfer of mortgage loans constituted in entities located in offshore jurisdictions.

With each succeeding transfer of the property, the price of the land was increased. The participants in the individual transfers were shell companies controlled by the lawyer. Finally the mortgage was cancelled with a cheque issued by a correspondent account. The cheque was received by a company different from the one that appeared as acquirer on the deed (cheque endorsement). Since the company used a correspondent account exclusively, it can be concluded that this company was a front company set up merely for the purpose of carrying out the property transactions.

After investigation it was learned that the purchaser and the seller were the same person: the leader of a criminal organisation. The money used in the transaction was of illegal origin (drug trafficking). Additionally, in the process of reclassification, administrative anomalies and bribes were detected.

Example 27: Exploitation of a legitimate charity[33]

A suspicious transaction report (STR) was made following an attempt by Individual A, to deposit substantial amounts of cash into the account of a charity – over which he had power-of-attorney – with the instruction that it be transferred onward to a notary as an advance for the purchase of real estate. The Investigation revealed that payments into the account consisted of multiple cash deposits (presumably donations), but also payments directly from the account of Individual A. In turn, A's personal account revealed multiple cash deposits that corresponded to donations from private individuals. The debit transactions consisted of transfers to the non-profit organisation and international transfers to Individual B. Police sources revealed that A had links with individuals that were known for terrorist activities, including B.

Example 28: Use of company to launder money through a real estate purchase and sale[34]

[33] Terrorist Financing Typologies, FATF, February 2008, p. 12.

[34] *Money Laundering & Terrorist Financing through the Real Estate Sector*, FATF, June 2007, p. 10.

An East European was acting under a cover name as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients."

The funds were then used to issue a cheque to a notary for the purchase of a property. The attention of the notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross border transaction and wire transfers to launder money that, according to police sources, came from activities related to organised crime. It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Example 29: Abuse of a notary's client account[35]

A company purchased property by using a notary's client account. Apart from a considerable number of cheques that were regularly cashed or issued, which were at first sight linked to the notary's professional activities, there were also various transfers from the company to his account.

By using the company and the notary's client account, money was laundered by investing in real estate in Belgium, and the links between the individual and the company were concealed in order to avoid suspicions.

Police sources revealed that the sole shareholder of this company was a known drug trafficker.

Example 30: Use of Individuals and Companies to Conceal the Source of Illicit Funds[36]

A criminal organisation (led by a Hungarian citizen) committed tax fraud with the use of individuals and companies dealing in the area of service provision (labour force for the security industry). The proceeds obtained from tax fraud were transformed into tangible assets (e.g. real estate, cars, etc.) of another company (a legitimate one) run by the

[35] Ibid., p. 12

[36] Typologies Report on Laundering the Proceeds of Organised Crime, MONEYVAL, April 2015, p. 74.

offender, in order to cover its origin. In the course of the investigation it was established that the company had no income-generating activities and no registered employees.

The dirty money was provided in cash by the leader of the criminal organisation with instructions to purchase real estate. In order to disguise the origin of the proceeds, the money was deposited in smaller amounts in bank accounts by natural persons and then transferred into the company's account. Furthermore, for the real estate transactions, VAT refunds were claimed and obtained from the state budget. Due to those VAT refunds, the company made apparently legitimate sources of revenue.

11.7.10 Indicators of Suspicious Transactions for Auditors

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 business activity. The following list of red-flag indicators of potentially suspicious transactions is therefore by no means exhaustive.

Auditors 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 Client's Beneficial Owner or Controlling Person:

- Is reluctant or refuses to provide personal information, or the auditor 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.

- Actively avoids personal contact without sufficient justification.

- Does not maintain contact or communication after initial appointment of the auditor, when this would normally be expected.

- Refuses to co-operate or provide information, data, and documents usually required to facilitate an audit, or is unfamiliar with the details of the company's business.

- Makes unusual requests (including those related to secrecy) of the auditor 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 the signatory to multiple company accounts (especially unrelated companies) without sufficient explanation.
- Attempts to improperly conceal beneficial ownership from competent authorities.
- Has previously been prohibited from holding a directorship role in a company.

The Client Entity:

- 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 transactions.
- 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.

- Is not normally a cash intensive business, but appears to have substantial amounts of unexplained cash.
- 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 owned by or affiliated with a legal entity incorporated or established in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk.
- Is owned by or affiliated with a legal entity 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 auditor is not notified in a timely fashion.
- Uses intermediaries (either professional or informal) to carry out transactions, without sufficient justification, or regardless of unnecessary additional costs.
- 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.
- Disposes of assets under conditions which are unusual, or which involve unnecessary expense or losses, without a logical explanation.
- Makes deposits or other payments from multiple accounts or sources.
- Uses the pooled client account or escrow account of a professional service provider (lawyer, accountant or TCSP) to receive funds without sufficient justification.
- 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 owned by or affiliated with a legal entity incorporated or established in a jurisdiction with weak or absent AML/CFT laws.
- Transfers its registration or domicile from another jurisdiction without any evidence of genuine economic activity in the country of origin.
- Establishes or acquires 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 activities).
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Uses services of professional intermediaries that deliberately provide or depend upon more anonymity than is normal under the circumstances.
- Uses nominee agreements to hide the beneficial ownership of companies or legal arrangements.
- Acquires or uses shelf companies, or pre-constituted shell companies, in jurisdictions that allow their use but do not require updating of ownership information.

The client's transactions:

- Involve 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.
- Appear to involve parties with a questionable connection, or generates doubts that cannot be sufficiently explained by the client.
- Involve family members of one or more of the parties without a legitimate business rationale.
- Involve 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.
- Are financed by a non-financial institution third party, whether a natural or a legal person, with no logical explanation or commercial justification.
- Involve loans or other financing from private third parties without adequate supporting agreements, collateral, or regular interest payments or principal repayments.

- Involve funds received from a legal entity which subsequently goes into liquidation or receivership, or is struck off the register (either voluntarily or compulsorily).
- Involve the acquisition of a legal entity in bankruptcy, liquidation or receivership, without a logical legal, tax, business, economic or other legitimate reason.
- Are executed from a business account but appears to involve personal purchases or sales, or public finances.
- Involve complicated transaction routings or multi-jurisdictional corporate structures without sufficient explanation or trade records.
- Include contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involve frequent or high-value transactions between a small number of related natural or legal persons.
- Involve 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.
- Involve requests for payments to/from third parties without a substantiating reason or corresponding transaction.
- Involve assets purchased with cash, which are then used as collateral for a loan within a short period of time.
- Involve the unexplained use of powers-of-attorney or other delegation processes.
- Appear to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involve 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.
- Involve 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.
- Involve a legal arrangement (such as a trust or foundation) whose beneficiaries or class of beneficiaries have no apparent association with the settlor or founder.
- Involve 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.

- Involve 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.).
- Involve recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involve 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.
- Involve legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involve contributions to the share capital of a company which has no registered address or permanent establishment in the country.
- Show 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.
- Involve 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).
- Involve a significant increase in capital, or successive capital contributions over a short period of time, for a recently incorporated company with no logical explanation.
- Involve 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.
- Involve prices that appear excessively high or low in relation to the value (book or market) of the assets being transferred, without a logical explanation.
- Involve 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.
- Involve circumstances in which the client could have obtained a muc better price or an improvement in payment terms, but did not attempt to do so;
- Take place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.

- Involve 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).
- Involve 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.
- Involve 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.
- Involve 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).
- Involve payments of “consultancy fees” to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies.
- Involve unusual sophistication or complexity in control or ownership structures, governance arrangements without a clear explanation (especially when certain transactions, structures, geographical locations, international activities or other factors are not consistent with the auditor’s understanding of the client’s business).
- Involve unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involve 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.
- Involve a business with an unexpected profile or unusual business cycle, especially when it is incompatible with the professional or personal experience of the principals.
- Involve indications that the client does not have or does not wish to obtain necessary governmental approvals, filings, licences, or other official requirements.
- Involve the use of virtual assets for the purpose of preserving anonymity, without adequate and reasonable explanation.

- Involve any attempt by the beneficial owner 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 Auditor:

- Is unreasonable and without a clear explanation, given the size, location or specialisation of the auditor.
- Has changed a number of times in a short space of time (i.e. the client has changed or engaged multiple auditors) without legitimate reason.
- Is due to the fact that the business relationship was refused by another auditor or the relationship with another auditor was terminated without an adequate explanation.

Other:

- The client requests that shortcuts be taken, or that the work is completed in an unreasonably short time period, and is prepared to pay substantially higher fees than usual in exchange.
- The client's requested or preferred means of payment is unusual (e.g. precious metals or stones, virtual currencies, or other unconventional payment methods).