Financial
Intelligence Centre

ASSESSMENT OF THE INHERENT MONEY LAUNDERING AND TERRORIST FINANCING RISKS

COMPANY SERVICE PROVIDERS

December 2023

CONTENTS

1. INTRODUCTION AND SCOPE AND LIMITATIONS OF THE SECTOR RISK ASSESSMENT

Money laundering can be described as the process whereby criminals attempt to conceal the proceeds of their criminal activities from the actual crime, thereby giving the funds derived from criminal activities an appearance of legitimacy.

Terrorist financing is the process by which individual terrorist and terrorist organisations obtain funds to commit acts of terrorism.

The Financial Action Task Force (FATF), the global standard-setting body for anti-money laundering and combating the financing of terrorism (AML and CFT) include “Trust and Company Service Providers” (TCSPs) in the description of designated non-financial businesses and professions (DNFPBs) in the FATF Recommendations 2012, as updated in November 2023.

In its definition of DNFBPs, FATF Recommendations 2023[1] states in paragraph (f) that the term trust and company service providers” refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
Acting as a formation agent of legal persons
Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons,
Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement,
acting as (or arranging for another person to act as) a nominee shareholder for another person.”

Although the risks associated with trust service providers and company service providers, are related, this document focuses only on company service providers.

[1] FATF Recommendations 2023, page 127.

FATF's guidance for a risk-based *Approach for Trust and Company Service Providers*, published in 2019 states in the cover webpage to this guidance the following: "Trust and company service providers (TCSPs) are involved in a wide range of services and activities for their clients. These services include:
Acting as a director or secretary of a company or similar position
Providing a registered office or business address for a company
Acting as trustees of an express trusts, among others.
Not all of the persons and professionals active in this sector provide the same servicesi.

Company service providers can also take different forms, from individual firms to subsidiaries of large financial institutions. Criminals may seek company service providers' services to help them retain and expand control of proceeds of their crimes, while disguising the origin and ownership of these assets. Through the creation of shell companies or trusts, criminals can conceal their ownership and control, and create a veneer of legitimacy."

The Financial Intelligence Centre (FIC) conducted an assessment of the inherent money laundering and terrorist financing risks faced by trust service providers in South Africa, which was published in March 2022. At the time, only trust services providers (and not company service providers) were included as accountable institutions in the Financial Intelligence Centre Act, 2001, No. 38 of 2001 (FIC Act). However, as explained in paragraph 3 below, individuals and institutions performing certain services relating to the establishment and management of companies, were subsequently also included as accountable institutions under the FIC Act.

This sector risk assessment is specifically aimed at the providers of certain services, described in more detail hereunder, to companies. The FIC also conducted a sector risk assessment on accountants in so far as they provide the services prescribed in the FIC Act to trusts as well as companies. Although there may be duplications between the risks pertaining to accountants providing these services and the company service providers described in this document, it is important that a specific assessment be done in respect of the risks of company services providers, in particular.

This risk assessment report provides information on the company service providers' sector risk assessment and contains open-source information on the inherent national and international money laundering and terrorist financing risks of company service providers.

LIMITATIONS AND METHODOLOGY OF THE RISK ASSESSMENT

This sector risk assessment report addresses principally the inherent money laundering and terrorist financing risk factors facing company service providers in South Africa pertaining to products, services, clients, transactions, delivery channels and geographical areas, and some reference is made to the potential mitigation of these risks by complying with the FIC Act. The reference to company service providers in this document applies to individuals and institutions that are providing the services to companies described in item 2 of Schedule 1 of the FIC Act.

Although it is recognised that these risks could be mitigated by introducing processes and procedures in accordance with the requirements of the FIC Act, details of such mitigation factors were not included in this report. The report focuses on inherent risks.

2. OVERVIEW OF THE SECTOR AND LEGISLATIVE FRAMEWORK PERTAINING TO THE FIC ACT

2.1. Nature and regulation of the sector

2.1.1. Schedule 1, item 2 of the FIC Act was amended and took effect from Monday,19 December 2022 and now includes, in addition to trust service providers, company service providers (CSPs) as accountable institutions. Any institution performing any of the TCSP activities listed under item 2 of the FIC Act are regarded as an accountable institution. This report focuses on the money laundering and terrorist financing (ML and TF) risks of institutions and individuals performing the services referred to in Schedule 1, Item 2 of the FIC Act, **specifically in relation to companies**.

2.1.2. The FIC has issued guidance to the sector in the form of public compliance communication (PCC) 6A to clarify the scope of TCSPs, (which include company service providers). PCC 6A states that: "*A person who performs the activities of a TCSP, regardless of the professional accreditation they hold, is an accountable institution. Any person that carries on any one or more than one of the listed activities under amended item 2 of Schedule 1 is an accountable institution and is collectively*

referred to as a trust and company service provider (TCSP). Given that the TCSP definition is based on the activity that is performed by a person, it means that different professions are included in this category.

A TCSP in terms of item 2 of Schedule 1 to the FIC Act, is dependent on the activity performed. As such, a person that performs the business of a TCSP, regardless of the professional accreditation they hold, is an accountable institution and must register as a TCSP with the FIC. In practice, this means that financial institutions, legal professionals and accountants, among others, can meet the definition of a TCSP."

2.1.3. The FIC's approach is to include accountable institutions in the FIC Act based on those activities that pose the highest ML and TF risks and not merely based on the profession.

2.1.4. Schedule 1, item 2 of the FIC Act defines a TCSP as follows:

(a) A person who carries on the business of preparing for or carrying out, transactions for a client, where-

(i) the client is assisted in the planning or execution of-

(aa) the organisation of contributions necessary for the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008 (Act 71 of 2008);

(bb) the creation, operation or management of a company, or of an external company or of a foreign company, as defined in the Companies Act, 2008; or

(cc) the operation or management of a close corporation, as defined in the Close Corporations Act, 1984 (Act 69 of 1984.)

(b) A person who carries on the business of-

(i) acting for a client as a nominee as defined in the Companies Act, 2008 (Act 71 of 2008); or

(ii) arranging for another person to act for a client as such a nominee.

(c) A person who carries on the business of creating a trust arrangement for a client.

(d) A person who carries on the business of preparing for or carrying out transactions (including as a trustee) related to the investment, safe keeping, control or administering of trust property within the meaning of the Trust Property Control Act, 1998 (Act 57 of 1988).

2.1.5. PCC 6A further clarifies that TCSPs do not include the following:

- Activities that relate solely to the recording, or capturing of company data or information, including book-keeping functions
- The administrative submissions of information or data for legislative purposes, such as the filing of tax returns
- Activities that do not amount to decision-making within the client's business activities
- Activities that do not steer, impact or influence the client's business operations.

Although these activities do not constitute the business of a TCSP and are not subject to FIC Act obligations, it must always be noted that the reporting of suspicious and unusual transactions under section 29 of the FIC Act applies to all businesses.

The fulfilling of a statutory function, specifically the liquidation of an entity or the functions of business rescue, is not considered to meet the definition of operations or management of a client. However, if the client undergoing such a statutory application is themselves an accountable institution in terms of Schedule 1 to the FIC Act, this client would remain an accountable institution, and the appointed liquidator or business rescue practitioner would be required to make sure their client applies the full provisions of the FIC Act in relation to their (the client's) business activities.

The providers of services to companies, as explained in Item 2 of Schedule 1 of the FIC Act is not supervised by a statutory regulator in South Africa. Company service providers who also perform the function of an auditor are required to register with the Independent Regulatory Board for Auditors (IRBA) as an auditor. It is also possible that some company service providers may act as a financial services provider by providing

advisory and/or intermediary services in respect of a financial product. In such instances, they are required to register under the Financial Advisory and Intermediary Services Act, 2002, No. 37 of 2002 (FAIS Act).

3 INTERNATIONAL MONEY LAUNDERING RISKS, TERRORIST AND PROLIFERATION FINANCING RISKS

It is internationally recognised that criminals use company structures to conceal the identity of the real beneficiaries of such institutions and to hide the proceeds of illicit activities through such structures. This can be done through the formation of companies that may be established for this specific purpose or by creating complex legal structures – often with a footprint in jurisdictions that are known or suspected to facilitate or enable tax evasion or ML.

Institutions providing the company services described in Item 2 of Schedule 1 of the FIC Act are often involved in conducting research on business conditions, and with finding investors or generating capital as start-up capital for the formation of companies or for other purposes such as providing trade finance or project finance. Other services include the provision of advisory and administrative services on complex legal structures, including in jurisdictions with a questionable regulatory regime, in the registration of shell companies and acting as a nominee for shareholder(s) who wish to remain anonymous while exercising control over the nominee shareholders.

Company formation

Company formation services can include the following:

- Incorporating companies or other legal entities
- Acting or arranging for someone to act as company director, partner, or nominee shareholder or
- Providing a registered office or business address.

Criminals are attracted to anonymity and can use corporate vehicles to move and conceal illicit funds. The use of companies – particularly offshore ones – to act as corporate vehicles can distance the criminal from the corporate structure and make it harder for law enforcement to identify the origin of funds. Criminals may obscure association between

corporate structures by using a company formation agent to form multiple companies with different registered addresses. Criminals seeking a veneer of respectability may purchase companies with established histories and thereafter change the constitution of the company.

Shell companies

Another method that is internationally known to be used to hide the proceeds of crime is the creation of shell companies. Shells or shell companies are companies that do not have any business activity or operations, physical operations, assets, or employees. Although some shell companies may be perfectly legitimate business entities that are used to raise money and fund the operations of a startup company or to manage a merger or acquisition, others may involve criminals who want to hide illegal activities and/or avoid paying taxes. Many individuals do this by setting up shell companies in jurisdictions that guarantee anonymity, allowing them to make deposits and transfer money into different accounts. Shell companies also allow people to avoid reporting income and paying taxes.

Nominee shareholders

Nominee shareholders can be used as fronts for criminal activity in much the same way that nominee directors can - especially corporate directors. In South Africa, the Companies Act, 2008, No. 71 of 2008, allows that shares in a company may be held by a nominee on behalf of a beneficial owner. A nominee essentially acts as an agent for the true owner of the shares, but the nominee may be registered as the owner of those shares.

According to an article entitled *What is a nominee shareholder*[2], the 'use' of nominee shareholders in the United Kingdom includes the following activities:

- A large company may choose to use a nominee shareholder company to consolidate multiple diverse shareholders into one registered member. This nominee company can engage in corporate actions and otherwise act on behalf of the actual shareholders. This works in cases where the shareholders are willing to hand over some or all of their decision-making ability to the nominee.
- A foreign investor may also choose to use a nominee for simplicity and to reduce costs.
- A financial institution or stockbroker buys and holds shares for a client. They act as nominee shareholders because it would be costly and time-consuming to register the

[2] www.informdirect.co.uk/shares/nominee

client as the shareholder for every share transaction that takes place. Strong bonds of trust, usually codified and documented, ensure that the beneficial owner has full access to and control over their shares.

- Confidentiality rather than obfuscation. For example, a politician or other public figure may wish to conceal their interest in a company or their wealth in general, to avoid possible reputational damage.

The above examples indicate that, although the use of nominees may be legitimate, it can be abused by criminals or other individuals to obscure the real ownership or control of a corporate and to hide the proceeds of illegitimate activities.

An international example where the true identity of beneficial owners was concealed can be found in the 2016 release of the 'Panama papers', followed by the 2021 release of the 'Pandora Papers'. In the Panama Paper disclosure, 11.5 million leaked documents containing personal financial information about wealthy individuals and public figures that had previously been kept private, were disclosed. The reason for such privacy could range from simply a desire for privacy, especially for the rich and famous, to hiding wealth from family members, and/or to hiding wealth because it was generated through criminal activities or to prevent paying taxes.

Incidents such as the Panama papers and the Pandora papers highlighted the importance internationally of company service providers as gatekeepers to the financial system to prevent criminals from hiding the source of their wealth and enjoying the proceeds of their criminal activities.

4. REGISTRATION AND REPORTING BY COMPANY SERVICE PROVIDERS UNDER THE FIC ACT

4.1 During the financial year from 1 April 2022 to 31 March 2023, all trust and company service providers submitted 254 cash threshold reports and 17 suspicious and unusual transaction reports. It must, however, be noted that up to 19 December 2022, only trust service providers had an obligation to register with the FIC and submit cash threshold reports. It is likely that the number of regulatory reports to the FIC will increase following the obligation of all trust and company service providers to register with the FIC.

4.2 The number of active registered company service providers on 17 December 2023 was 943. It must be noted that this number may include institutions that are conducting the business of a company service provider, but that may also be registered under other Items in Schedule 1 of the FIC Act, such as a legal practitioner or a financial services provider.

5. RISKS BASED ON RESEARCH

The risk factors used in this report align with those used in the FIC's Guidance Note 7 and also includes a short reference to terrorist financing risk. Guidance Note 7 is available on www.fic.gov.za. Company service providers must consider these factors when conducting their daily business.

a. Products and services risks

i. Certain products and services are regarded as posing a higher risk for money laundering purposes.

ii. The products and services provided by company services providers that are internationally recognised (and also mentioned under paragraph 4 above) as more likely to be abused by criminals in the ML process include:

- Company formation – Criminals may attempt to confuse or disguise the links between the proceeds of a crime and the perpetrator through the formation of corporate vehicles or other complex legal arrangements. Company service providers must determine the business activities of the company, its subsidiaries, its shareholding structure and, where applicable, the purpose of shell company registrations in the structure.
- Trustees or directors of companies – Company service providers acting in the capacity of independent trustees or directors, are required to obtain the necessary information about the nature of the transactions of the company, the natural persons or legal persons that are parties to transactions with the company and ascertain whether the transactions make economic or commercial sense. They must also determine the origin of the funds received by the company to make an informed decision about the ML and TF risks associated with such a transaction.
- Financing of companies – To establish the potential ML and TF risks associated with the formation of a company, company service providers involved in the raising of capital for new and existing companies should verify the origins of the

capital, establish the identity of the investors in the case of potentially higher risks and verify the need and use of the capital.

iii. The method of payment for services provided by company service providers could, in some instances, also be a channel for ML. The use of cash usually points to a higher risk for ML because it is more difficult to trace its origin.

iv. Company service providers should consider instances where there is a lack of original documentation or where such documentation is difficult to obtain as a potentially higher risk area.

v. Transactions that appear to be unrelated to the business of the client should be subject to additional scrutiny. In instances where the business of the client of the company service provider is under financial strain, the client may resort to other sources of income and in such instances the company service provider should, if necessary, obtain additional information on the transaction to verify its legitimacy.

vi. Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

vii. Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

b. Client risks

i. Listed as accountable institutions under the FIC Act, CSPs are required to assess, identify, understand and then risk-rate the inherent ML and TF risks associated with their clients. Some clients, such as domestic politically exposed persons (DPEPs), foreign politically exposed persons (FPEPs), prominent influential persons (PIPs), complex legal structures or foreigners, potentially pose a higher risk for ML, depending on the identified circumstances. Company service providers should consider enhanced due diligence on such clients and should also, as part of their risk assessment of all clients, determine the possibility of such politically exposed person(s) being the ultimate beneficial owners or decision makers behind a corporate structure.

ii. The establishment of complex local or international structures involving legal persons (companies) and partnerships as part of a group structure that does not make economic sense, or sudden changes in ownership of companies, could possibly be aimed at concealing the ultimate beneficial owners of such legal persons and arrangements. Enhanced due diligence should be considered in such instances, in particular if part of

such structure is established in a jurisdiction that is suspected or known to be a high-risk area or a high-secrecy jurisdiction.

iii. Although company service providers are not expected to have an in-depth knowledge of the business of their clients at the company formation stage, a basic understanding of such business activities and future plans will place the company service provider in a better position to identify and report suspicious activities.

iv. Where clients are hesitant to allow the company service provider access to its business premises or its employees but, expect advisory services to be rendered, it may make it difficult for the accountant to verify the financial and corporate information provided by the client. Such clients should be treated as potentially high risk.

v. When dealing with their clients, company service providers should be aware of*, inter alia*, the following possible scenarios pertaining to the nature and behaviour of the clients that could point to possible ML:

- Clients trying to conceal their identities;
- Transactions or legal entity formations that involves large amounts or that are inconsistent with the client's stated income, occupation or interests or where there is no legitimate or economic reason for such transaction or formation;
- Clients use an unusual source of funds to transact or to finance legal entities;
- Clients cease their business relationships upon a request for customer due diligence (CDD) information;
- Clients requesting funds to be paid into or from a third-party account that have no obvious link to the client;
- Clients requesting a company to be registered in the name of another institution or person with no valid reason for such request;
- Clients that are difficult to reach or hesitant to provide customer due diligence information and information on their business activities;
- Clients requesting informal arrangements to be made such as using friends or family members as registered owners or directors without an acceptable explanation;
- Sudden activity from a previously dormant client without a clear explanation.

c. Transaction risks

i. International literature and research indicate that criminals can potentially use company service providers acting as corporate advisors to transact on their behalf, thereby creating an impression of legitimacy to transactions involving the proceeds of crime. Monitoring the nature and purpose of these transactions, their monetary worth and the means of payments involved, will contribute to understanding and monitoring the ML risks associated with such transactions.

ii. Examples of transactions that are potentially high risk for ML include the use of cash or crypto currencies, including to finance a legal entity, the reversing of transactions with a request to repay funds already paid and transactions that do not make economic sense. Company service providers should be aware of the potential ML risks associated with such transactions and take the necessary steps to mitigate such risks.

iii. In some instances, requests for company formations or company financing may be split unnecessarily across different providers of such services to prevent anyone involved in the transactions getting a full picture and raise suspicion. Company service providers must attempt to obtain additional information if it is suspected that a transaction or company formation forms part of a larger range of transactions or corporate structure.

iv. The unnecessary use of loans by the client of a company service provider in starting or expanding a business, could be done to conceal the origin of illegal funds, where the company service provider notes that such loans are being repaid earlier than originally agreed upon.

v. When advising on transactions relating to mergers and acquisitions, a company service provider must consider whether a transaction makes economic and business sense and whether the prices of assets and other legal entities obtained or disposed of, are market-related. The use of cash, if applicable, for any transaction, without a proper explanation thereof, must also be considered for enhanced due diligence measures by a company service provider. Although cash is still used extensively in South Africa, large amounts of cash for no specific reason could be used to conceal the origin of the funds and should be treated as potentially suspicious.

d. Risks relating to delivery channels

i. Company service providers must be aware of the delivery channels they use to attract and deal with clients. Delivery channels that may obscure or conceal the true identity of the client, or that result in clients not being on-boarded face-to-face, may increase

the risk of the company service provider being abused by criminals to launder the proceeds of crime. Where an intermediary is used to on-board clients or the client is represented by an agent or an intermediary, or a client is hesitant to provide the necessary information, a company service provider must do proper due diligence on the intermediary or agent and its business and must be familiar with the risk-mitigation processes and procedures the intermediary may have in place.

ii. Various forms of technology are used to advertise services and conduct business. Where social media platforms and third-party service providers are used to share information on products or services or to on-board clients, a company service provider must ensure that such clients are properly identified and verified and that all the relevant information pertaining to the risks posed by such clients are obtained.

e. Geographic risk

i. Some foreign jurisdictions pose a higher risk for ML. It is important that company service providers be aware of the risks posed by clients from these jurisdictions or where company structures include such jurisdictions and that they have the necessary risk mitigation processes in place. This risk is exacerbated by the fact that transactions can take place electronically across regions and national jurisdictions and that such transactions often require the services of company service providers.

ii. The geographic location and services provided by company service providers are also important factors for determining ultimate ML risks.

iii. Company service providers must be aware of the potential higher risks posed by clients (including their directors or trustees, shareholders and branches or subsidiaries), transactions or counterparties involving types of countries that are:

- Subject to a travel ban;
- Regarded by FATF as a high ML risk;
- Regarded as high-secrecy jurisdictions;
- Regarded as tax havens;
- Known to have high levels of organised crime, corruption or from which terrorist organisations are known to operate;
- Subject to United Nations Security Council sanctions;
- Generally known to provide funding or support to terrorist organisations or that host such organisations, including their neighbouring countries;

- Regarded as having weak governance systems, law enforcement and regulatory regimes, including countries regarded by FATF as having weak AML and CFT regimes.

This includes requests from clients to register companies or subsidiaries or holding companies in such areas.

iv. The transfer of the seat of a company to another jurisdiction without any genuine economic activity in the country of destination poses a risk of creation of shell companies which might be used to obscure beneficial ownership.

f. Terrorist financing and proliferation financing risks

i. Where company service providers provide services to non-profit companies and non-governmental organisations, they should ensure that the funds used are in accordance with the stated objectives of these organisations.

ii. Company service providers should also be aware of the appropriate compliance obligations referred to in sections 26A and 28A of the FIC Act which relate to the screening of clients to ensure that clients are not included in United Nations Security Council targeted financial sanctions lists. For proper risk assessment, this requirement could, in some instances, be extended to the branches, holding companies and subsidiaries that are being established as part of the company formation process, as well as their directors and senior management.

iii. Company service providers must know how to access the referenced targeted financial sanctions list and determine whether they are conducting business with individuals and institutions on such lists, including individuals and institutions that are involved in the larger company structures of clients.

iv. Requests for company services from offshore clients or local clients with offshore operations may possibly carry a higher risk for TF and financing the proliferation of weapons of mass destruction, depending on the nature of the client's business and their geographic location. Company service providers must be aware of such higher risk areas and the areas that are regarded as having a higher risk and they must take the necessary steps to mitigate and manage these risks.

v. Clients who are involved in the manufacturing or distribution of any product that may be used in the proliferation of weapons of mass destruction or that are exporting to countries regarded as high risk for such activities, including countries that are

geographically close to high-risk countries, should be considered for enhanced due diligence.

vi. Where a company service provider identifies payment from or to the client for travel arrangements to or from high-risk terrorist jurisdictions, enhanced due diligence must be applied.

vii. Clients who are claiming to provide loans or finance to individuals and institutions, particularly in high-risk areas, need to be scrutinised to determine whether such "loans" are being repaid. This includes instances where the client makes funds available for establishing companies in such jurisdictions.

viii. Clients who appear to have extremist political, religious or world views, may potentially carry a higher risk for terrorist financing and may have to be subjected to enhanced due diligence.

6. INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITY FOR THE SECTOR

In its document *Money laundering using Trust and Company Service Providers*, published in October 2010, FATF listed the scenarios below as possible indicators of ML. This list was derived from responses to a FATF questionnaire and case studies they featured in the document. Although the FATF document was published in 2010, the possible scenarios they mentioned are still relevant and company service providers need to consider this in their day-to-day business:

- Transactions that require the use of complex and opaque legal entities and arrangements.
- The payment of "consultancy fees" to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies.
- The transfer of funds in the form of "loans" to individuals from trusts and non-bank shell companies. These non-traditional "loans" then facilitate a system of regular transfers to these corporate vehicles from the "borrowing" individuals in the form of "loan repayments".
- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain or submit to competent authorities' information on the beneficial ownership of corporate structures formed by them.

- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs.
- The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws.
- The use by prospective clients of nominee agreements to hide from the TCSP the beneficial ownership of client companies.
- The carrying out of multiple intercompany loan transactions and/or multijurisdictional wire transfers that have no apparent legal or commercial purpose.
- Clients who require the use of pre-constituted shell companies in jurisdictions that allow their use but do not require updating of ownership information and
- TCSPs that market themselves and/or their jurisdictions as facilitating anonymity and disguised asset ownership.

In addition to the scenarios in the FATF document, company service providers should also consider the following scenarios as potentially high risk**:**

- The use of cash for payment of services.
- Anonymity of clients and transactions that are complex in nature.
- New payment technologies e.g. crypto currencies.
- High-risk customers and jurisdictions such as clients linked to institutions or jurisdictions on the United Nations Security Council targeted financial sanctions lists.
- DPEPs, FPEPs, PIPs, and high-net-worth individuals which are internationally regarded as high-risk clients.
- Organised crime can use company service providers to conceal the proceeds of crime, obscure ultimate ownership through complex layers and legal entity structures, avoid paying tax, work around financial regulatory controls, create a veneer of legitimacy to criminal activity, create distance between criminal entities and their illicit income or wealth, avoid detection and confiscation of assets, and hinder law enforcement investigations.
- Clients who offer to pay extraordinary fees for services that would not warrant such fees.
- Payments from non-associated or unknown third parties and payments for fees in cash where this practice is not typical.
- Where company service providers, including those acting as financial intermediaries, physically handle the receipt and transmission of funds through accounts they control.

They may be requested to transfer assets between parties in an unusually short period, thereby hindering the know-your-client process and potentially contribute to concealing the beneficial ownership of the client or other parties to the transactions(s) from competent authorities.

- Funds are received from or sent to a foreign country when there is no apparent connection between the country and the client.
- The client is using multiple bank accounts or foreign accounts without good reason.
- Possible involvement of DPEPs, FPEPs and PIPs in instances where the entity, structure or relationships of the client make it difficult to identify its beneficial owner or controlling interests e.g., the unexplained use of legal persons or legal arrangements.
- Instances where clients, for no apparent reasons, change the way in which transactions are concluded or change their instructions to the company service provider on short notice or in a manner that does not make economic sense.

7. CONCLUSIONS

a. Based on the international experience and research, the risk factors described above and the range of services they offer, it is evident that company service providers are potentially at high risk of being exposed to the inherent risk of ML. They should therefore take all the necessary precautionary steps to reduce the risk of being exposed to abuse by criminals who want to launder the proceeds of crime through the sector.

b. Overall, the inherent risk of ML for company service providers based on national and international experience, is classified as high, particularly in respect of the formation of complex structures and the involvement of high-risk jurisdictions.

c. Company service providers who provide services to non-profit organisations and companies are at a higher inherent terrorist financing risk.

d. The provisions of the FIC Act are aimed at making it more difficult for criminals to launder the proceeds of criminal activities through accountable institutions. It is envisaged that the specific inclusion of company service providers would be a deterrent for criminals wishing to use this avenue to launder illicit funds.