GUIDANCE ON

SUSPICIOUS ACTIVITY / SUSPICIOUS TRANSACTION REPORTING

Financial Intelligence Agency | Turks & Caicos Islands

REVISED FIA-SARGUIDE-0222 V2.0

Financial Intelligence Agency
Turks & Caicos Islands

Guidance on Suspicious Activity / Suspicious Transaction Reporting

REVISED FIA-SARGUIDE-0222 V2.0

This is a Financial Intelligence Agency of the Turks & Caicos Islands (FIA-TCI) product for reporting entities, law enforcement authorities, supervisory and competent authorities, and the public regarding the preparation of Suspicious Transaction/Activity Reports (STRs/SARs) for submission to the FIA-TCI.

Copyright

Website: www.fia.tc

Revised Publication February 2022. FIA-SARGUIDE-0222 V2.0

Cover Photo: Romello Williams (Unsplash.com); Retrieval: February 7, 2022

Table of Contents

Table of Contents *(cont'd)*

Table of Contents *(cont'd)*

Table of Contents *(cont'd)*

Table of Contents *(cont'd)*

Guidance on Suspicious Activity / Suspicious Transaction Reporting

1.0 INTRODUCTION

The Proceeds of Crime Ordinance Chapter 3.15 hereafter "POCO," the Prevention of Terrorism Ordinance Chapter 3.21 hereafter "POTO" and the Financial Intelligence Agency Ordinance Chapter 3.20 hereafter “FIAO” establish the legal framework for the reporting of suspicious activity or suspicious transactions regarding money laundering and terrorist financing to the Financial Intelligence Agency hereafter the "FIA." To assist relevant entities and individuals, this guidance document contains general information which is intended to assist those meeting the reporting requirement and persons who want to report suspicious activities and transactions related to suspected money laundering and terrorist financing. This Guidance should not be interpreted as legal advice or a replacement to the POCO, the POTO and any subsequent amendments to both Ordinances, the Anti-Money Laundering and Prevention of Terrorist Financing (AML/PTF) Regulations 2010 and the Anti-Money Laundering and Prevention of Terrorist Financing (AML/PTF) Code 2011; all of which should be referenced in conjunction with this guidance.

This guidance document provides information on Suspicious Activity Reports/ Suspicious Transaction Reports (SARs/ STRs) and Terrorist Property Report (TPR). It describes who must file, when to submit and instructions on completing the SAR/ STR and TPR forms. It also contains indicators of suspicious activities and transactions, which you may find useful when used in conjunction with your own internal guidelines and assessments on whether a transaction or activity is suspicious or warrants reporting to the FIA.

The guidance provided herein cannot anticipate all circumstances and therefore is not exhaustive. Where permitted by the Anti- Money Laundering/ Prevention of Terrorist Financing AML/PTF Regulations 2010 or the AML/PTF Code 2011, regulated entities are expected to adopt an appropriate risk-based approach to AML/CFT. This document is meant to be a guide, it should be noted that the definitive source of information on the law must always be the Ordinances and Regulations. If in doubt, the Ordinances should be referred to, or legal advice sought.

2.0 MONEY LAUNDERING

Money Laundering in general terms is the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have been derived from legitimate sources. The proceeds may include funds or other properties derived from activities such as fraud, corruption, drug trafficking, human trafficking and smuggling, arms trafficking and smuggling, white collar crimes and other conduct designated as predicate offences to money laundering.

The process of Money Laundering can take place at three distinct stages; placement, layering and integration with the likelihood of overlapping amongst the stages. However, it is important to note that in some transactions all three stages may not be present for example where money may already be in the financial system and is moved from account to account.

2.1 PLACEMENT STAGE

The placement stage represents the initial entry of the illicit proceeds of crime into the financial system. This stage can be the most difficult for criminals as they try to place criminally derived funds into the financial system since they encounter gatekeepers who act as intermediaries that can prevent or disrupt criminals' access to the financial system. Examples of gatekeepers include accountants, lawyers, corporate services providers, company formation agents, bank staff and other financial intermediaries in the financial services sector.

These gatekeepers are usually subject to regulation and are required to adhere to laws and regulations designed to ensure that only legal transactions are permitted into the financial system. Money launderers are most vulnerable of being caught at this stage as large amounts of cash can raise suspicion to staff and agents in the financial services sector, attracting unwanted attention from regulatory bodies and law enforcement. Getting the funds into the financial system provides opportunities to gain the appearance of legitimacy, for example depositing the proceeds of crime into a bank, which is then used to purchase luxury items, real estate, and other assets.

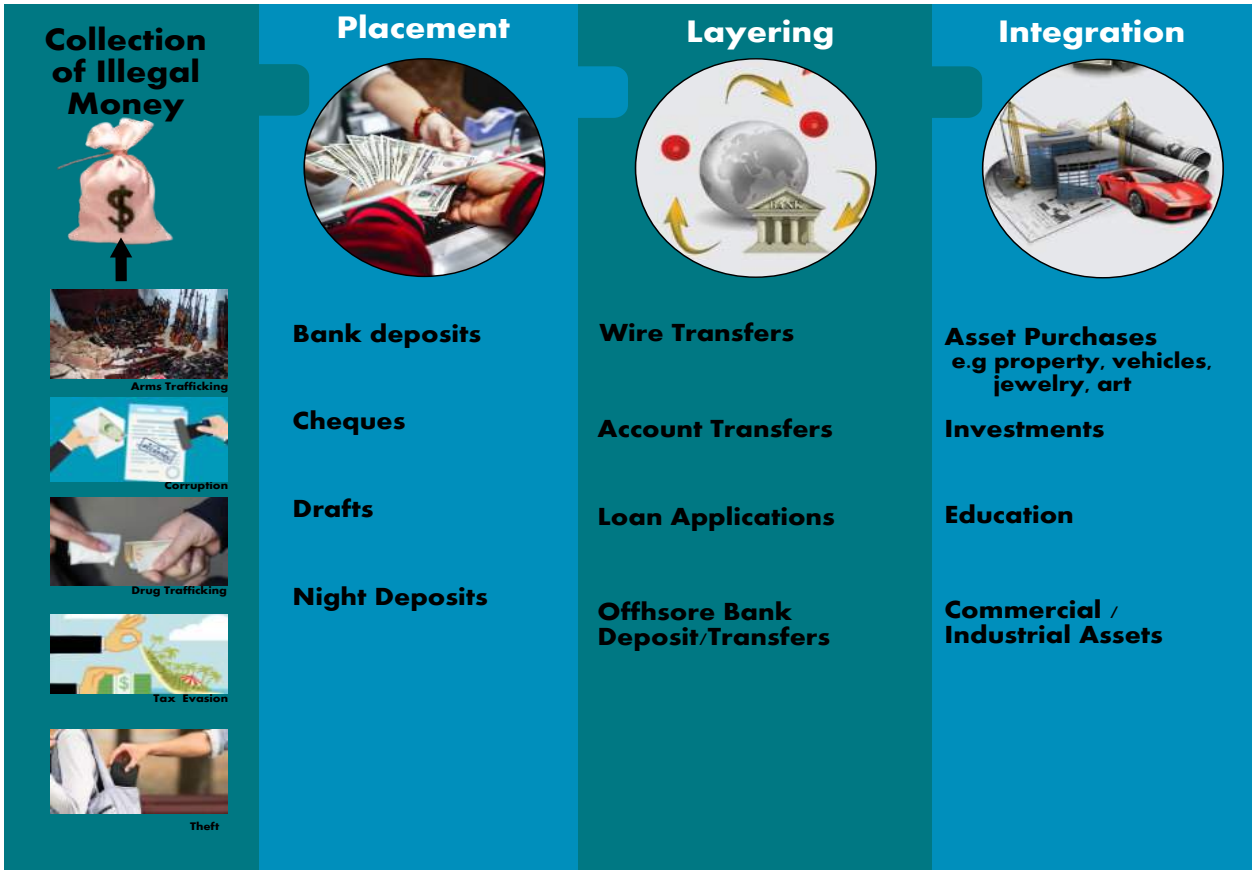
2.2 LAYERING STAGE

This stage further distances the funds from the original source making it harder for law enforcement to trace. The layering stage can be complex. It often entails the international movement of funds, as complex structures are utilised to launder the money. These structures include passing funds through various accounts whether onshore or offshore or to accounts in the names of different persons; changing money from one currency to another, the purchase of high value items or assets such as vehicles, yachts, aircraft, real estate, jewellery, companies and stocks. At this stage, the source and ownership of the funds becomes difficult to trace as funds are comingled with legitimate finances through the sophisticated layering of financial transactions that obscure the audit trail and sever any links to the original crimes from which the funds were derived.

2.3 INTEGRATION STAGE

The integration stage is where the funds are re-introduced in the financial system appearing as though they were derived from legitimate transactions or sources. Having been placed initially as cash into the financial system and layered through various financial transactions, the proceeds from criminal activities are now fully integrated and can be utilised for any financial transactions without raising suspicions. For example, the launderer during the layering stage purchased a property in country B which was put in a trust, and a few years later the property is sold. The funds from the sale of the property are transferred into the launderer bank's account. The funds now appear to come from a legitimate source (the sale of the property) and the launderer may develop a sense of validation in the use of their 'legitimately' obtained proceeds.

Money Laundering Process



Source: FIA (2022)

3.0 TERRORIST FINANCING

Terrorist Financing is the conduct of wilfully providing or collecting funds by any means, directly or indirectly, with the knowledge or intention that they are to be used or should be used in full or in part to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of a person who finances terrorism.[1]

Unlike money laundering where funds are mostly derived from illicit activities, funds used for terrorist financing can be sourced from both legitimate and illicit means. Funds can be raised through legitimate sources such as donations from individuals and countries, and profits from businesses and charitable organizations. Funds can also be derived from illicit sources such as drug trafficking, human

1. Sec.2 "Interpretation" Proceeds of Crime Ordinance CAP 3.15

smuggling and trafficking, smuggling of weapons, precious stones and other goods, various types of fraud and many other crimes from which there can be financial gain. Terrorists utilise techniques similar to those of money launders to avoid detection, protect the identity of their sponsors and the eventual beneficiaries. Further, the financial transactions associated with terrorist financing are usually smaller amounts, making the detection and tracking of these funds more difficult.

Reporting entities should apply additional due diligence measures when establishing a business relationship with individuals and legal entities from or connected to countries which feature in terrorism, terrorist financing and related lists such as the United Nations sanctions list.

4.0 REPORTING ENTITIES REQUIRED TO REPORT SUSPICIOUS ACTIVITY OR TRANSACTIONS

The following reporting entities are required to report suspicious activity or transactions when they know or suspect or have reasonable grounds for suspicion of Money Laundering or Terrorist Financing Offences[2] as mandated under the POCO and the POTO.[3]

4.1 REGULATED BUSINESSES

- a bank licensed under section 4(2) (a) & (b) of the Banking Ordinance;
- a trust company licensed under section 4 of the Trustees Licensing Ordinance;
- an insurance company licensed under the Insurance Ordinance;
- a person or company licensed under the Mutual Fund Ordinance;
- a person or company licensed under Money Transmitters Ordinance;
- investment dealer or advisor licensed under the Investment Dealers (Licensing Ordinance);

2. Money Laundering and Terrorist Financing Offences are specified under Sections 124-126 of the POCO (Revised Dec. 2014) and Sections 10-13 of the POTO respectively.

3. Requirements for for reporting are found under Section 127 & 128 of the POCO and Section 14 of the POTO respectively.

- providers of company services under the Company Management (Licensing) Ordinance.

4.2 FINANCIAL BUSINESS

The following are listed as financial[4] under Schedule 2 of the Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010:

4.2.1 Money Services Business

The business of providing the following services

- money transmission,
- cheque cashing,
- currency exchange,
- the issuance, sale or redemption of money orders or traveller's cheques and such other services as the Governor in Cabinet may specify by notice published in the Gazette.

4.2.2 Trust and Company Service Providers

Persons who prepare for and carry out the transactions for a client including but not limited to:

- acting as formation agent of legal persons,
- acting as secretary of a company, a partner of a partnership, or similar position in relation to other legal persons or arranging for another person to act in one of the forgoing capacities or as director of a company,
- providing a business, accommodation, correspondence or administration address for a company, partnership or any other legal person or arrangement,

4. Financial Business has its meaning specified in the Anti-Money Laundering and Prevention of Terrorist Financing Regulations.

- ▷ acting as or arranging for another person to act as a nominee shareholder for another person.

4.2.3 A person or entity who conducts as a business the following on behalf of a customer

- ▷ lending, including consumer credit, mortgage credit, and financing or commercial transactions
- ▷ financial leasing
- ▷ issuing and managing means of payment including credit and debit cards, cheques travellers' cheques, money orders, and bankers' draft and electronic money
- ▷ financial guarantees or commitments
- ▷ participation in securities issues and provision services related to such issues
- ▷ providing advice on capital structure, industrial strategy and related questions and advice services to mergers and the purchase of undertakings
- ▷ safekeeping and administrations of cash
- ▷ investing administering or managing funds or money
- ▷ money broking.

4.2.4 A person or entity who as a business, trades for his own account or for the account of customers

Money markets instruments, including cheques, bills, certificates of deposits and derivatives

- ▷ foreign exchange
- ▷ exchange, interest rate and index instruments
- ▷ financial futures and options

- commodities futures or shares and other transferrable securities.

4.2.5 Lawyers, other independent legal professional, accountants and auditing service providers.

A person who provides or carry out transactions for their clients including but not limited to:

- buying and selling of real estate and business entities
- the managing of client's money;
- opening or managing of bank, savings or securities accounts;
- organisation of contribution necessary for creation, operations or management of companies;
- creation, operation of management of trusts and similar structures that requires a license under the Trustees Licensing Ordinance or Company Management (licensing) Ordinance.

Note: an attorney at law or other independent legal professional is not required to disclose any information during communication(s) between a client in privileged circumstances regarding offering legal advice. However, this does not apply in situations where legal advice is being sought with the intention of furthering a criminal purpose.

4.2.6 High Value Dealers

High value dealers[5] include motor vehicle dealers/salespersons, jewellers, antique and fine art dealers, boat dealers, builders, bathroom and kitchen suppliers and auctioneers and brokers). A person who by way of business trades in goods, precious metals or stones who receives, in respect of any transaction executed in a single operation or in several linked operations, a payment or payments of cash of:

- in the case of precious metals or stones at least $15,000.00, or equivalent in another currency,
- in the case of any other goods, at least $50,000.00, or the equivalent in another currency.

5. Section 2 of the AML/PTF Regulations 2010.

4.2.7 Real Estate Companies and Agents

Persons involved in transactions for or on behalf of client concerning the buying, leasing or selling of real estate in relation to both the purchasers and vendors of property.

4.2.8 Casinos

Any person who operates by way of business whenever a transaction involves accepting a total cash payment of $3,000.00 or more or equivalent in another currency in a single transaction or multiple transactions that are linked.

4.2.9 Entities that manage or support the creation of legal persons, partnership or arrangements.

Such persons have a duty to report suspicion of Money laundering or terrorist Financing to the FIA. The "Duty to disclose knowledge or suspicion of Money Laundering" is found under Sec. 127 of the Proceeds of Crime Ordinance which refers to "relevant business." Under the AML-PFT Regulations 2010, "relevant business" means a business which, if carried on by a person, would result in that person being a "financial business." For the purpose of explaining this relationship to legal persons please refer to Schedule 2 (1) (c i, ii, iii) of the AML-PTF Regulations 2010. The AML-CFT Code 2011 outlines the obligations for such businesses as it relates to the Customer Due Diligence (CDD) requirements to be carried out on their customers or prospective customers.

- Money markets instruments, including cheques, bills, certificates of deposits and derivatives
- foreign exchange
- exchange, interest rate and index instruments
- financial futures and options
- commodities futures or shares and other transferable securities.

5.0 WHAT IS A SUSPICIOUS TRANSACTION/ACTIVITY?

Simply put, this is a transaction or activity where there is suspicion or reasonable grounds to believe the commission of a money laundering or terrorist financing offence has occurred, or reasonable grounds to suspect there is an attempt to commit a money laundering or terrorist financing offence.

At the stage when a transaction/activity is deemed suspicious, it is important that the Money Laundering Reporting Officer (MLRO) put into context other factors of assessing such suspicion. Transactions can be evaluated as to whether they seem proper at the time and within the normal activities of that specific business, the general knowledge of the customer, patterns and volumes of transactions, previous instructional patterns and other possible connections linking accounts to accounts or customers to customers and so on. Importantly, consider whether the transaction or attempt thereof is consistent with those conducted before or comparable to other businesses in that specific area or not.

Other areas of significance in the assessment of suspicion should include factors based on your knowledge of the customer or client's business, financial history and background. Reasonable grounds or suspicion will also depend on your own internal compliance regime, assessment, evaluation and CDD information.

5.1 INFLUENCING FACTORS LEADING TO SUSPICION OR REASONABLE DOUBT ARE AS FOLLOWS BUT NOT EXHAUSTIVE

- Unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- use of false documents to open an account;
- inability, failure or reluctance of a customer/ client to provide necessary due diligence information;
- account activity or income inconsistent with the customer's profile;
- unusually large numbers /volumes of wire transfers or repetitive wire transfer patterns inconsistent with normal activity;

- business transactions with persons (natural or legal) connected to high-risk country or countries known for drug trafficking, high levels of organised crime, vulnerability to corruption or terrorist activity, lax Anti Money Laundering/ Combating the Financing of Terrorism (AML/ CFT) regime or which do not apply or insufficiently applies the Financial Action Task Force (FATF) international standards or combating money laundering and the financing of terrorism and proliferation.

- complex/ unusual series of transactions indicative of layering between multiple accounts, individuals, banks and jurisdictions.

5.2 TRANSACTIONS USED IN CONTEXT INCLUDES

- Transactions of any amount and value: no monetary threshold is required for a transaction to be deemed suspicious;

- occasional transaction: that is, a transaction carried out otherwise than as part of a business relationship;

- two or more one-off transactions seemingly linked;

- attempted transaction: one which the client or customer intended to conduct but subsequent action(s) by you or the client cause it not to be carried out or completed.

5.3 EXAMPLES OF ATTEMPTED TRANSACTIONS

- A financial institution refuses to process a wire transfer because the customer fails to provide the source of funds details.

- A Money Services Business declines to process a request to transfer a large amount of cash because the customer refuses to provide identification when requested or has met the threshold on the amount of funds allowed to wire transfer for a specific period.

- A client makes an offer to buy a property on sale through a real estate agent however the client wants to pay the amount in cash, the real estate agent declines the transaction.

5.4 THE IMPORTANCE OF FILING SARS/STRS

Filing reports of suspicious activity or transactions to the Financial Intelligence Agency (FIA) is an important step in the combating of money laundering and terrorist financing. According to Sec. 127 of the Proceeds of Crime Ordinance it speaks of a duty to disclose this information to the FIA as soon as it is practicable. The filing of SARs reflects the level of commitment and cooperation of reporting entities in:

- Identifying potential and actual criminal activity related to money laundering, terrorist financing offences, and other connected financial crimes;
- detecting, disrupting and preventing the flow of illicit funds;
- identifying emerging threats through analysis of patterns and trends;
- it highlights the MLRO's understanding and application of AML/CFT /PF measures and demonstrates their awareness of the risk to their various businesses and their ability to identify red flags when they occur;
- it is a duty under the Proceeds of Crime Ordinance and the Prevention of Terrorism Ordinance.
- assisting law makers and policy makers in the implementation of laws and regulations to combat money laundering, terrorist financing and proliferation financing.

5.5 WHEN TO SUBMIT A SAR/STR TO THE FIA

When the money laundering reporting officer has knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing, he or she has a duty to submit to the Financial Intelligence Agency suspicious activity reports as soon **as practicable and in any event within twenty -four (24) hours.**[6]

6. See section 32 (1) under the AML/CFT Code 2011.

5.6 HOW TO IDENTIFY A SUSPICIOUS TRANSACTION OR SUSPICIOUS ACTIVITY

The lists on the following pages are comprised of general indicators commonly called "red flags" geared towards assisting stakeholders in the financial and non-financial sectors to recognise or identify suspicious transactions and activities which give rise to suspicion or reasonable grounds for suspicion of money laundering and terrorist financing. Indicators on their own do not mean that a person has committed a money laundering or terrorist financing offence. MLROs should consider additional factors such as the client's occupation, business, financial history, transactional patterns, the original or recipient country referencing the transaction along with his/ her own internal scrutiny to determine whether it warrants making a suspicious activity/ transaction report.

6.0 GUIDANCE ON TERRORIST FINANCING

Indicators which may point to or relate to Terrorist Financing in some cases share similarities to those relating to money laundering. Funds derived from legitimate sources or proceeds of crimes/unlawful activities can be used to fund Terrorist activities. Hence, this Guidance document combines indicators for aspects of both Money Laundering and Terrorist Financing.

In addition to suspicion with regard to transactions or activities carried out or attempted by natural or legal persons, entities within the relevant sectors must be wary of establishing business relationships or handling of transactions with individuals, entities or organisations listed as having ties to terrorist financing or terrorism as declared by the Security Council of the United Nations (UN) - namely Resolution 1267[7] and its subsequent amendments and other such resolutions or imposed sanctions by the European Union, the Turks and Caicos Islands or other countries. It is important that entities do not engage or establish any business relationships with any individual, or entity or organisation that is featured on such listings.

If after carrying out a transaction you become aware that it was conducted by or on behalf of an entity or individual on the designated list, you must submit a terrorist property report to the FIA on the prescribed form (See Appendix B). If there is

7. The names of individuals, entities or organisations can be found at http://www.un.org/sc/committees/1267/aq_sanctions_lists.html or you can access the list directly in PDF format at http://www.un.org/sc/committees/1267/1267.pdf.

suspicion that a completed or attempted transaction is related to terrorist financing, you must make a report to the police, a customs officer or the FIA without delay.

Reports in relation to knowledge or suspicion of terrorist financing whether completed, attempted or denied extend to reports regarding individuals or entities that have been prosecuted for such other matters in relation to money laundering, terrorist financing and other serious offences such as fraud, whether these prosecutions occurred within or outside the islands.

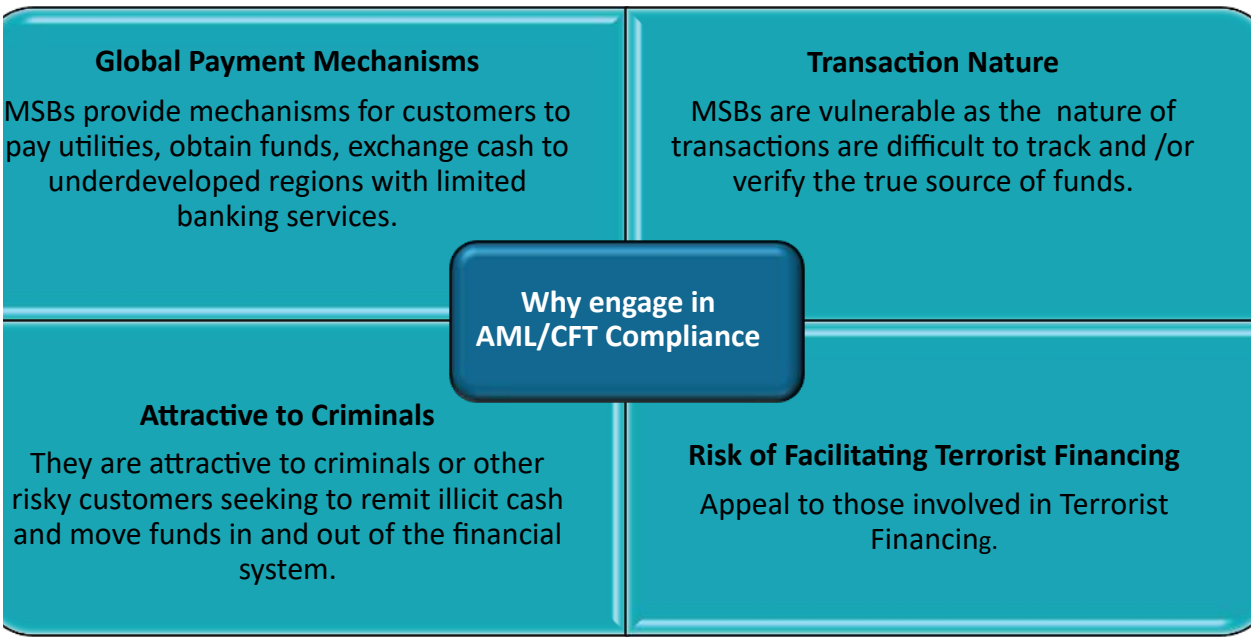
If you suspect or are aware that an act attempted, in progress or completed is related to terrorism you are required to report it to the police.

7.0 GUIDANCE, MITIGATING RISK AND INDICATORS BY SECTORS

The following charts are provided as a guide and as such will not reflect every possible scenario. It should also be viewed within the context as it would relate to the entity.

7.1 MONEY SERVICES BUSINESSES (MSB)

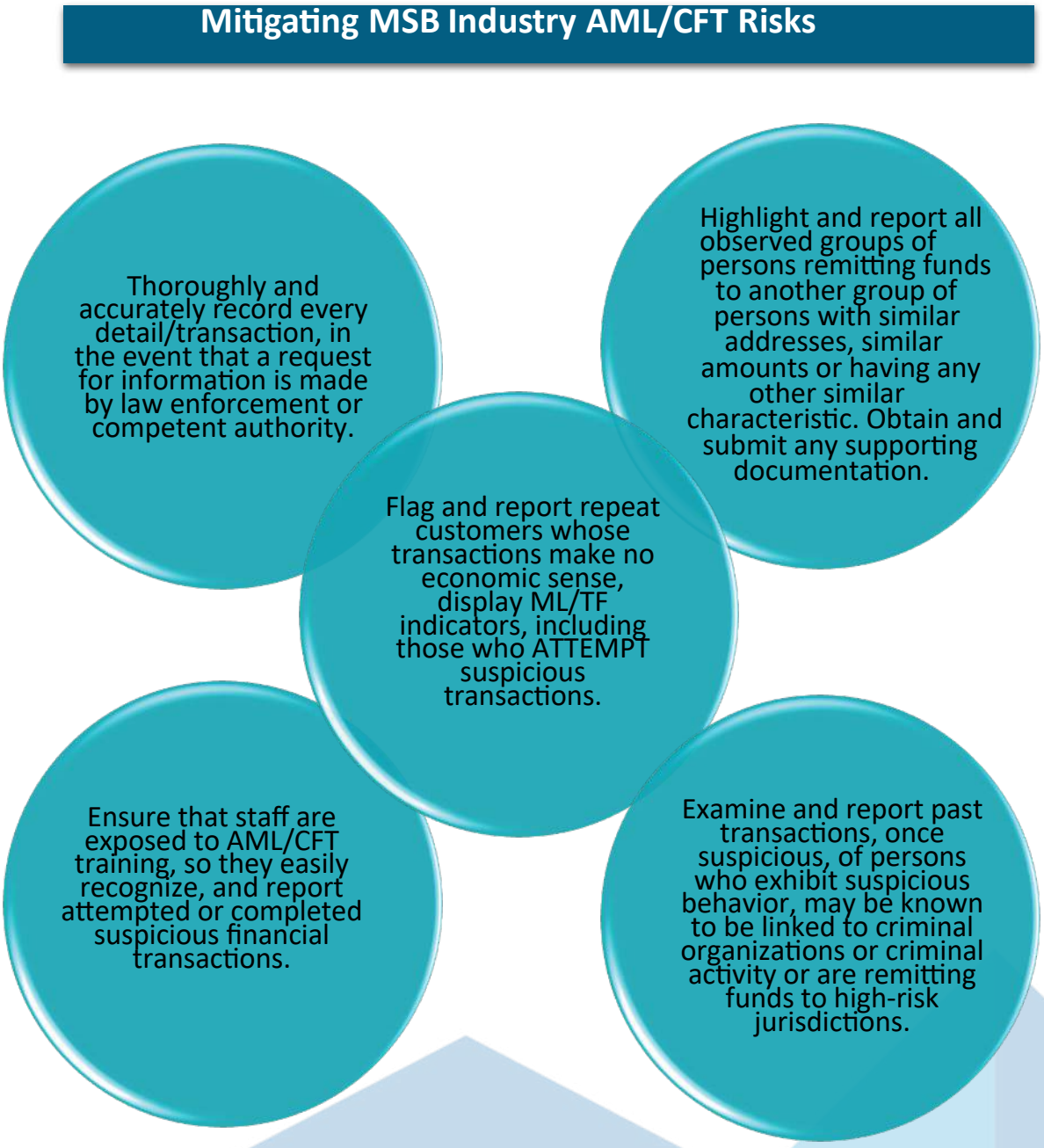
7.1.1 Why should MSBs engage in AML/CFT Compliance?



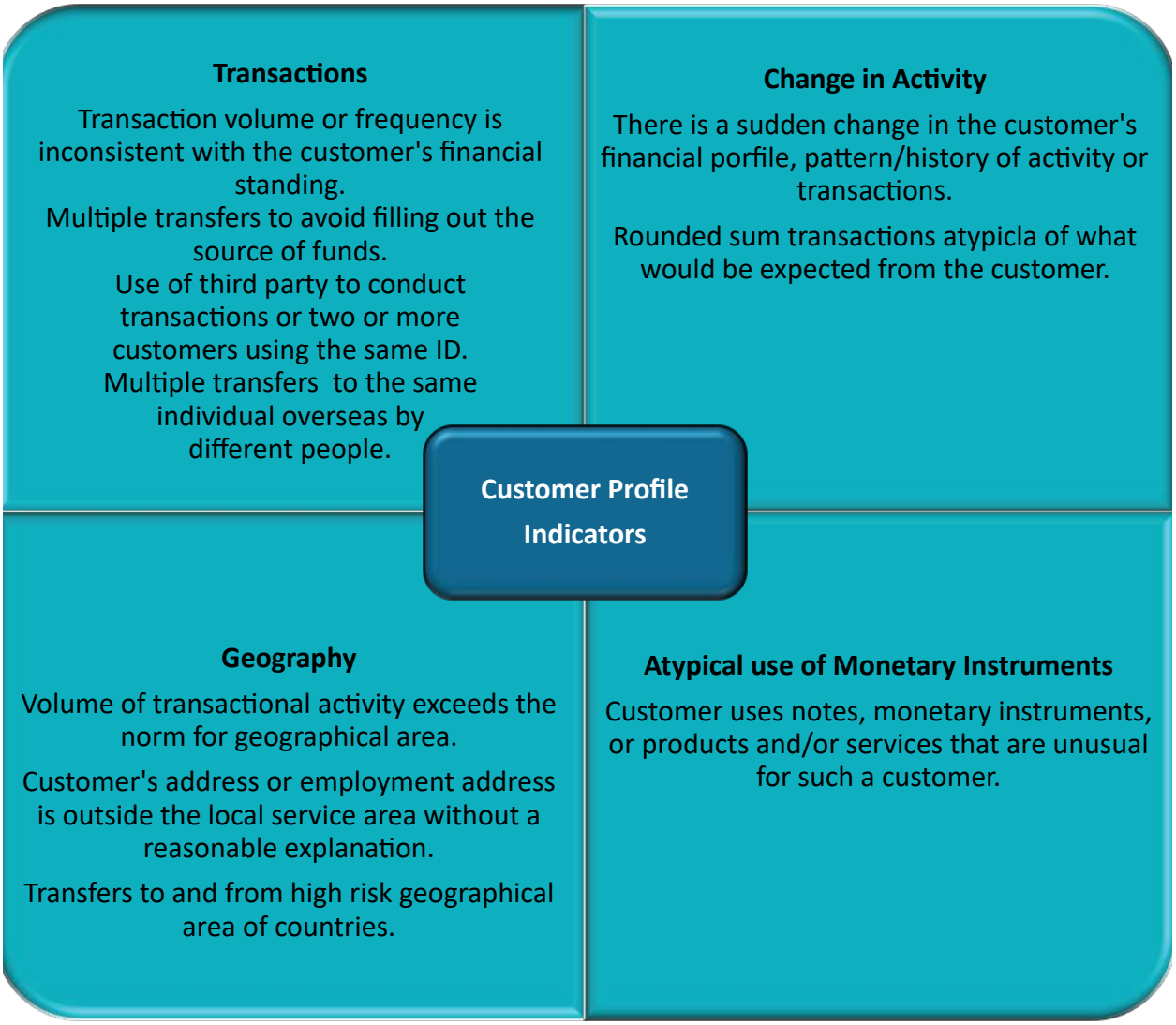
7.1.2 MSB Industry Risks

MSB Industry Risks			
Associated Crimes	**Exploitation**	**Possible Infiltration**	**Data Inaccuracy**
Crimes often associated with MSBs include human smuggling, human trafficking, narcotics trafficking, terrorist financing, elder abuse, mail order brides and heavenly offerings.	Criminals exploit MSB vulnerabilities to remit/receive cash, move cash across jurisdictions, exchange into foreign currency, convert cash to cheques or vice versa.	Organised Crime Gangs (OCGs) can also infiltrate MSBs through complicit employees, quick drop services, or through third party payment instructions.	MSB transactions can feature vast amounts of inaccurate information: customers may not be who they say they are, information may be incomplete or omitted, or the same ID could be assigned to multiple customers.

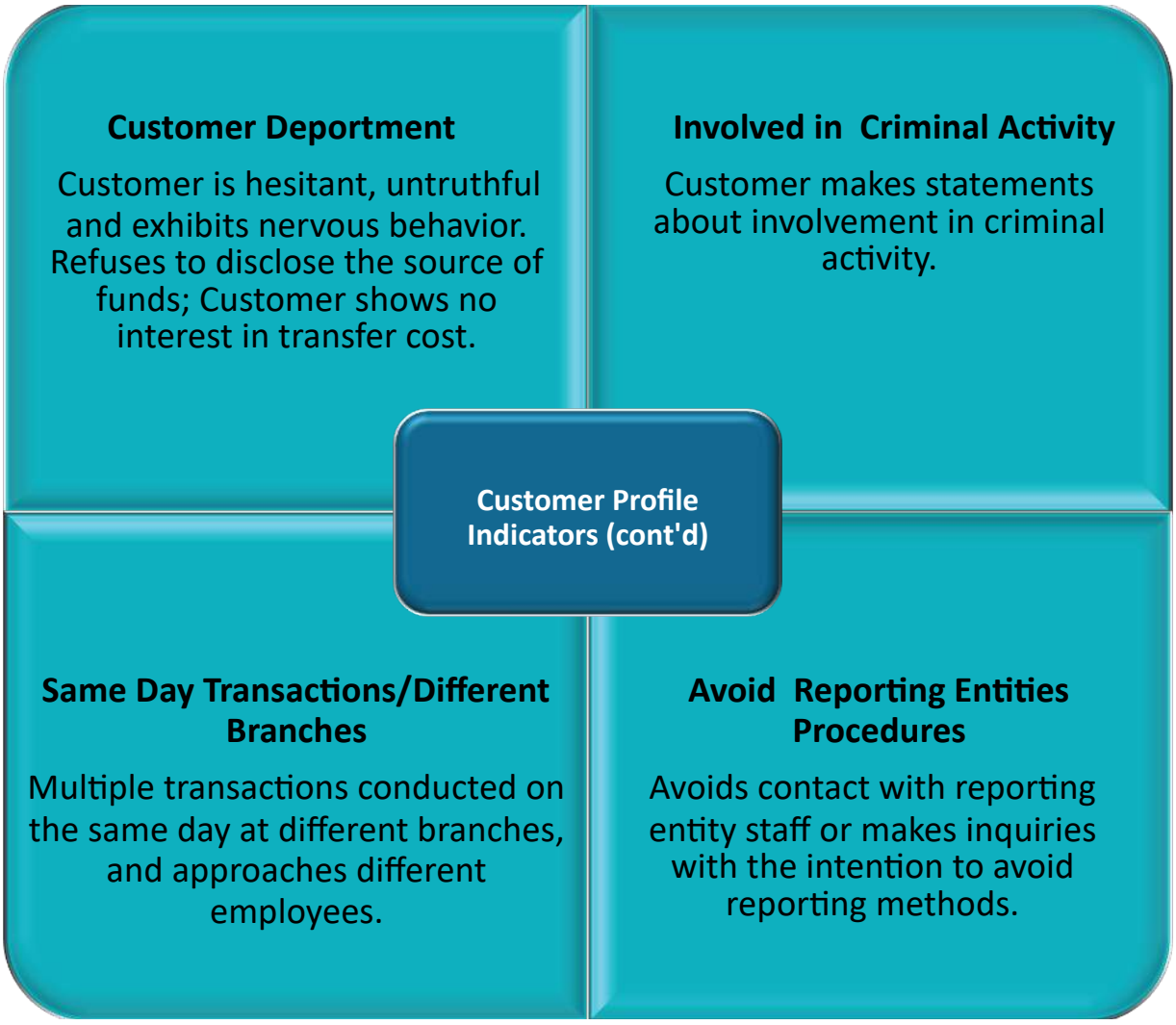
7.1.3 Mitigating MSB Industry AML/CFT Risks



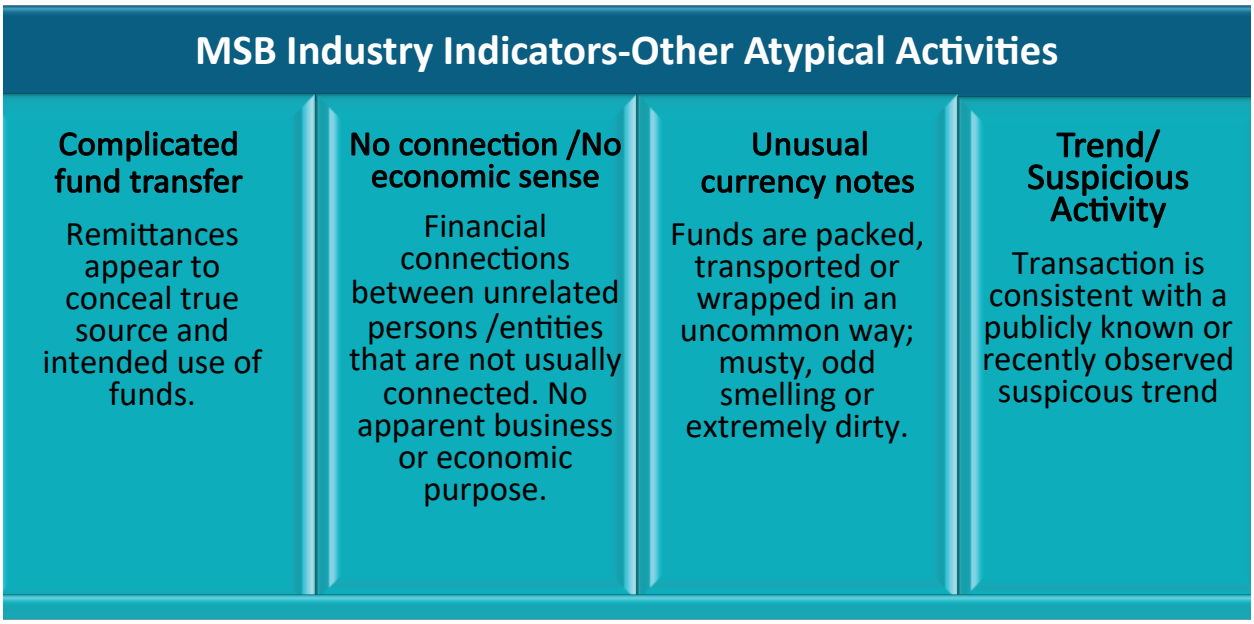
7.1.4 MSB Industry Indicators – Customer Profile



7.1.4 MSB Industry Indicators – Customer Profile (cont'd)

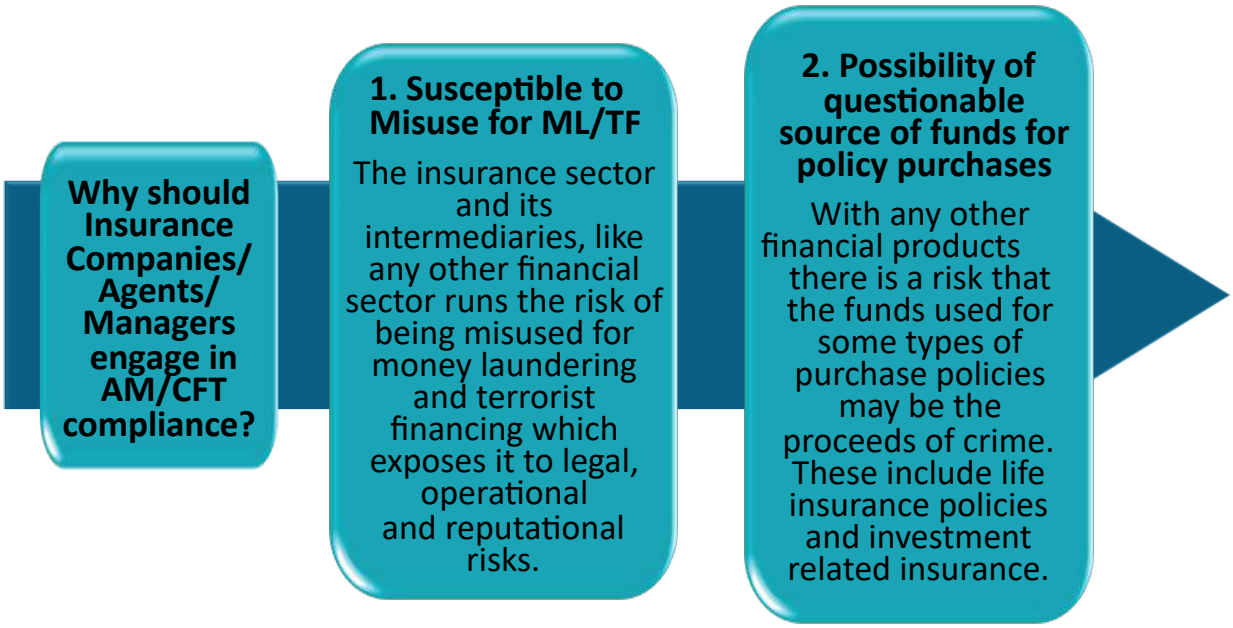


7.1.5 MSB Industry Indicators – Other Atypical Activities

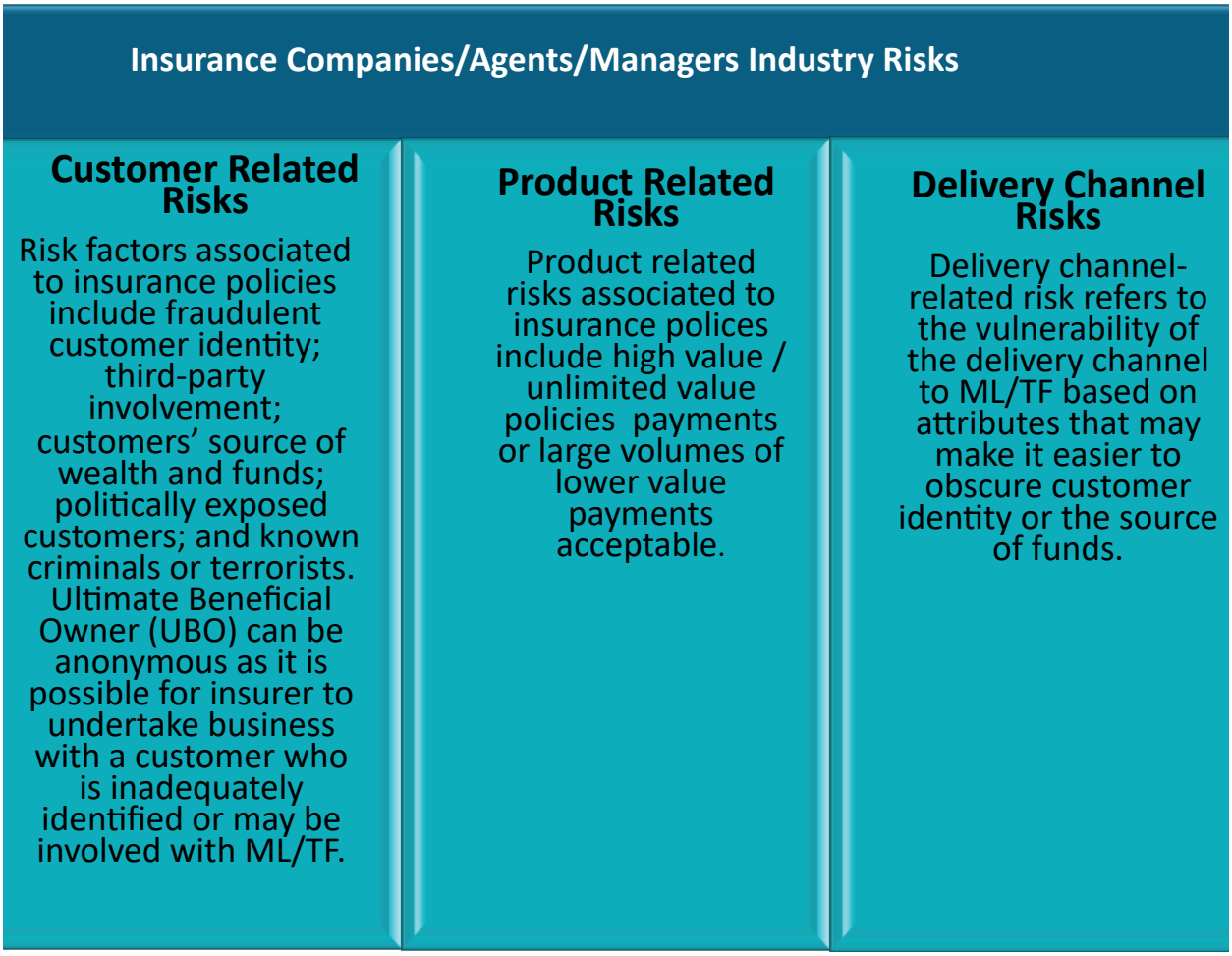


7.2 INSURANCE COMPANY/MANAGERS

7.2.1 Why should Insurance Company/Managers engage in AML/CFT compliance?

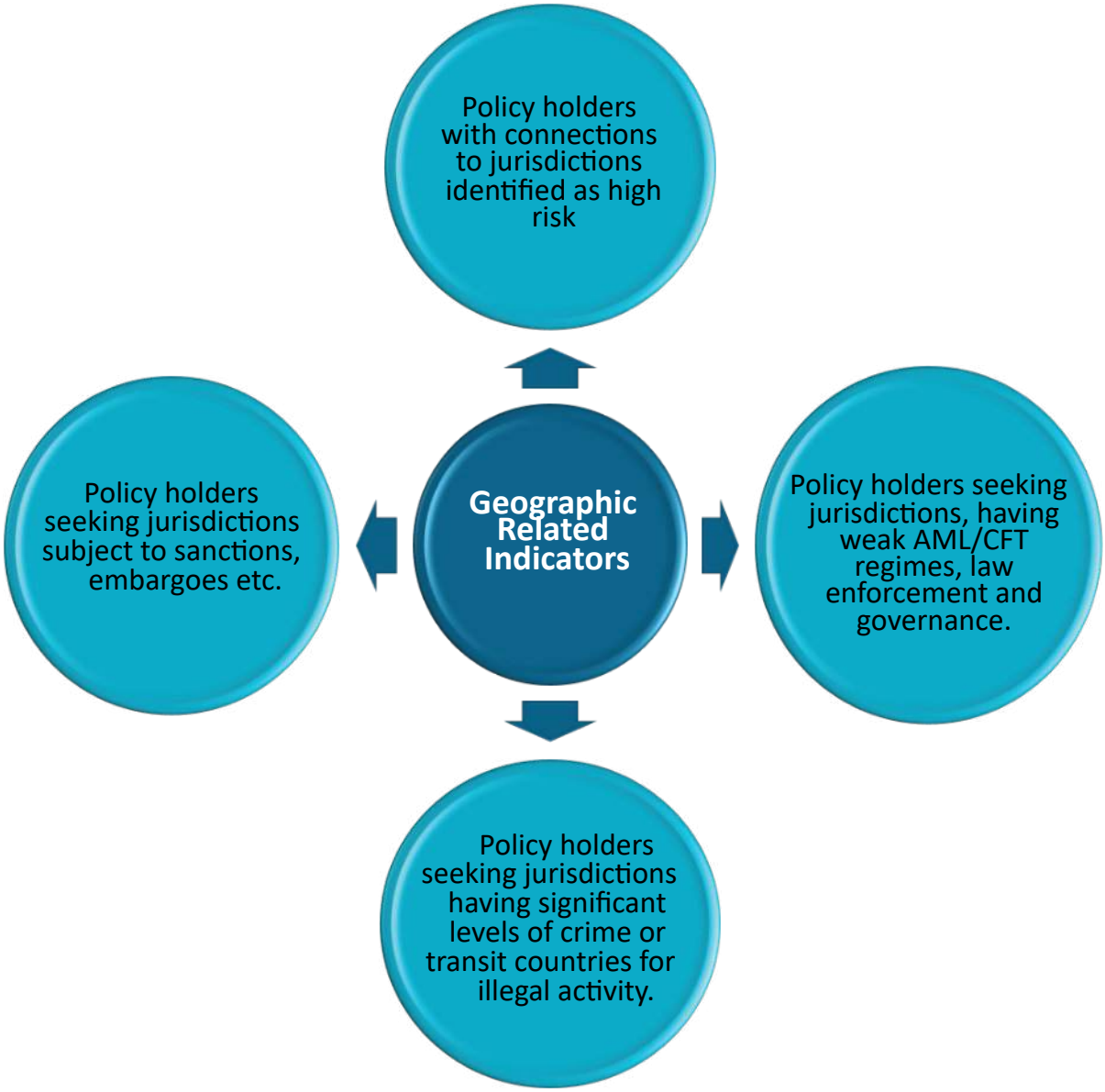


7.2.2 Insurance Company/Managers Industry Risks



7.2.3 Mitigating Insurance Company / Managers Industry Risks

7.2.4 Insurance Company / Managers Industry Indicators – Geographic Related



7.2.5 Insurance Company / Managers Industry Indicators – Product Related

7.2.6 Insurance Company / Managers Industry Indicators – Customer Related

Purchases unexpected for financial profile	• The customer purchases an insurance policy using cash or other monetary instruments for an amount inconsistent with his or her income.
Policy loan obtained with quick repayment	• The customer secures a policy loan against the cash value soon after policy is issued and quickly repays the loan with cash or various monetary instruments.
Policy premiums paid from foreign judication	• The customer enters into a contract for a considerable sum with the payment of the premiums coming from abroad, specifically from an offshore financial center.
Obscured Beneficial Owner & Identity details	• Legal entity / natural person who may obscure the ultimate beneficial owner or who has controlling interests. Unwillingness to provide clear identification details / supporting document.
Obscured Beneficial Owner & Identity details	• Gatekeeper/third party involvement when unnecessary or that is unrelated
Policy cancellation/ 3rd party beneficiary	• The customer cancels an insurance contract then directs that the funds be sent to a third party.

7.3. CASINOS

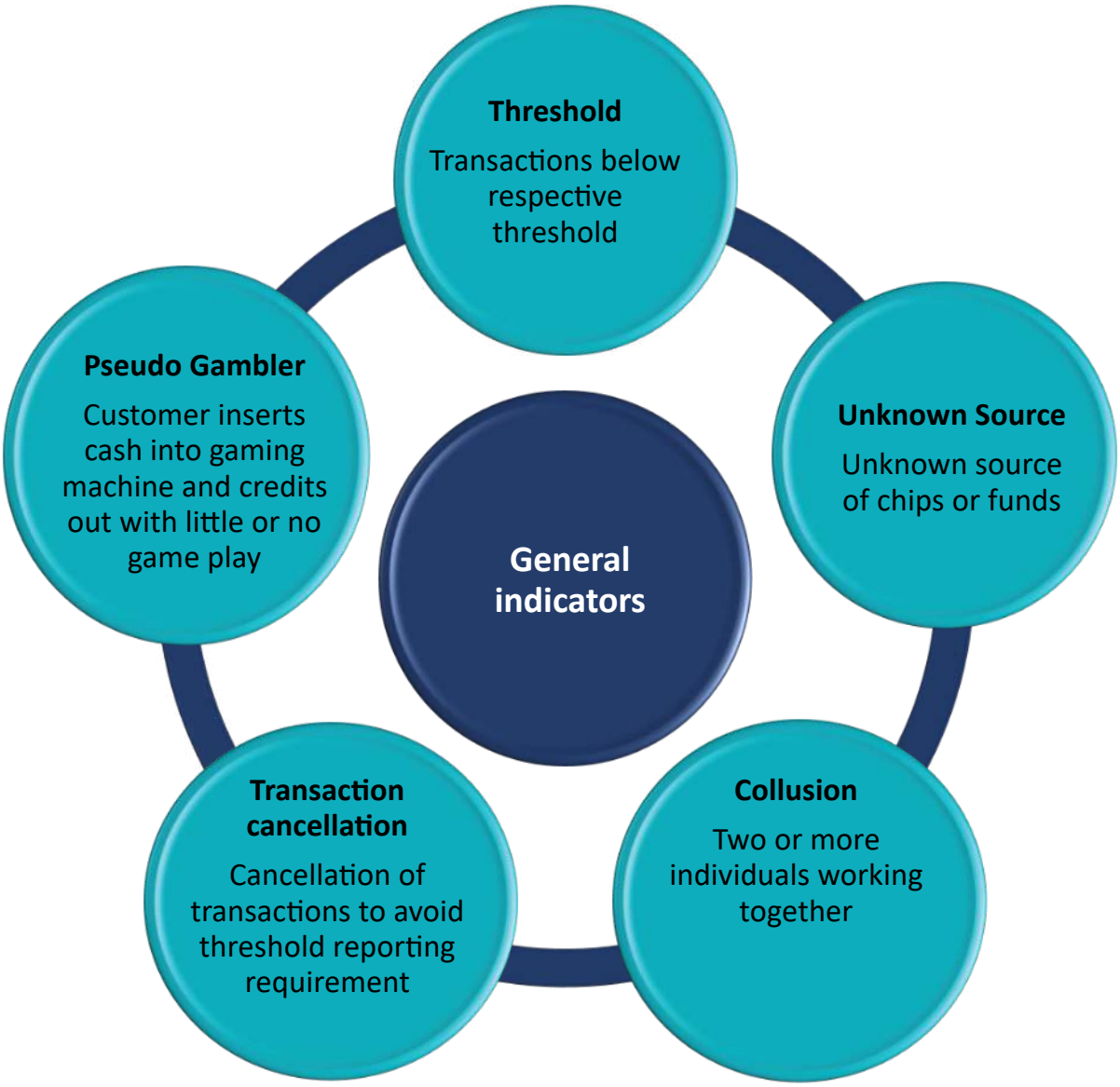
7.3.1 Why should Casinos engage in AML/CFT Compliance?

Why should Casinos Engage in AML/CFT Compliance?		
Target The casino industry is a target for criminals to launder profits obtained through illicit activity.	**DNFBPs** They are by definition non-financial institutions, which put them at risk of money laundering as: - They offer gambling for entertainment, - undertake financial activities that are similar to financial institutions.	**Transactions** Services are available 24 hours per day. Accept funds on accounts; conduct money exchange; conduct money transfers; foreign currency exchanges; stored value services; debit card cashing facilities, cheque cashing; safety deposit boxes.

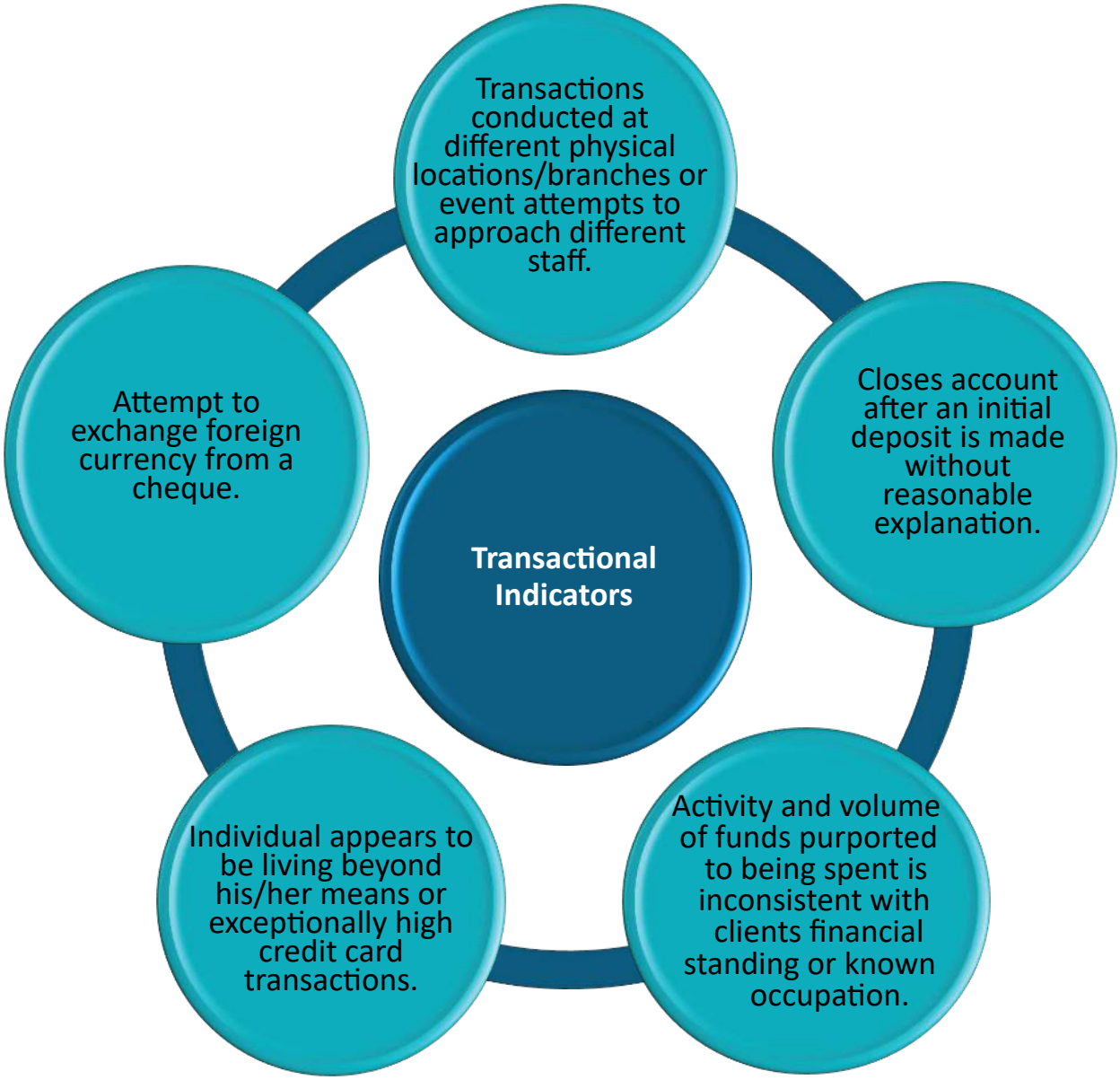
7.3.2 Casinos Industry Risks

7.3.3 Mitigating Casinos AML/CFT Industry Risks

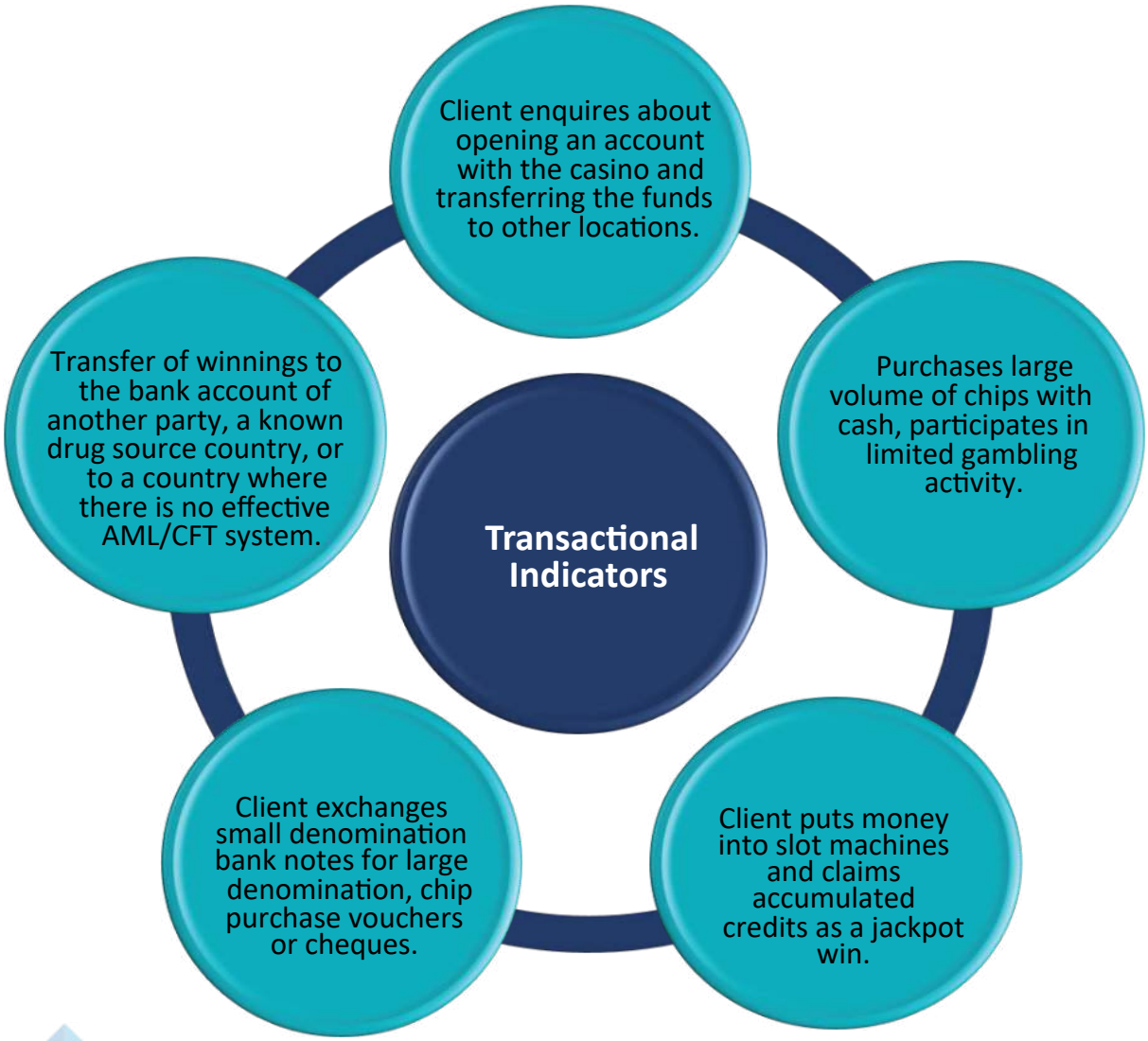
7.3.4 Casino Industry Indicators – General Indicators



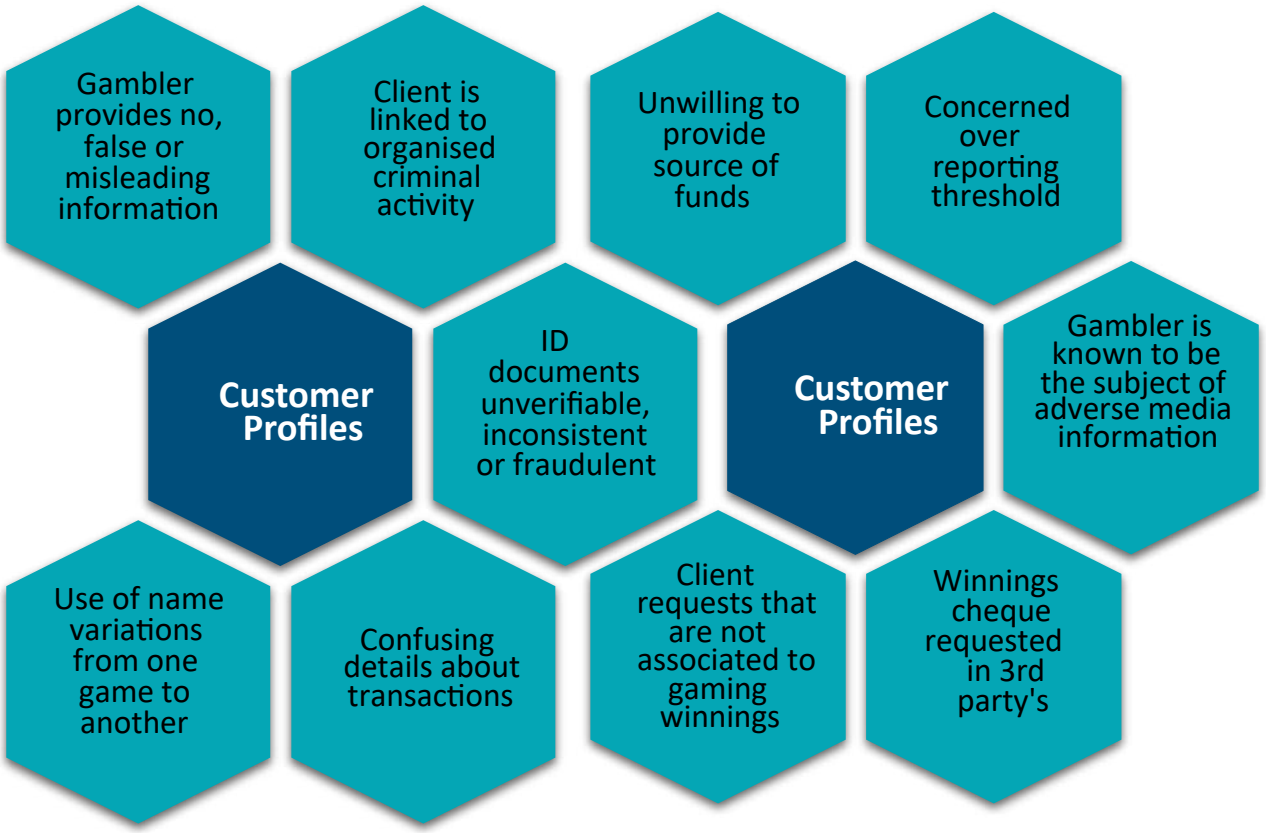
7.3.5 Casino Industry Indicators – Transactional Indicators



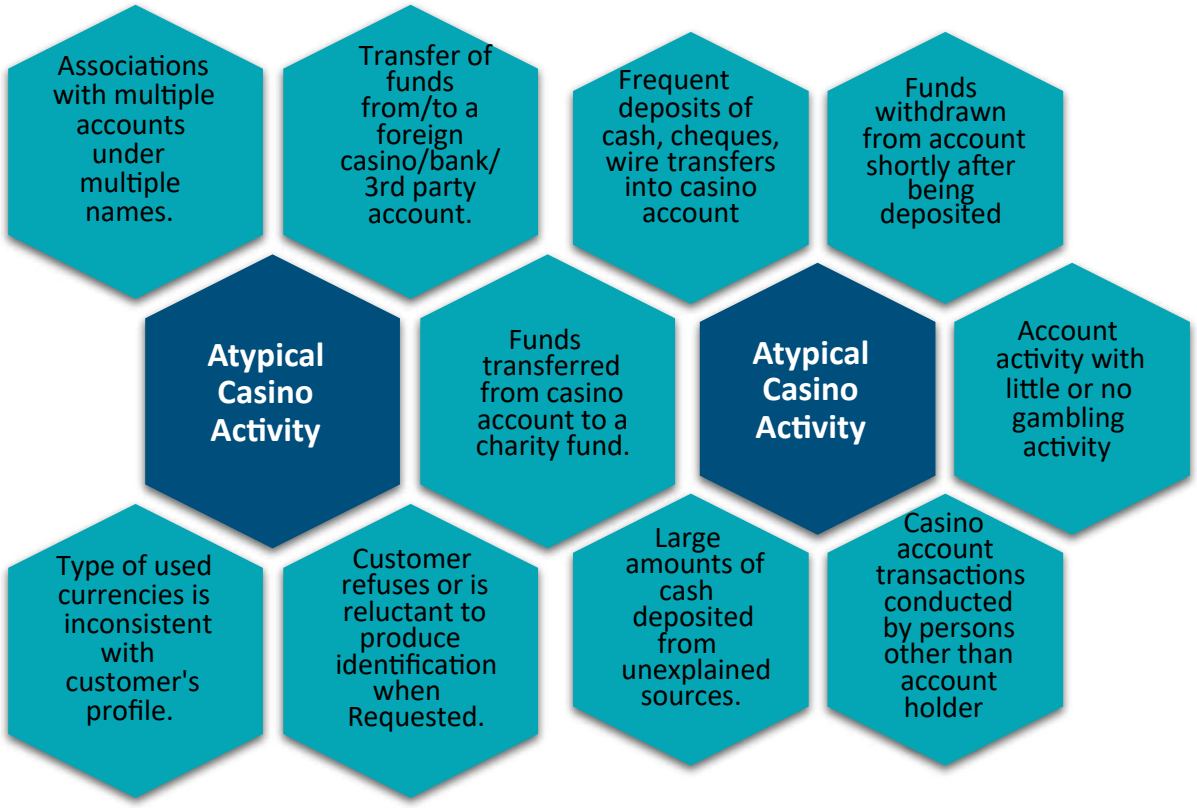
7.3.5 Casino Industry Indicators – Transactional Indicators (cont'd)



7.3.6 Casino Industry Indicators – Customer Profile Indicators



7.3.7 Casino Industry Indicators – Atypical Casino Account Indicators

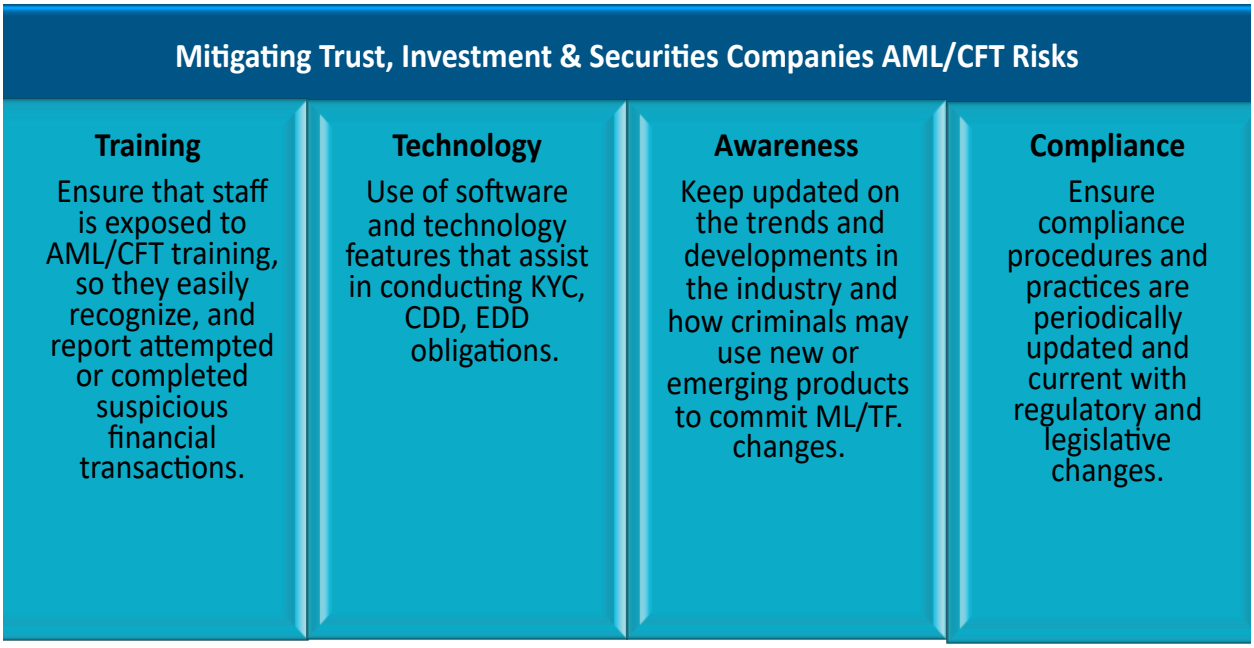


7.4 TRUST, INVESTMENT & SECURITIES COMPANIES

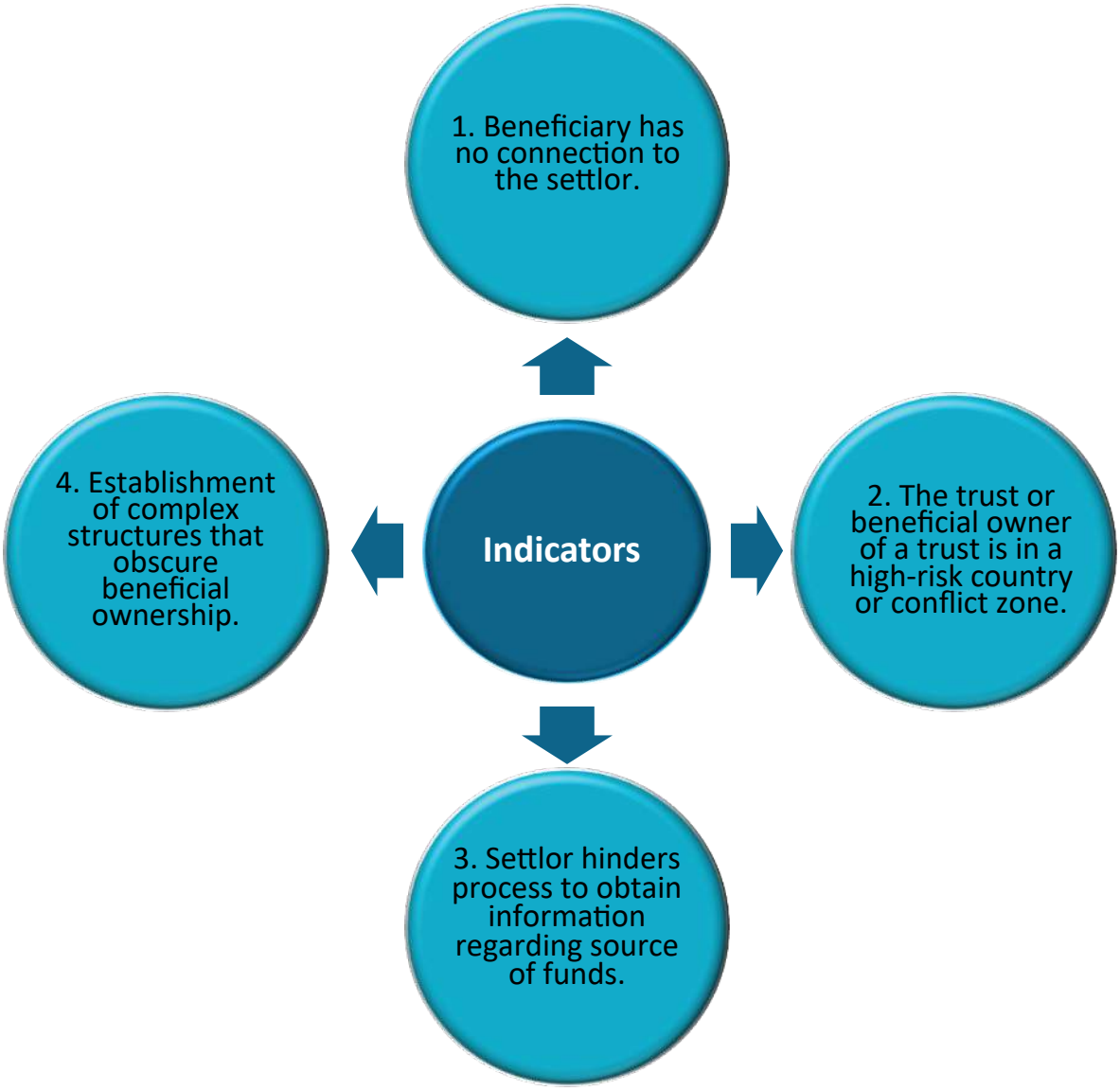
7.4.1 Why should Trust, Investment & Securities Companies engage in AML/CFT compliance?

7.4.2 Trust, Investment & Securities companies risks

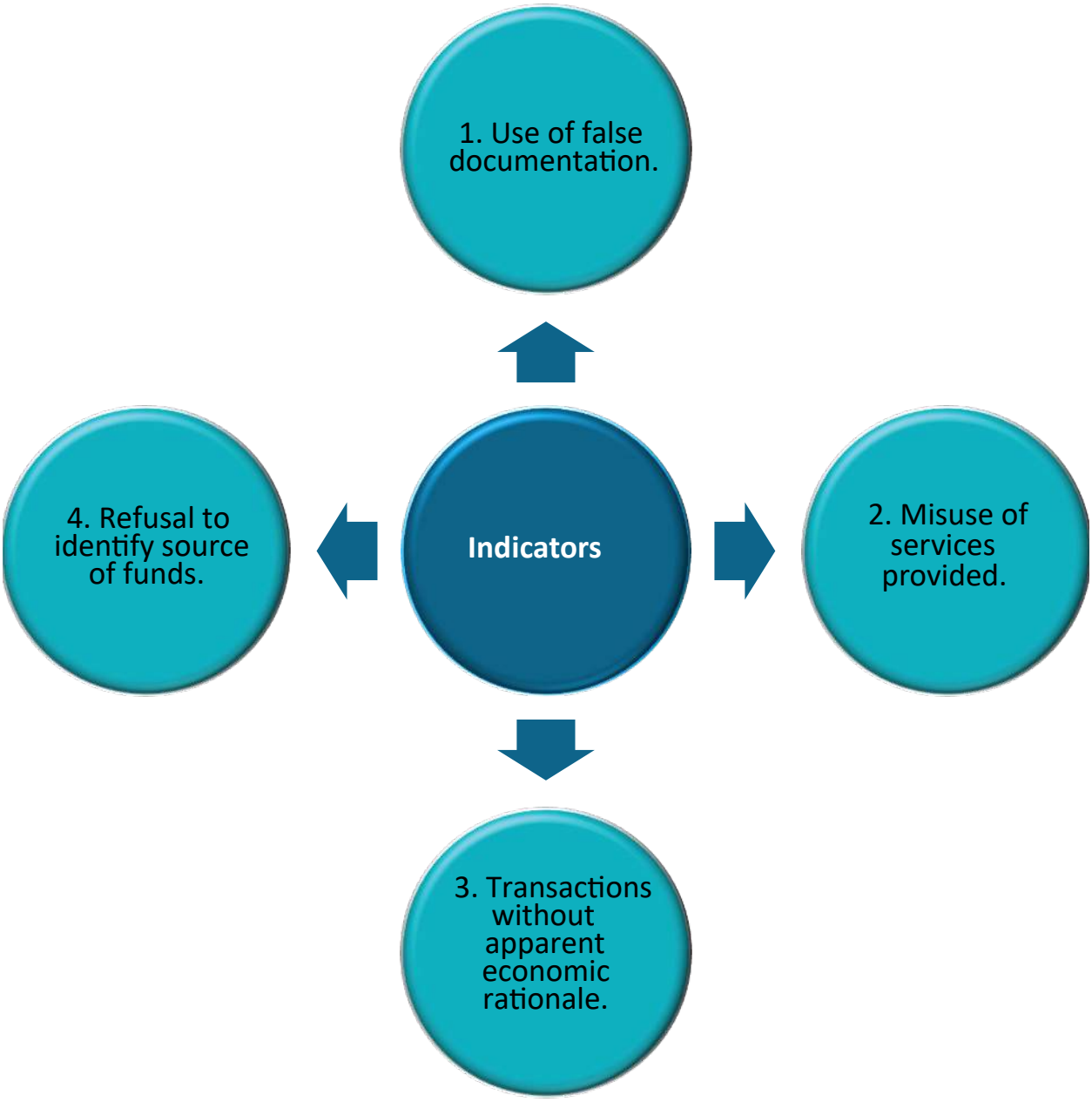
7.4.3 Mitigating Trust, Investment & Securities companies AML/CFT risks



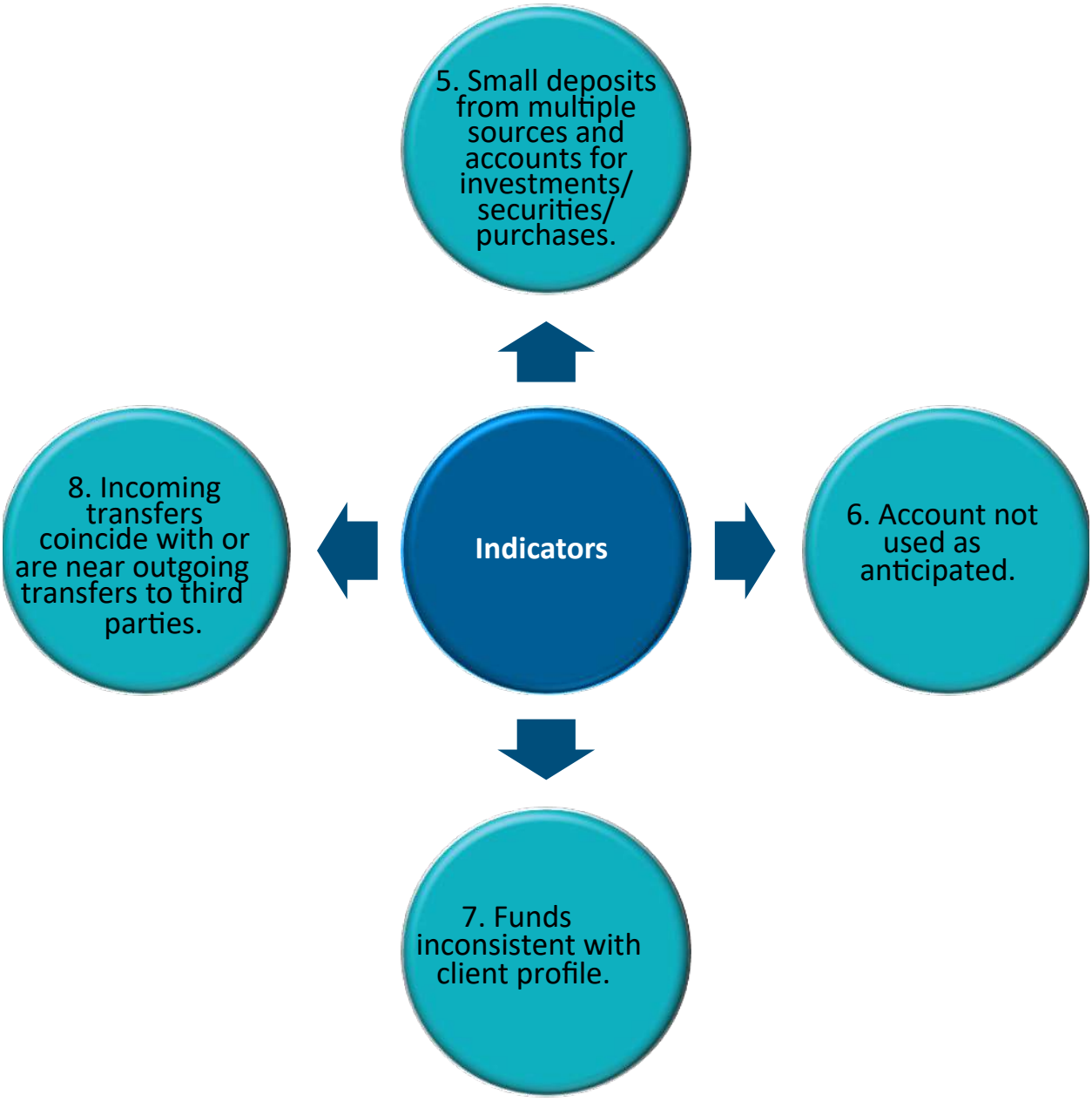
7.4.4 Trust, Investment & Securities Industry indicators – Trust related



7.4.5 Trust, Investment & Securities Industry indicators – Investment Securities related

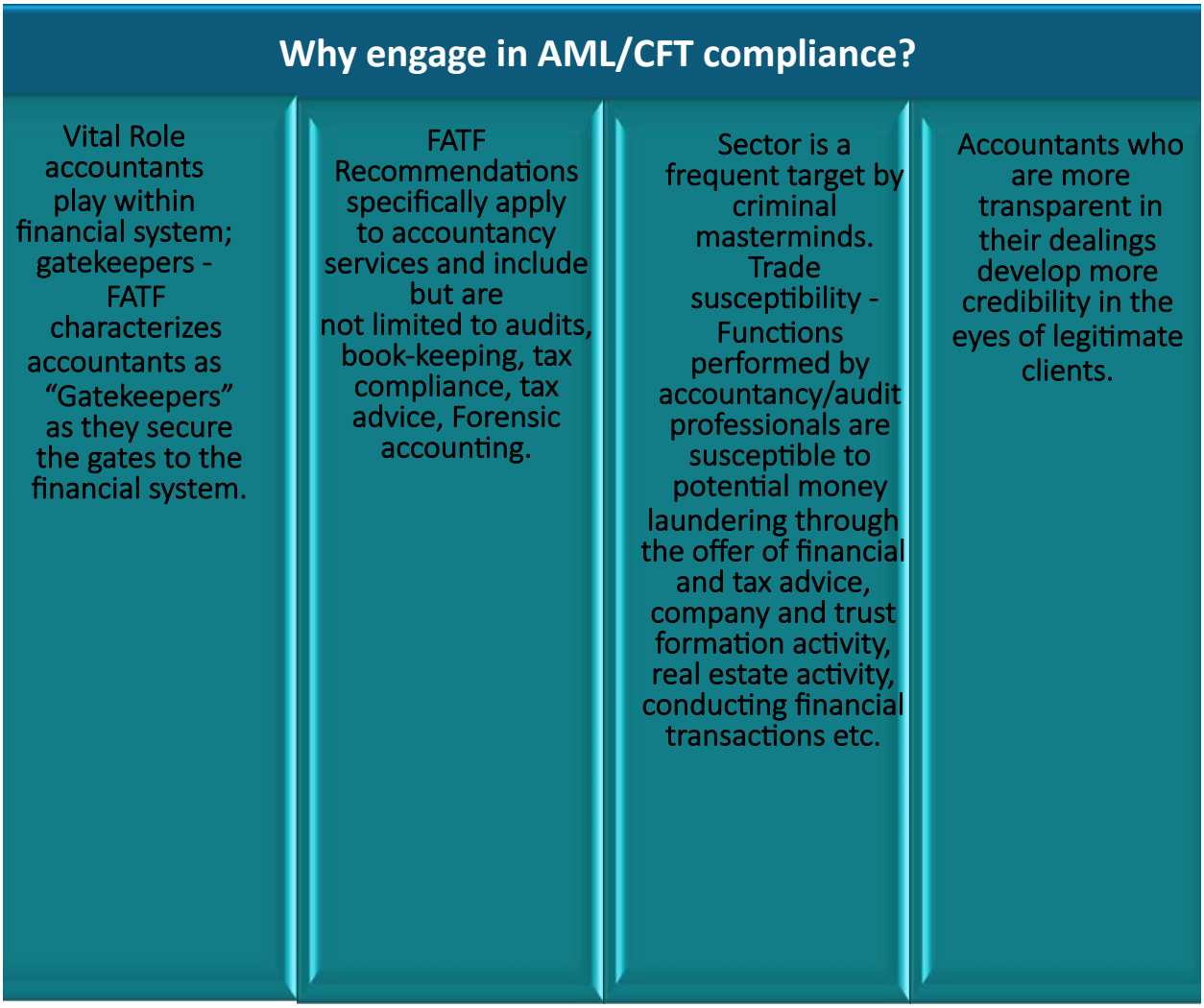


7.4.5 Trust, Investment & Securities Industry indicators – Investment/ Securities related (cont'd)



7.5 ACCOUNTANCY – ACCOUNTANTS/AUDIT COMPANIES

7.5.1 Why should Accountants/Audit firms engage in AML/CFT Compliance?



7.5.2 Accountants/Audit firms Risks

1. Sale/Purchase of Business Entities or Management of Legal Arrangements

Accountants involved in commercial activities such as mergers and acquisitions and the funds received or held for professional fees, expenses or disbursements that are not included in commercial activities.

2. Real Estate Transactions

Where accountants are involved in the residential and commercial purchase and sale, lease and mortgage transactions and transactions which also finance a purchase or sale of real estate.

3. Financial Management

Accountants must be conscious of the funds that move through the firm's trust or client's account (bank, savings, securities etc). Accountants handling or managing clients' funds must note AML/CFT obligations and potential risks involved.

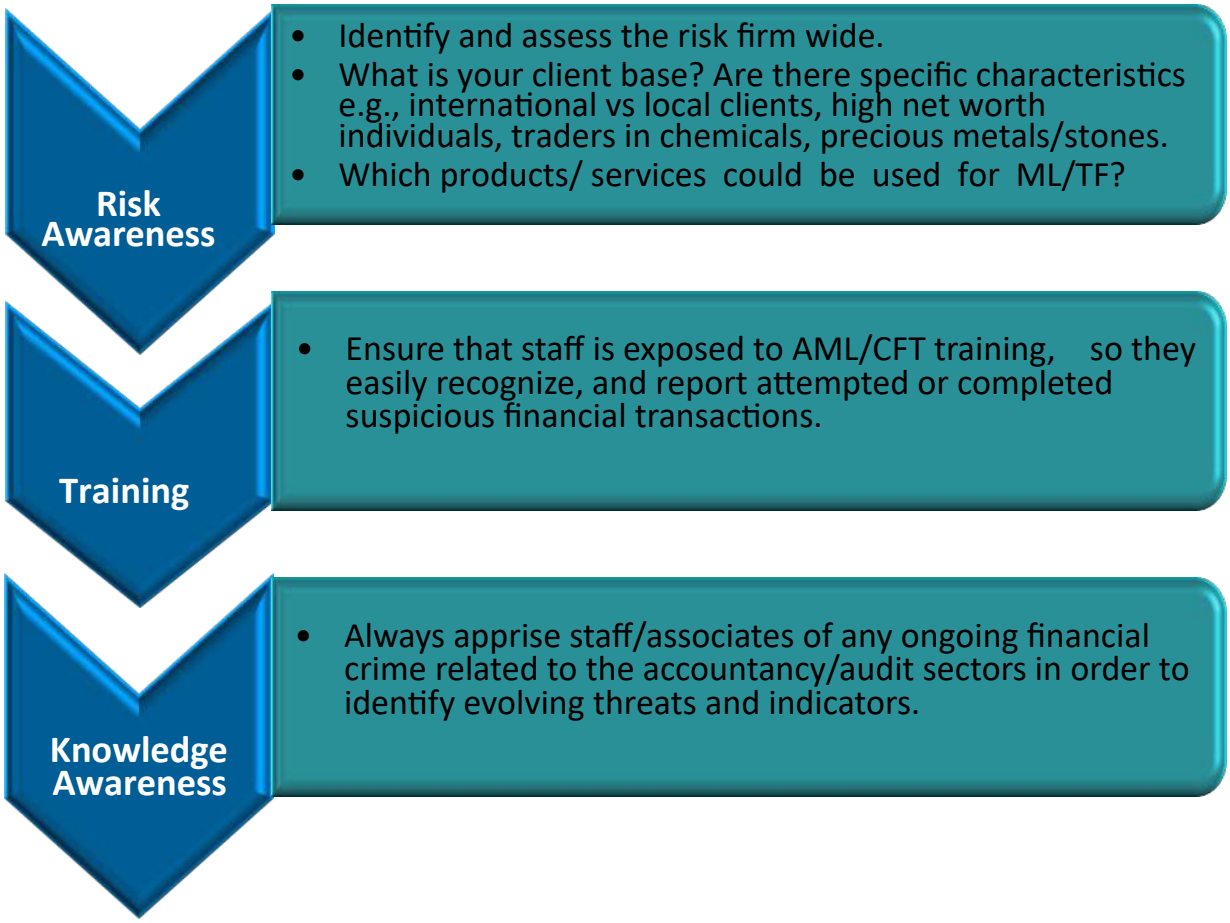
4. High Risk Connections

Higher risk clients occur when business transactions are connected to higher risk countries.

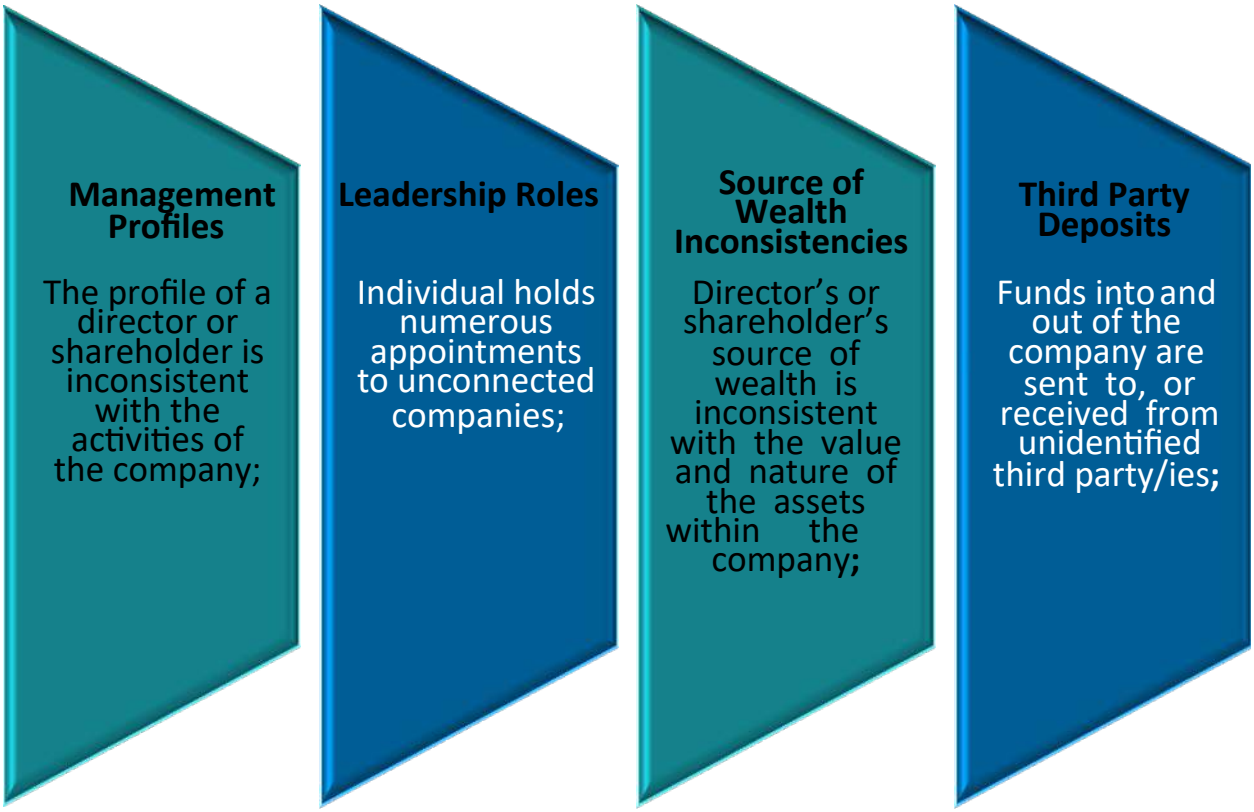
5. Creation or Management of Companies' Transactions

Occurrences where accountants undertake transactions where investors arrange to contribute capital to a legal entity and cover the financing and refinancing transactions.

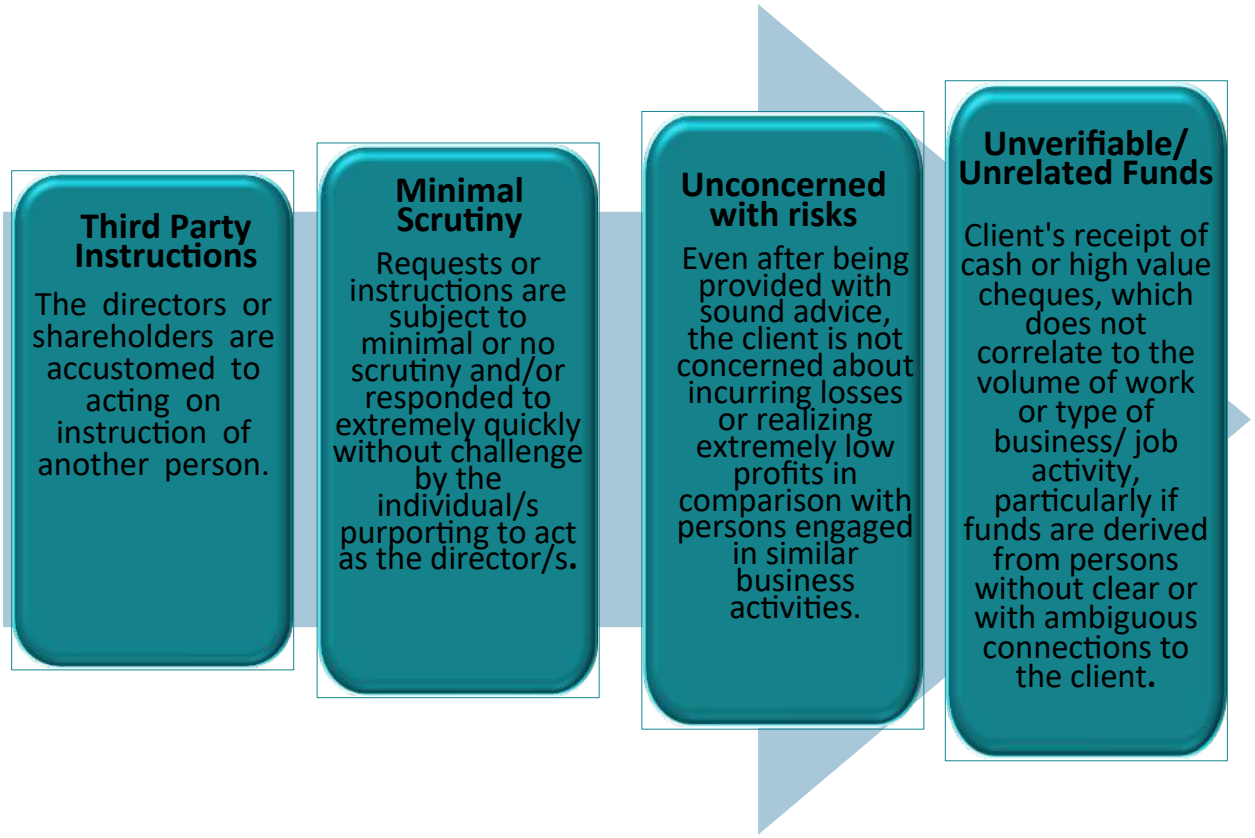
7.5.3 Mitigating Accountants/Audit firms AML/CFT risks



7.5.4 Accountants/Audit Industry AML/CFT Indicators



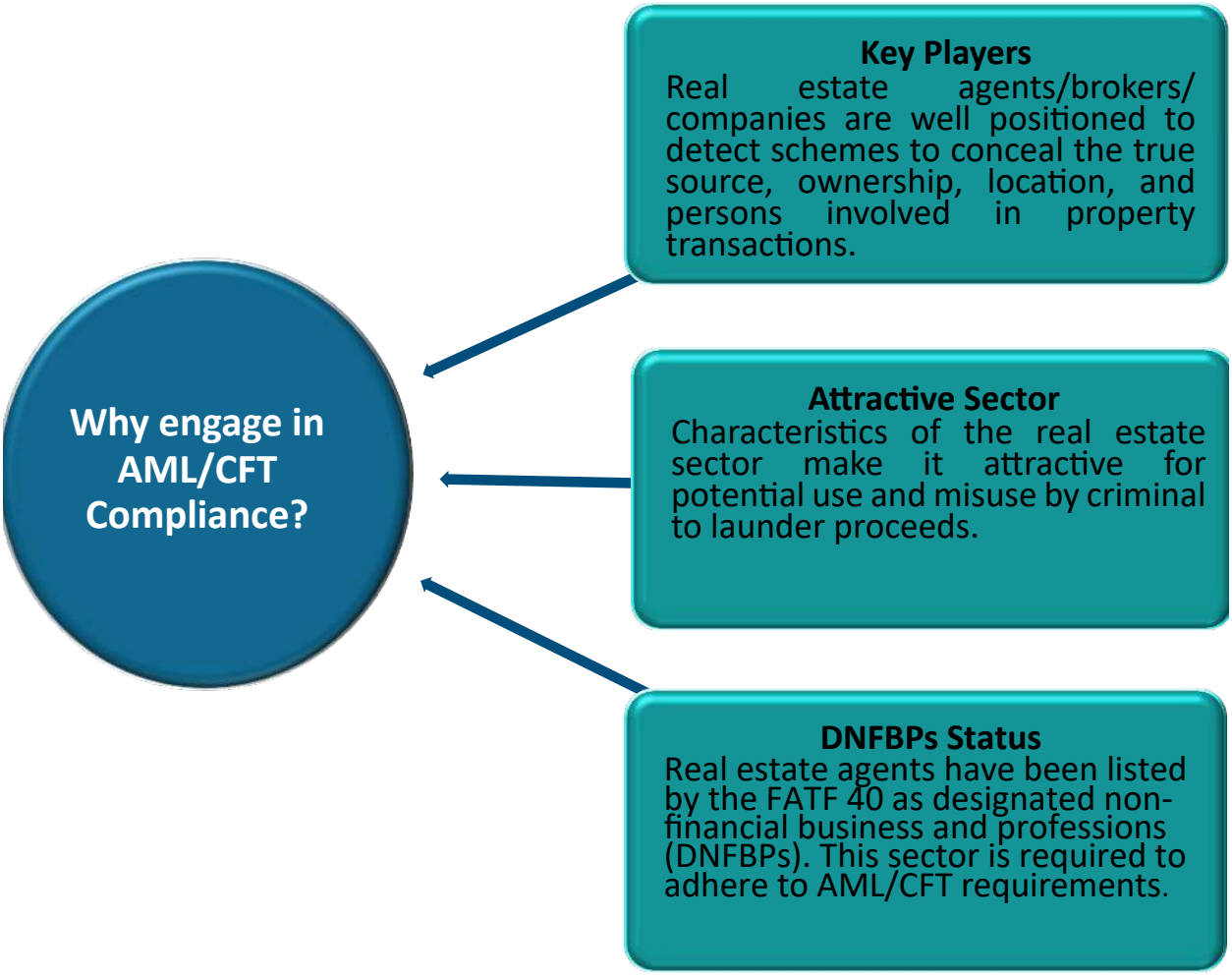
7.5.4 Accountants/Audit Industry AML/CFT Indicators (cont'd)



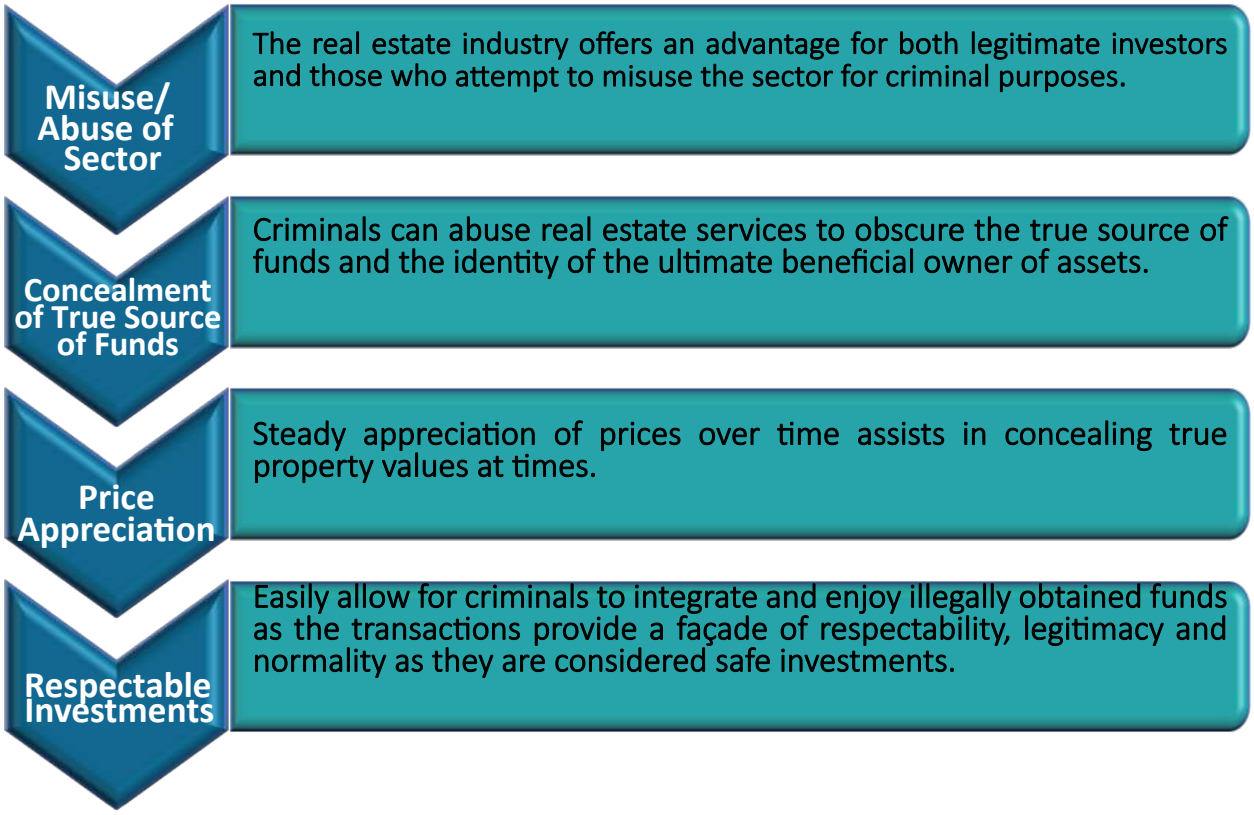
7.5.4 Accountants/Audit Industry AML/CFT Indicators (cont'd)

7.6 REAL ESTATE AGENTS

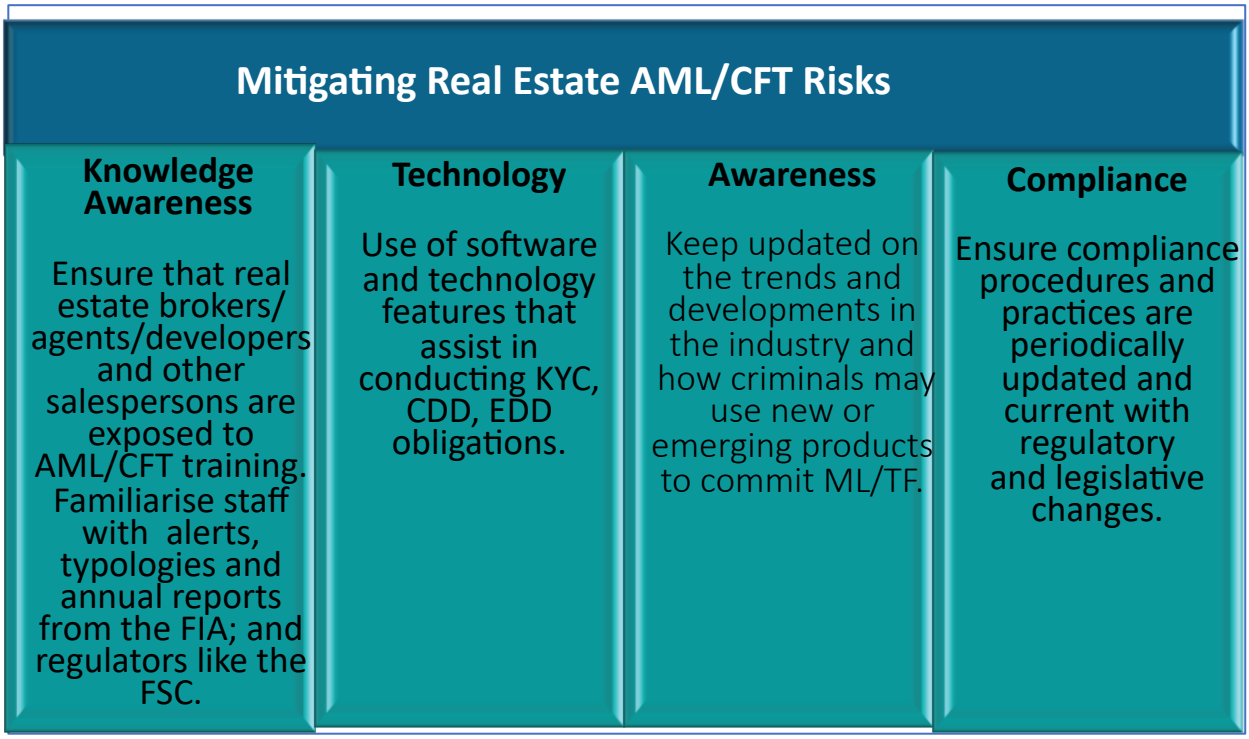
7.6.1 Why should Real Estate agents engage in AML/CFT Compliance?



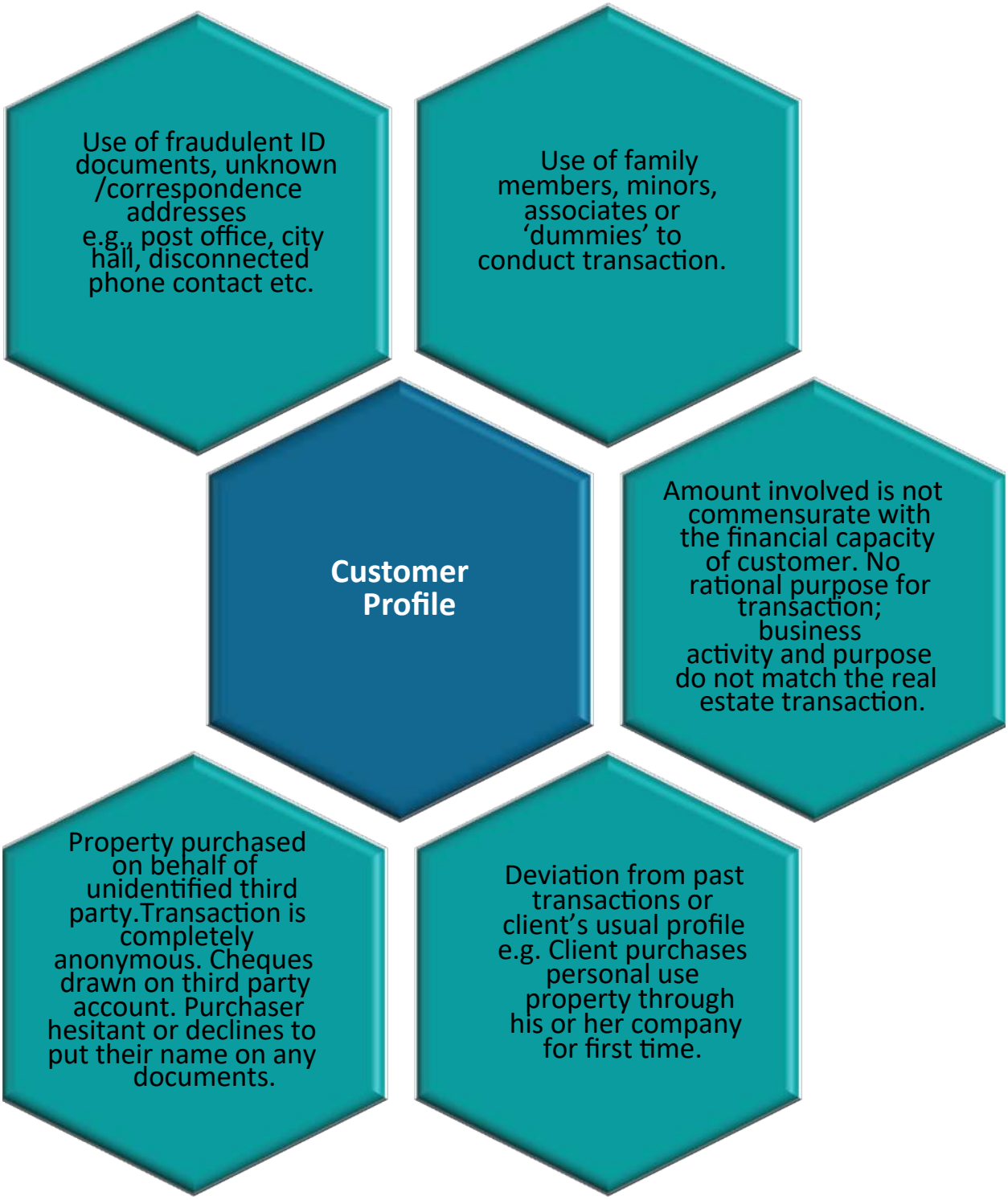
7.6.2 Real Estate Industry risks



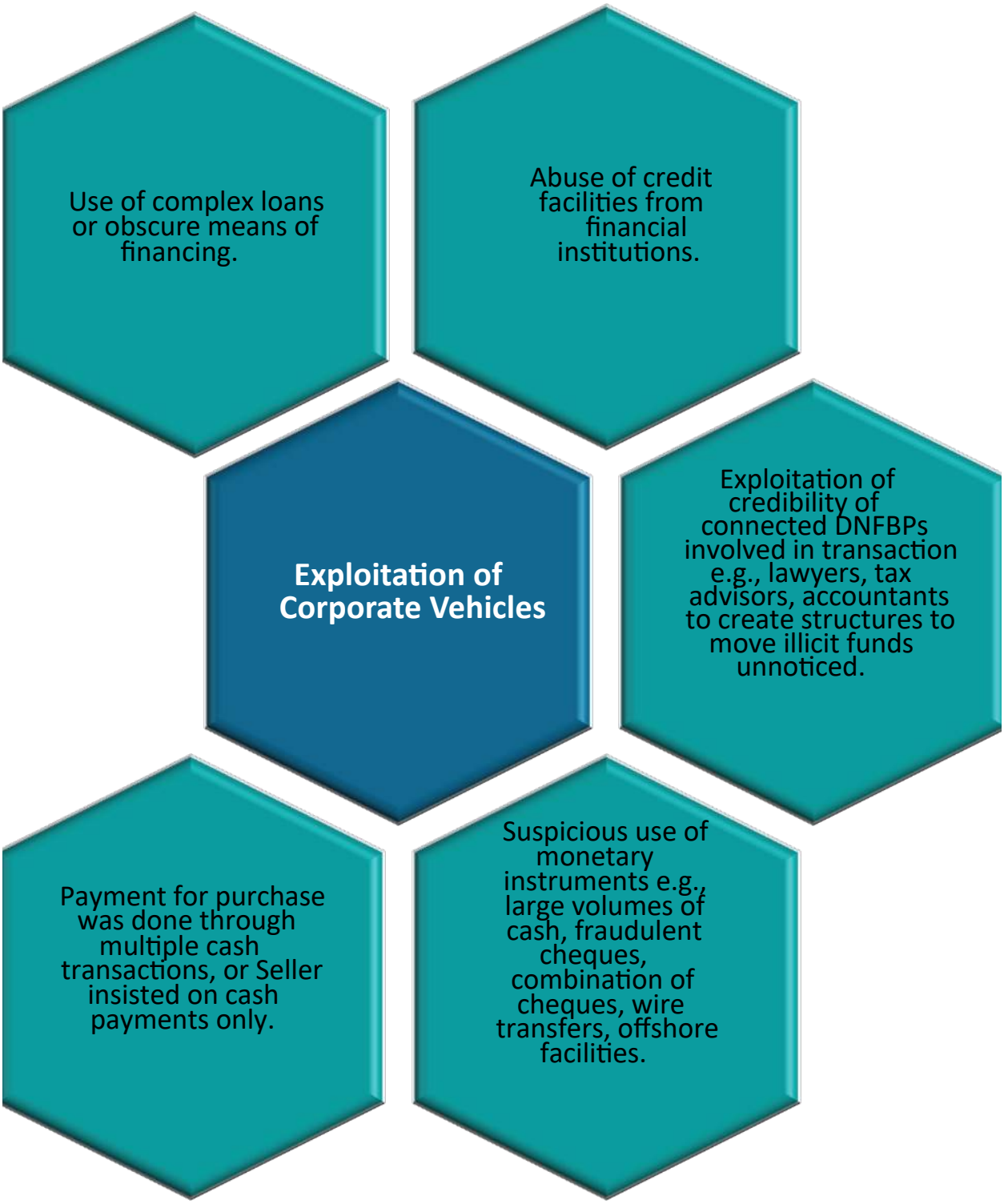
7.6.3 Mitigating Real Estate Industry risks



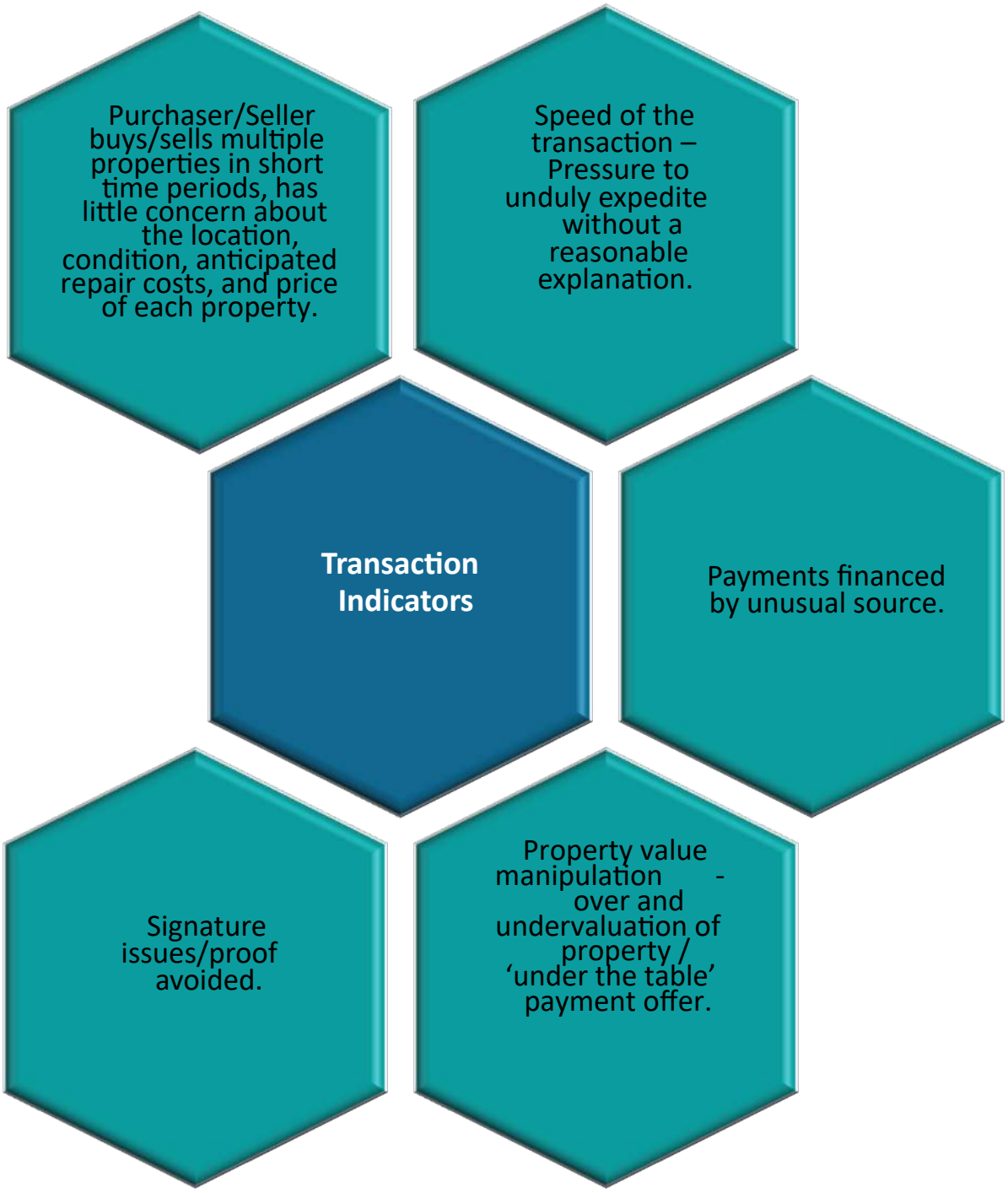
7.6.4 Real Estate Industry Risks - Customer Profile



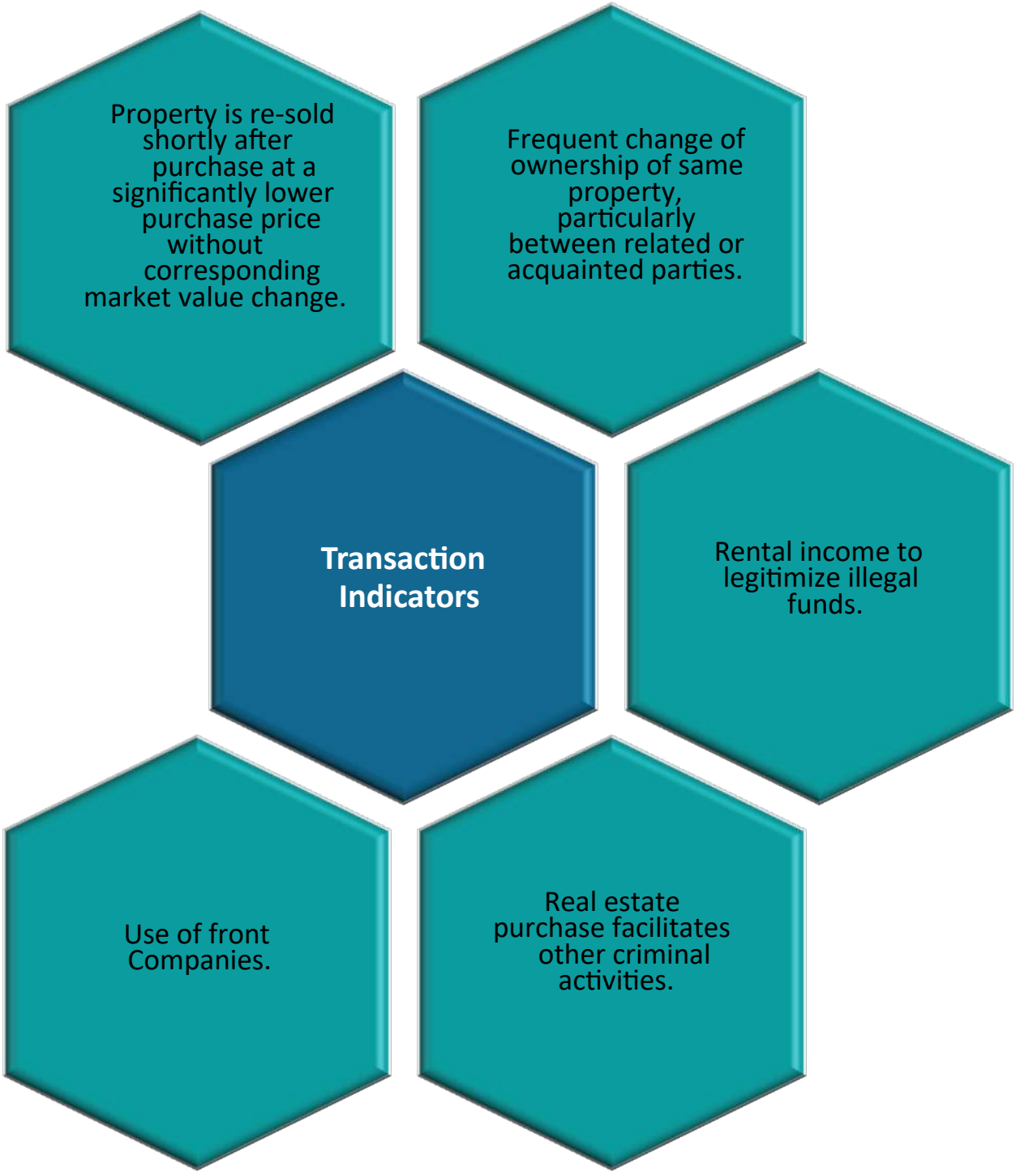
7.6.5 Real Estate Industry indicators – Exploitation of Corporate Vehicles



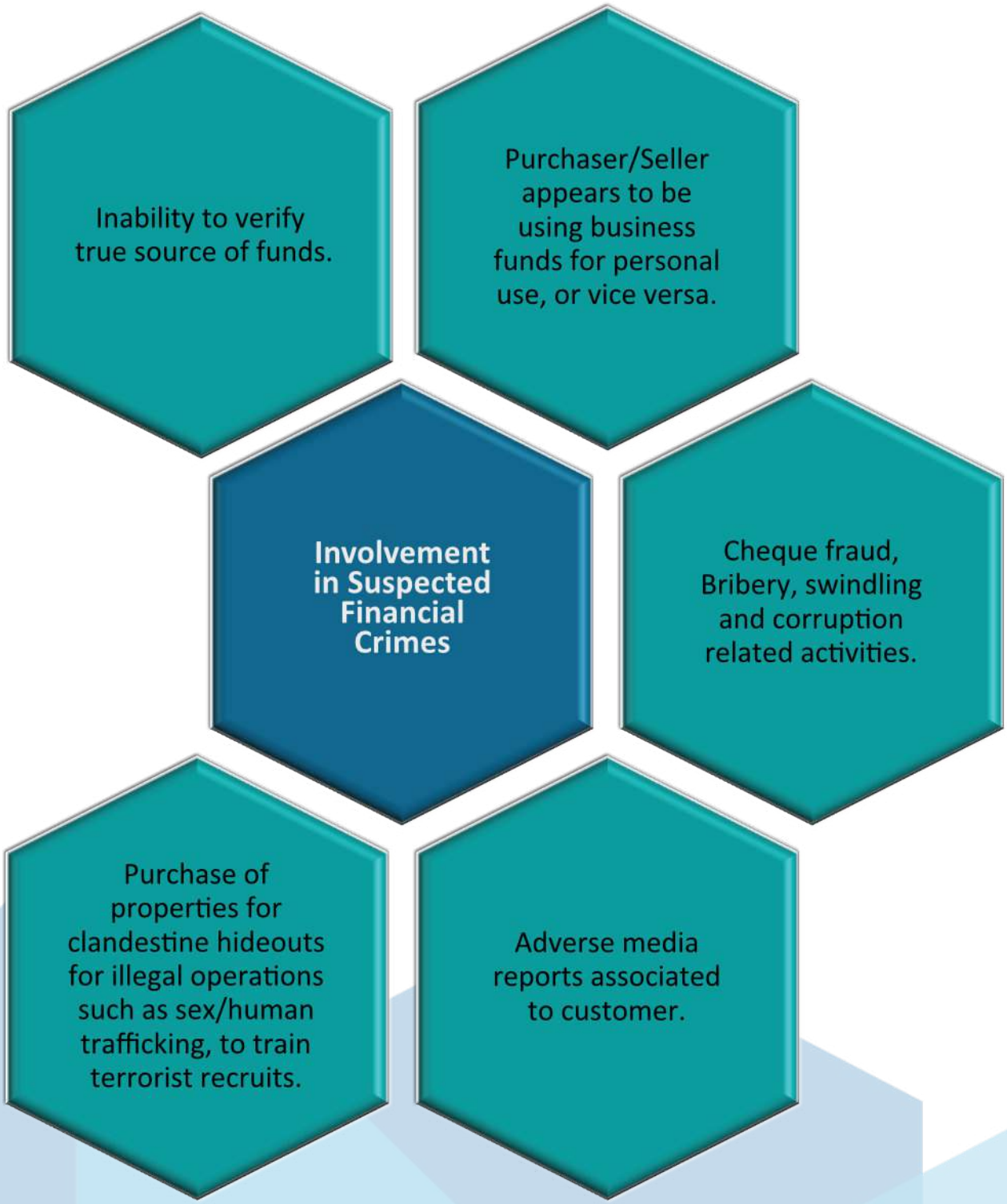
7.6.6 Real Estate Industry indicators – Transactions



7.6.6 Real Estate Industry indicators – Transactions (cont'd)



7.6.7 Real Estate Industry indicators – Involvement in Suspected Financial Crimes



7.7 ATTORNEYS AND LAW FIRMS

7.7.1 Why should Attorneys/Law Firms engage in AML/CFT compliance?

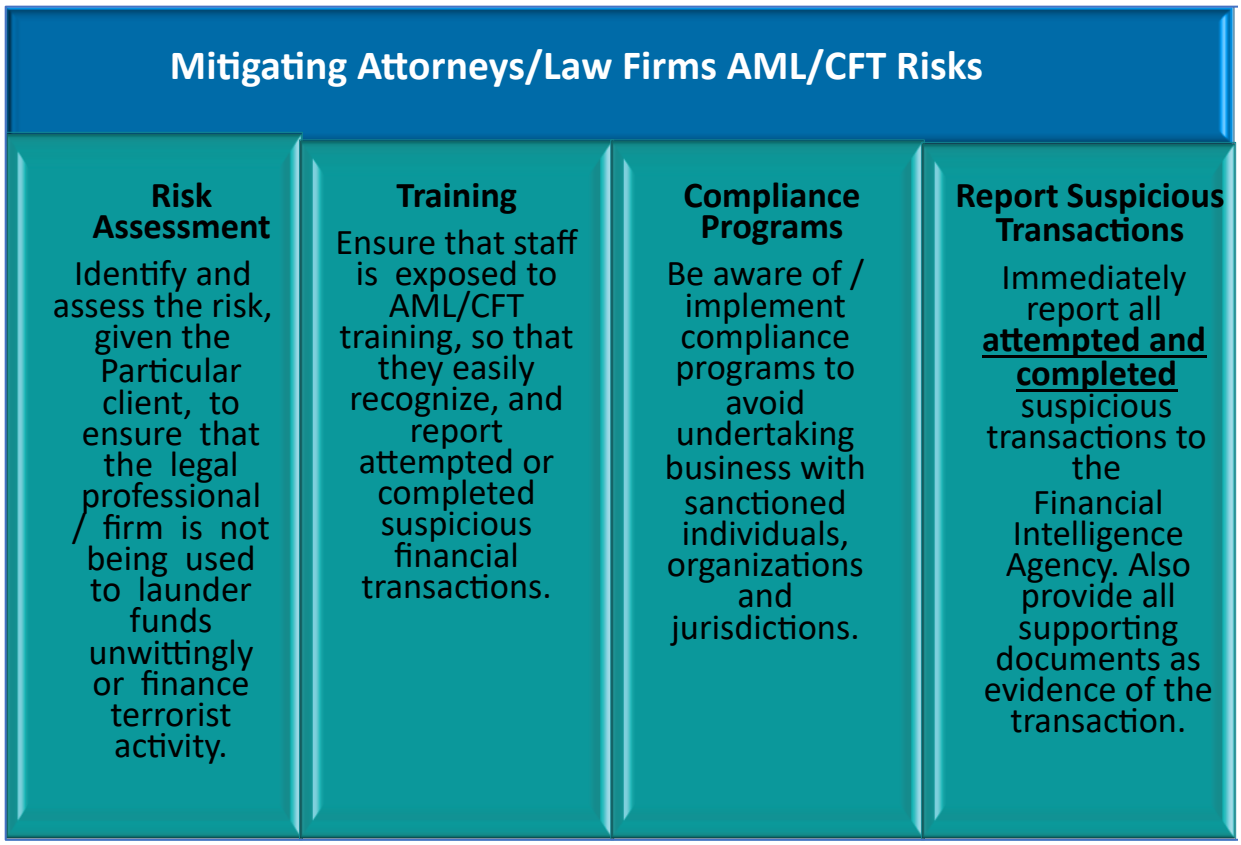
Why Should Attorneys/Law Firms Engage in AML/CFT compliance?

FATF has made recommendations which specifically apply to legal professionals – lawyers, notaries and other legal professionals. Legal professionals include barristers, solicitors, and other specialist advocates and notaries. These professionals are considered gatekeepers due to their ability to manage assets and funds, perform transactions efficiently, and avoid detection.

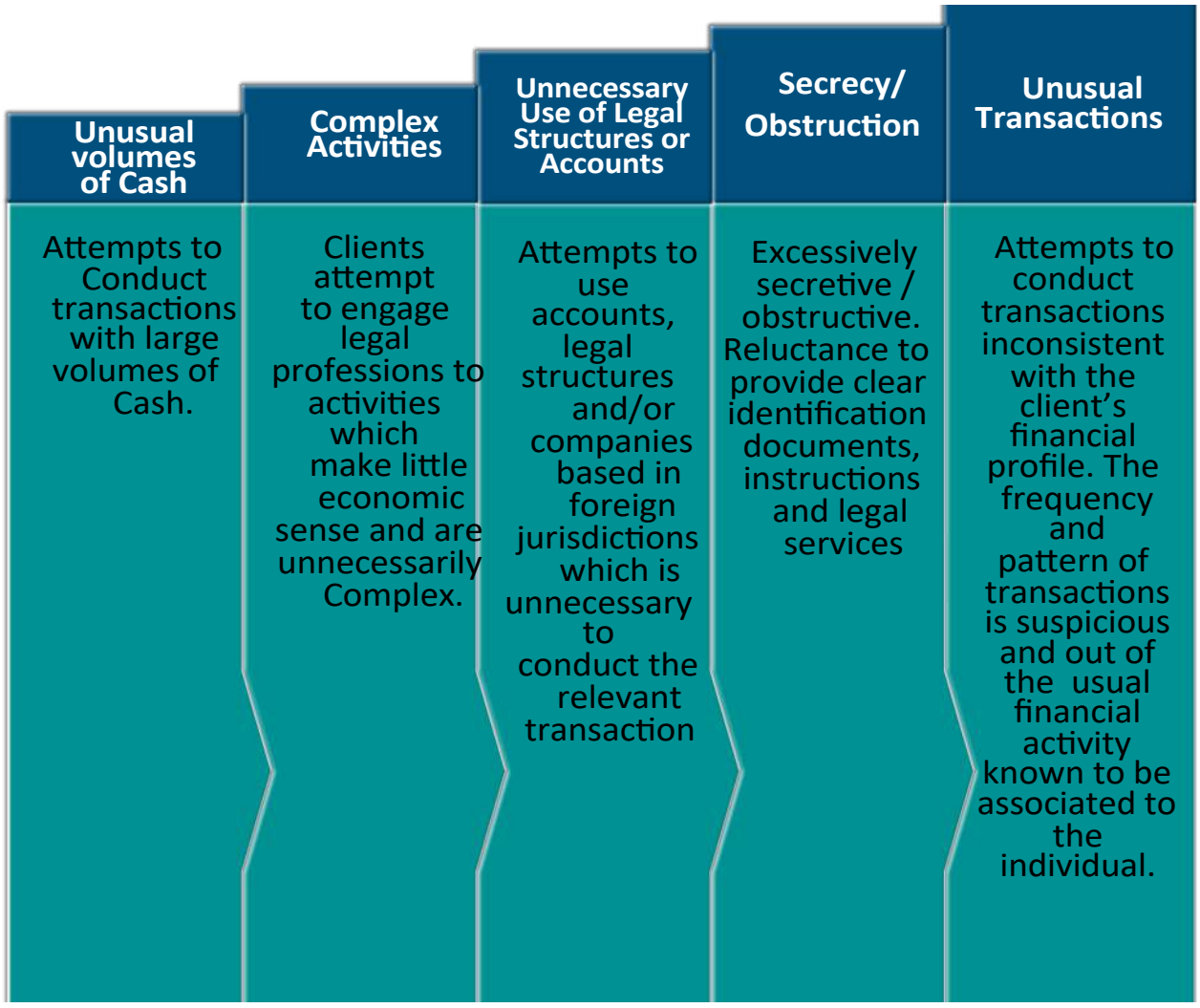
Many of the functions performed by lawyers, notaries and other legal professionals are susceptible to potential money laundering. These include but are not limited to involvement in the purchase and sale of real estate, asset/financial management, company creation/ management, purchase and sale of businesses.

7.7.2 Attorneys/Law Firms Industry risks

7.7.3 Mitigating Attorneys/Law Firms Industry AML/CT risks



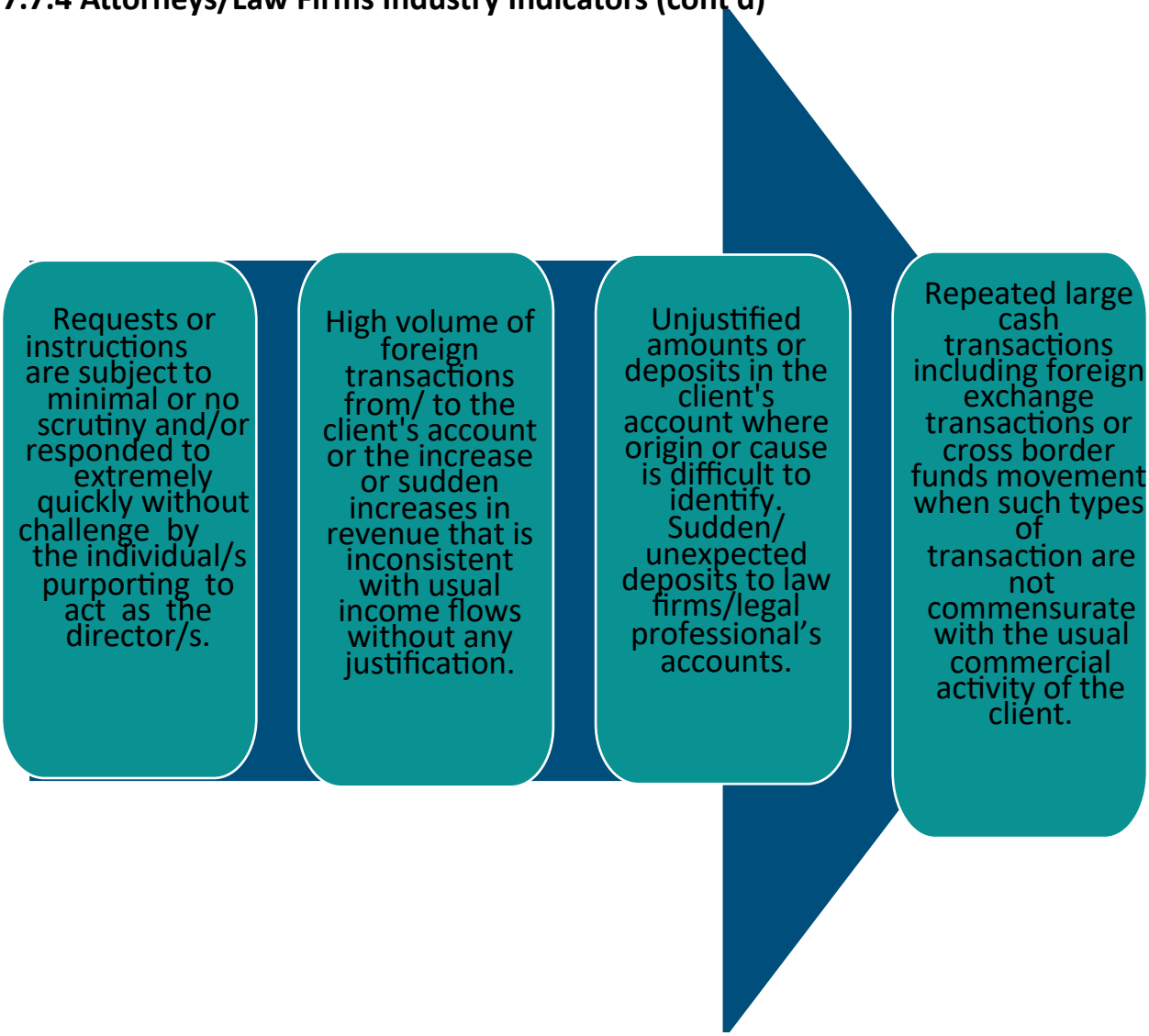
7.7.4 Attorneys/Law Firms Industry Indicators



7.7.4 Attorneys/Law Firms Industry Indicators (cont'd)

Disregard for Advice	High Value Monetary Instruments	Unexpected/ 3rd Party Funds	Disproportionate Transactions
Even after being provided with sound advice, the client is unconcerned about incurring losses or realizing extremely low profits in comparison with persons engaged in similar business activities.	Client's receipt of cash or high value cheques which does not correlate to the volume of work or type of business/ job activity, particularly if funds are derived from persons without clear, or with ambiguous connections to the client.	Unexpected funds, or funds into and out of the company are sent to, or received from unidentified third party/ies.	Disproportionate amounts, frequency and nature of transactions carried out by the customer that are inconsistent with the nature of his/her business, profession or known and declared activity. Particularly if these transactions are carried out with countries exposed to high ML/TF risks.

7.7.4 Attorneys/Law Firms Industry Indicators (cont'd)



7.8 BANKS

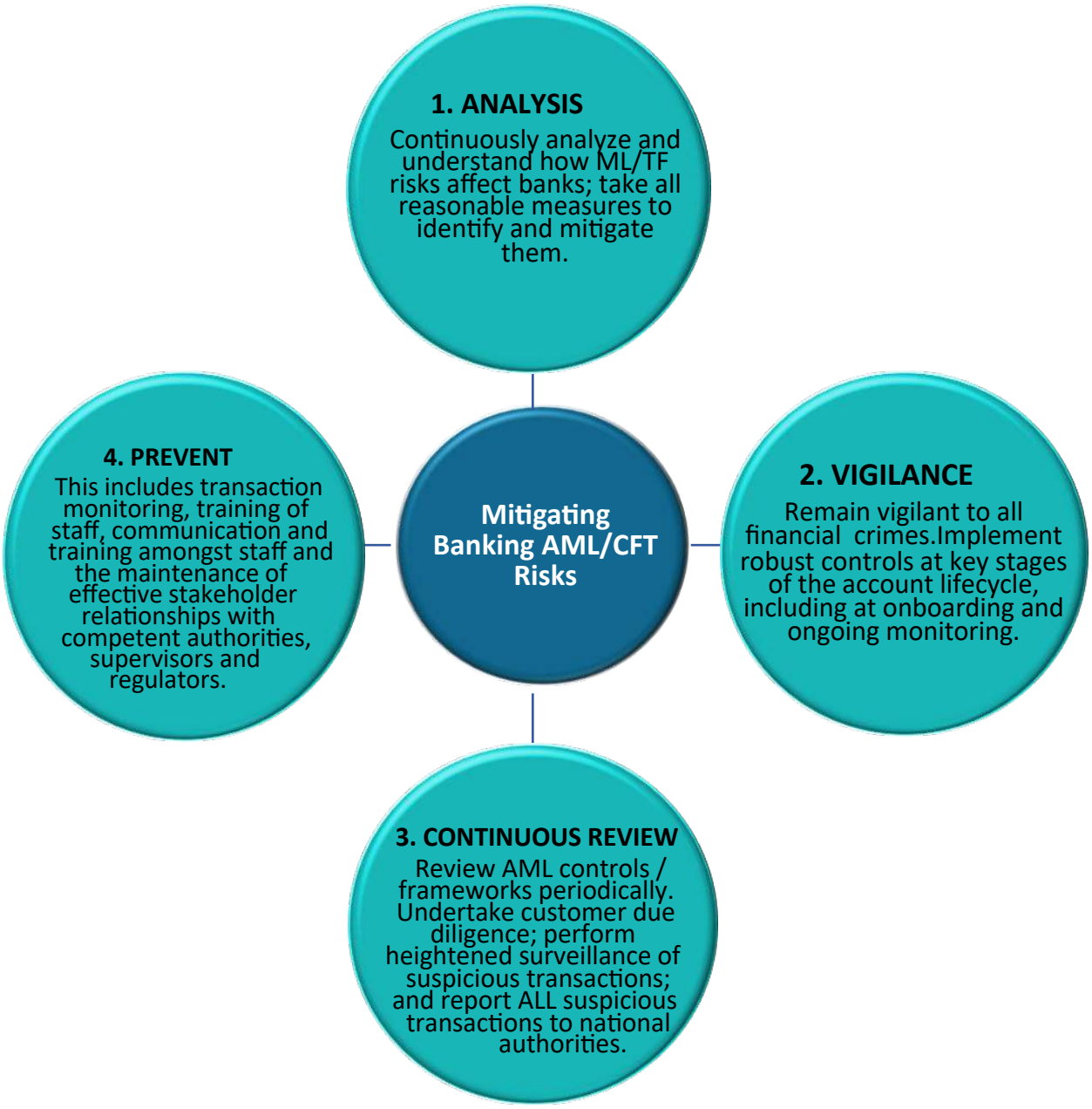
7.8.1 Why should banks engage in AML/CFT compliance?

Curb Criminality	Protect Rights	Financial System Integrity	Avoid Sanctions/ Blacklisting	Mitigate Risks
To curb criminality in general by making it difficult for criminals to benefit from the proceeds of their crimes.	To protect the rights of persons violated by financial and other related crimes by aiding the confiscation of illegally obtained funds.	To protect the integrity of the Financial system as Banks play a key role in the local and global financial system.	To avoid sanctions/ blacklisting by the Financial Action Task Force which could affect correspondent banking relationships.	AML/CFT compliance programs mitigate the risks faced in doing business with good risk management vs risk avoidance.

7.8.2 Banking industry AML/CFT AML/CFT risks

Banking Industry Risks			
1. Higher Exposure Based on the bank, customer attributes, transaction volumes and complexities, banks have a higher exposure to money laundering and terrorism financing.	**2. Financial Losses** Banks can incur millions in losses through financial crimes; and penalties.	**3. Destabilisation Volatility and Inflation** ML/TF/PF can damage national financial systems, destabilize economies through increased demand for cash, increased volatility in interest and exchange rates and inflation.	**4. Sanctions, Blacklists & Severed Correspondent Banking Relationships** Damaged country / reputation could lead to sanctions, backlisting and severed or challenging correspondent banking relationships.

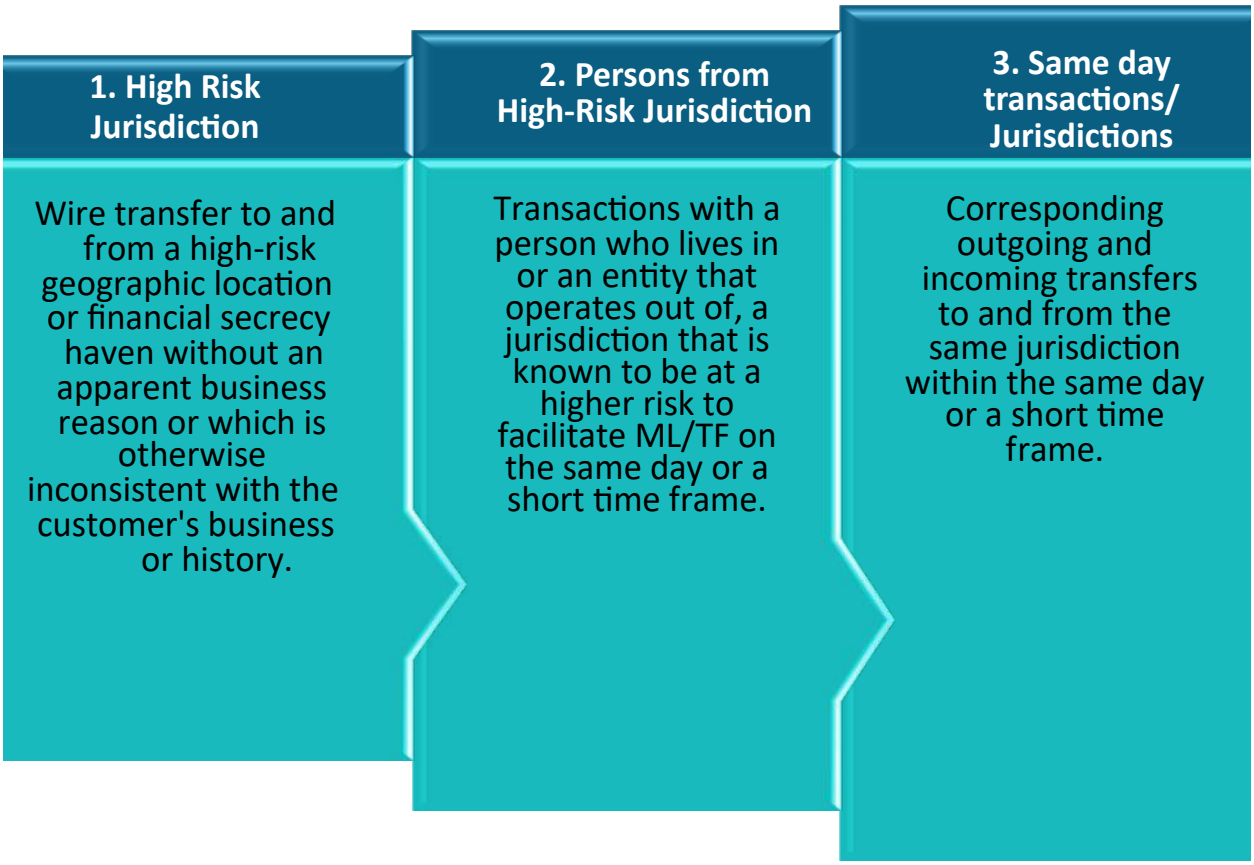
7.8.3 Mitigating Banks AML/CFT AML/CFT risks



7.8.4 Banks Industry Indicators – Customer Profile

1. Fraudulent ID/Documents	2. Financial Profile	3. Third Party Involvement	4. Unrelated Individuals	5. Unconcerned with Costs/Risks
Unverifiable ID documents; use of false documents or 3rd party identification to conduct transactions or open accounts. Apparent reluctance to provide identifyinginformation.	Opening an account where the account holder does not engage in any known form of economic activity or account activity inconsistent with the customer's profile.; Income inconsistent with the customer profile.	Using company accounts for personal purposes. Customer's home/ business telephone is disconnected or the customer gives the telephone number of a third party or third-party address.	Attempted account initiation for which several individuals have signing authority even though there is no apparent family or business relationship between them. Multiple accounts held by the same customer with the same institutions.	Customer seems unconcerned with the terms of credit or cost associated with completion of a loan transaction.

7.8.5 Banks Industry Indicators – Jurisdiction



7.8.6 Banks Industry Indicators – Transactions

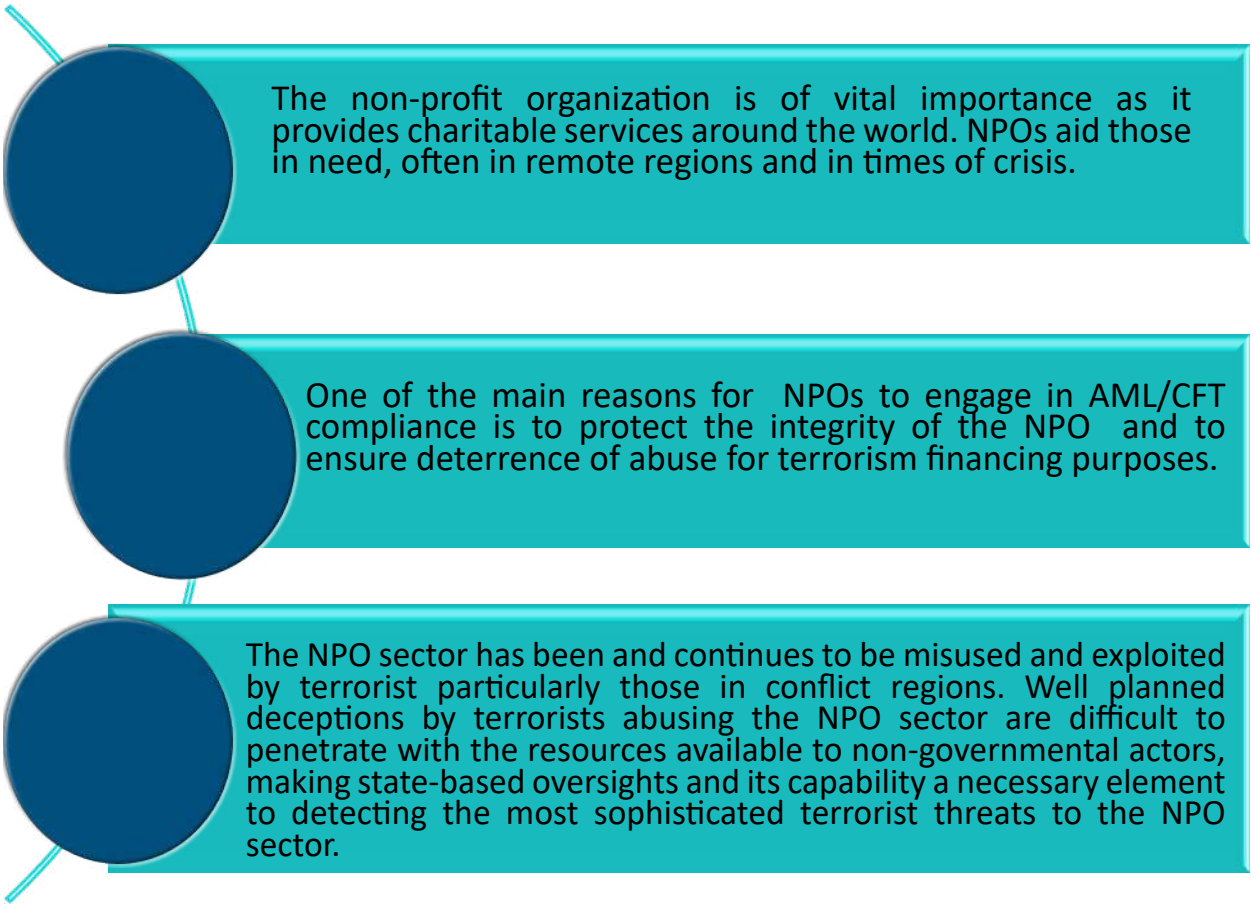
1. Fraudulent ID/Document	2. Avoid Reporting Thresholds	3. Frequent Users	4. Unusual Night Safe Use	5. Rapid Payment to Loan
Multiple deposits to one account then transferred to other account and finally request made for transfer of funds to an offshore account.	Customer makes effort to avoid the bank's reporting condition or threshold through activity such as: •Structured deposits; •Deposits across different branches; •Deposits below reporting thresholds.	Small and frequent transfers so as to avoid the bank's reporting threshold or recording of the source of funds.	Customer who prefer to use the night safe to make deposits not in line with their financial profile to avoid directly dealing with bank staff or their scrutiny.	Acquiring loan(s) and repaying same within a short period or paying back more than what is required.

7.8.6 Banks Industry Indicators - Transactions (cont'd)

6. Unusual Wire Transfer Activity	7. Delays to Information Requests	8.Other Multiple Deposit Activity
Unexplained, or repetitive wire transfers. The customer requests a high volume of incoming and outgoing wire transfers but maintains low or overdrawn account balances.	The information needed in order to enable verification or completion of application for new account.Some of the information may include the nature of the business, location of business, name of officers and directors, prior banking history, expected amount to account etc.	Multiple deposits made to the customer's account by 3rd party user or 3rd party loan repayment. Same home address provided for fund transfers by different people.

7.9 NON-PROFIT ORGANISATIONS (NPO)

7.9.1 Why Should NPOs engage in AML/CFT compliance?



7.9.1 Why Should NPOs engage in AML/CFT compliance? (cont'd)

FATF Recommendation 8	Among other recommendations raising and deepening "awareness among NPOs as well as the donor community about the potential vulnerabilities of NPOs to terrorist financing abuse and terrorist financing risks… is required by countries (FATF Standards 2012, R.8, 8.2(b)).
Non-Profit Regulations Proceeds of Crime Ordinance	•**175**. The Governor in Cabinet may make regulations providing for— •(a) the registration of non-profit organisations; •(b) the issuance by the NPO Supervisor of an Anti-money Laundering and Terrorist Financing Code applicable to non-profit organisations setting out measures, not inconsistent with this Ordinance, the regulations made under this section or the terrorist financing legislation, for the prevention and detection of money laundering and terrorist financing;

7.9.2 NPOs industry risks

1. DIVERSION OF FUNDS

When you donate to a charity, the idea is that the money you gave will go directly to help the cause they support. The diversion of funds is a risk that NPOs face because individuals within the organization can divert donated funds to non specified activities.

2. ABUSE OF PROGRAMMING

Often non-profit organizations have set programming to raise funds and benefit the mission of charity. This programming can be so that even if the flow of money into the organization is legitimate, it is used for other activities once received.

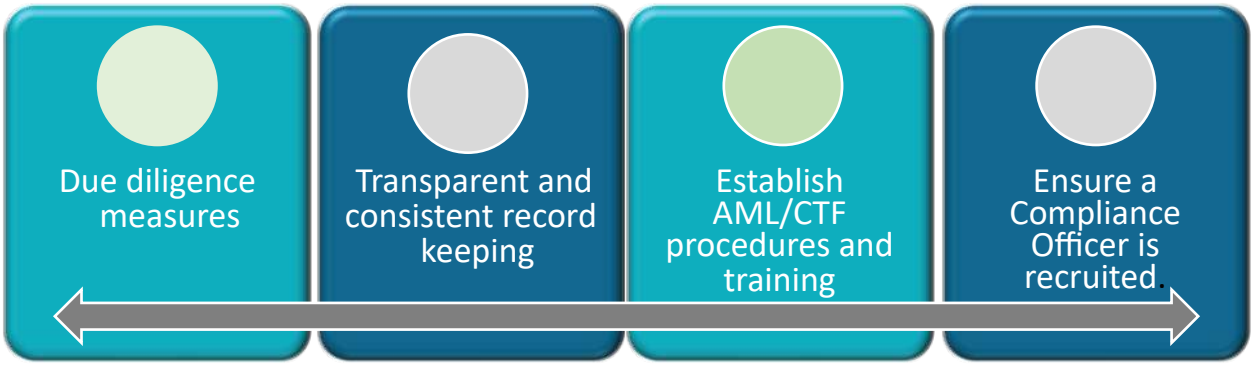
3. FALSE REPRESENTATION

An NPO may be making false representations that is working to serve the public or the environment when it is a sham used to collect funds for illegal activities. They disguise themselves as a charitable organization so that donors continue to provide support even though they are not using the funds as described.

4. AFFILIATION WITH TERRORIST GROUPS

Another high-risk area in the non-profit organization is the affiliation with terrorist groups. The group or its officials may knowingly – or unknowingly be affiliated with a terrorist organization that is using them to support their recruitment efforts and fund their illegal activities.

7.9.3 Mitigating NPOs industry AML/CFT risks

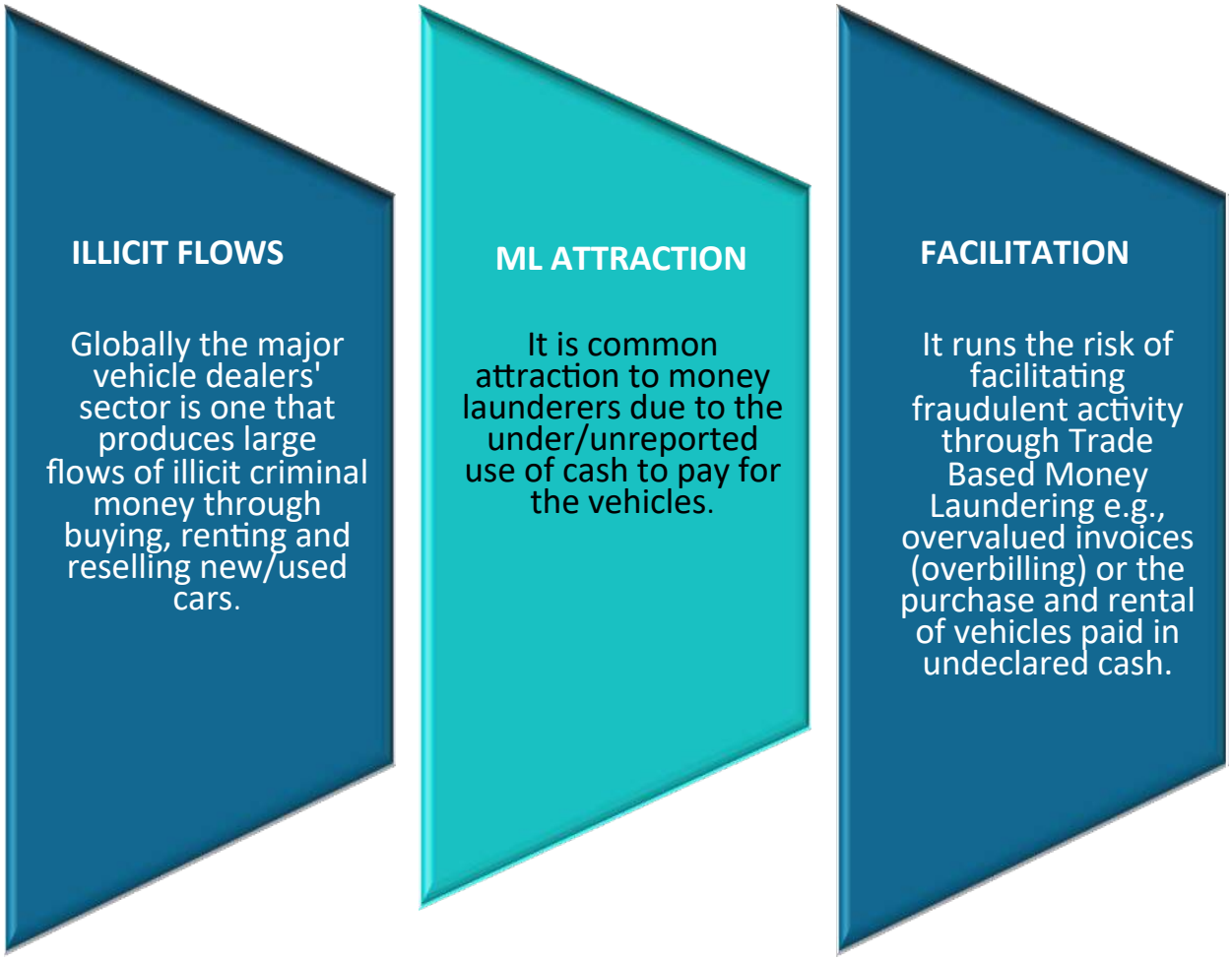


7.9.4 NPO Industry indicators

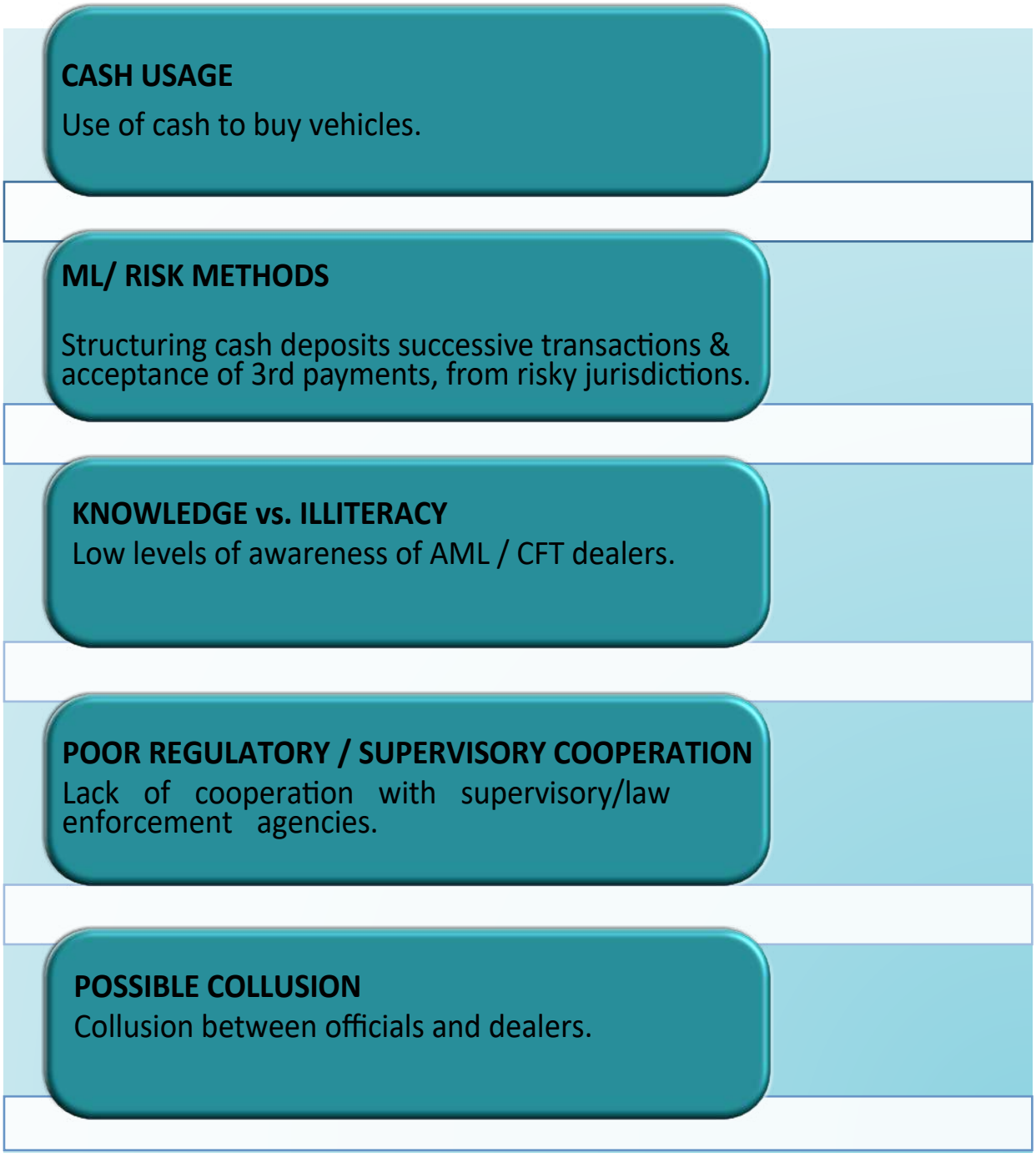
1. NPO treasurer or employee withdraws cash from NPO accounts and then deposits it into a personal account, before diverting the funds to a suspected terrorist's account.
2. Media reports the NPO is linked to known terrorist organizations or entities that are engaged, or suspected to be involved, in terrorist activities.
3. Parties to the transaction (for example: account owner, sender, beneficiary or recipient) are from countries known to support terrorist activities and organizations.
4. Funds sent from large international NPOs based in high-risk countries, to their branches in regional countries, are channeled to local NPOs based or operating in domestic conflict areas.
5. An NPO sending funds from a major public event and then authorizes a third party to be a signatory to the NPO account, who uses it to send funds to high-risk countries.
6. Unusual or atypical large cash withdrawals, particularly after a financial institution refuses to wire NPO funds overseas (thus raising cross-border cash smuggling suspicions).
7. Benefactor makes donation(s) to NPO then directs the NPO on how the funding should be distributed (possible ML indicator).

7.10 MOTOR VEHICLE DEALERS/SALESPERSONS

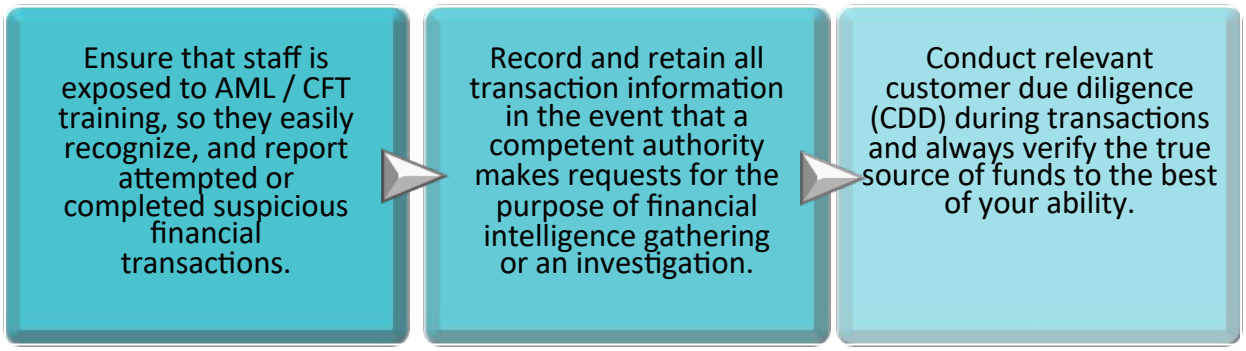
7.10.1 Why should Motor Vehicle Dealers/Salespersons engage in AML/CFT compliance?



7.10.2 Motor Vehicle Dealers/Salespersons Industry risks



7.10.3 Mitigating Motor Vehicle Dealers/Salespersons AML/CFT industry risks



7.10.4 Motor Vehicle Dealers/Salespersons Industry Indicators

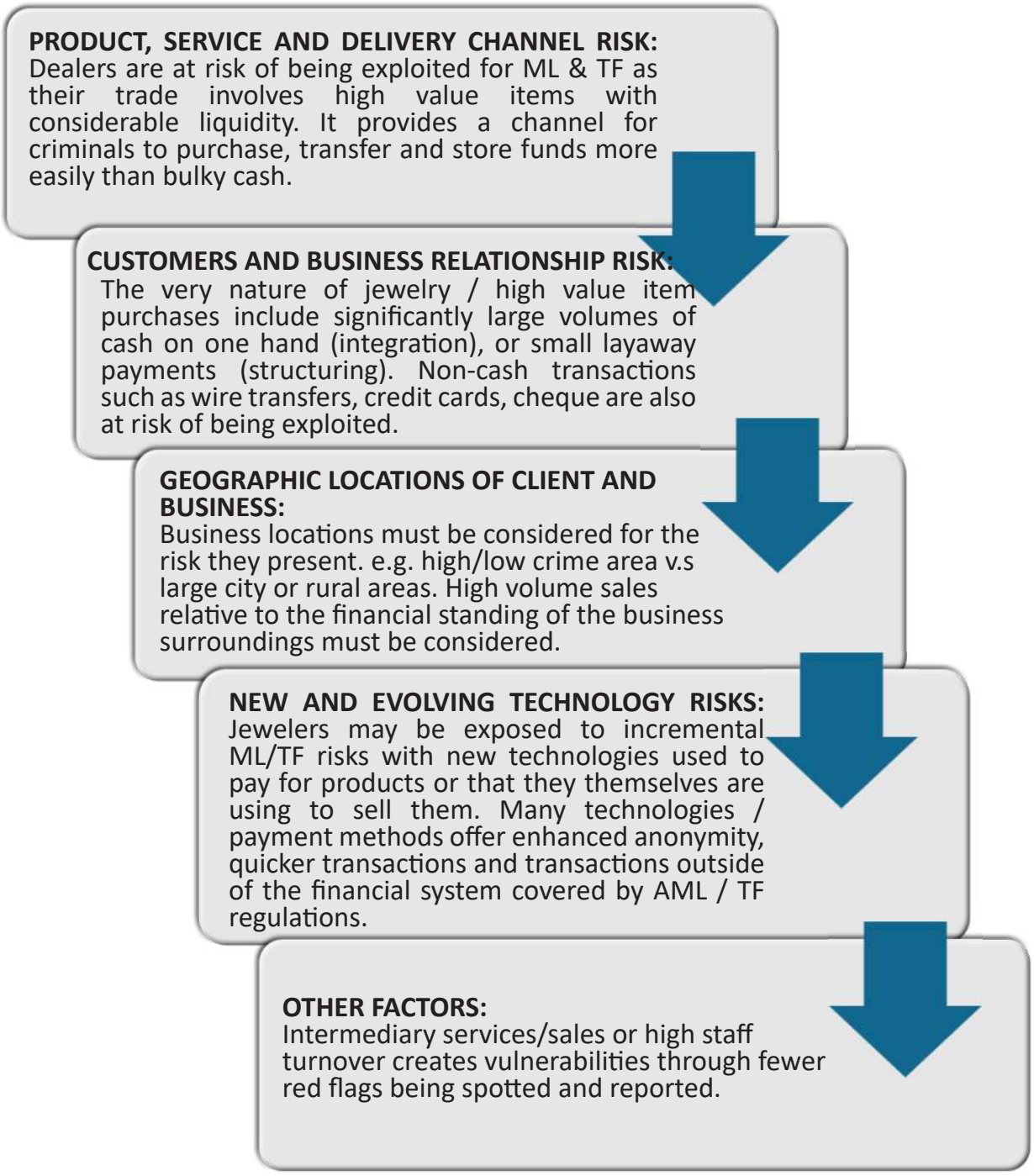
1	• Customer attempts to purchase vehicle with a significant amount of cash. • Customer is reluctant or refuses to produce personal identification documents for the transaction to be completed.
2	• Customer pays substantial down payment in cash and balance is financed by an unusual source e.g. a third party or private lender. • Purchases carried out on behalf of persons who appear to lack the economic capacity to make such purchases e.g. unemployed.
3	• Last minute cancellation of order, which means that funds would have to be reimbursed to the customer via a business cheque. • Customer purchases vehicle without inspecting it or interest in its features, specifications etc.
4	• Customer purchases multiple vehicles in a short time period, and seems to have few concerns about the type, cost, condition, etc. • Customer purchases vehicles and registers them in "Rental."
5	• Customer is known to have a criminal background. • Customer uses or produces suspicious identification / ID documents with different names.
6	• Customer does not want to put his/her name on any document that would connect him/her with the purchase of the vehicle. • Purchase appears to be beyond the means of the customer based on his/her stated or known occupation or income.

7.11 JEWELLERS/HIGH VALUE DEALERS

7.11.1 Why should Jewellers/High Value Dealers engage in AML/CFT?

- **Convenience of goods** - Jewelry, luxury brands and high value type companies are non-financial businesses who retail in high value products which represent a convenient and easier way to launder illicit proceeds.
- **Historical Method of ML** - Through luxury and high value items such as diamonds, gold, art and historical artifacts, launderers have been conducting cross-border illicit activities historically.
- **White Collar Preference** - Cash flow within these industries is also very high and they are commodities traded in international markets. Jewelry, luxury and high value items are preferred by both petty and white collar criminals.
- **Medium Risk** - The jewelers/High Value Dealer sectors has been assessed as medium risk in the TCI NRA (p.g. 116) There is an absence of any AML/CFT experience required to operate.
- **Sales Driven Environment** - The operating model of such an industry leads to sales driven cultures regardless of the source of funds.
- **High Cash Thresholds / Low SAR reporting** - The threshold of USD50,000 for High Value dealers may encourage criminals operating below such thresholds to integrate funds through this manner.

7.11.2 Jewellers/High Value Dealers Industry Risks



7.11.3 Mitigating Jewellers/High Value Dealers Industry Risks

Staff Training

Ensure that staff is exposed to AML/CFT training so that they can easily recognise and report attempted or completed suspicious transactions.

Record Details

Limit cash flow and record/detail every transaction or groups of transactions conducted by an individual above the recommended threshold.

Implement Compliance Programs

Engage in routine CDD and implement systems to track coming and outgoing payments.

Observe & Report Developing Trends

Observe any unusual or developing trend which could suggest suspicious or fraudulent activity, as well as criminal activity.

Record/Report All Suspicious Transactions

Record and report any attempted or successful suspicious transactions to the FIA and if necessary, the RTCIPF.

7.11.4 Jewellers/High Value Dealers Industry Indicators

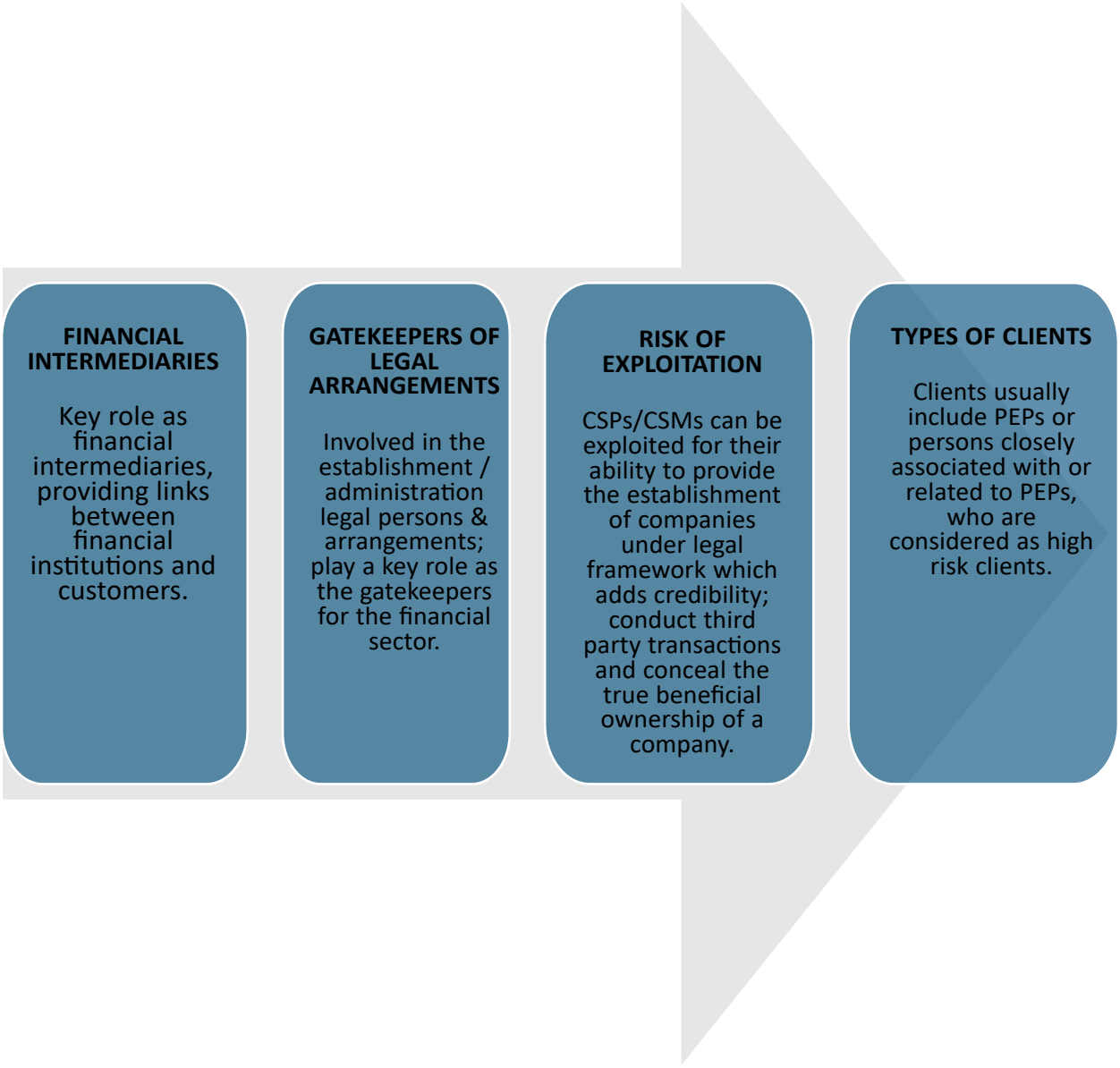
1	Customer activity does not match the customer/business' financial profile.
2	Customer is known to be involved in or indicates involvement in criminal activity .
3	Customer is hesitant, or fails to disclose identification details, utilizes unverifiable or fraudulent documents with observed name variations.
4	Customer makes purchases in the company of other individuals and is closely monitored/appears to be forced to conduct transaction. Customer places a large deposit on an item, then subsequently requests a refund of the deposit.
5	High value items purchased with large amounts of cash appears unusual and/or cash amounts presented appears dirty, musty or has an unusual smell.
6	Customer appears to be unconcerned about the price or fees associated to a particular item or customers who regularly purchase, begin making inconsistent purchases, refunds or trades.
7	Customer places large deposit on an item, then subsequently requests a refund of the deposit.
8	Customer attempts to return a recent purchase for refund with no satisfactory explanation / customer attempts to re-sell a recently purchased item at a significant discount.

7.11.4 Jewellers/High Value Dealers Industry Indicators (cont'd)

9	Customer makes attempts to develop close relationship with staff, may approach several staff members or aim to conduct transactions at different branches of the same business.
10	Customer attempts to bribe or offer favors for staff to provide suspicious or unusual services.
11	Attempts to convince staff to not complete required CDD documentation or makes effort to avoid reporting.
12	Customer cancels transactions when CDD requirements are disclosed.
13	Customer is oblivious to excessive fees or high costs or shows an uncommon interest in internal systems, controls, policies and reporting thresholds.
14	Customer tries to convincingly justify transaction which does not align with their financial profile.
15	Customer is hesitant or refuses to disclose source of funds, the source of funds raises suspicion.
16	Transaction is obviously suspicious, but customer is oblivious that he may be involved in money laundering.

7.12 COMPANY SERVICE PROVIDERS/COMPANY SERVICE MANAGER

7.12.1 Why should CSPs/CSMs engage in AML/CFT?



7.12.2 CSPs/CSMs Risks

PEPS/HIGH RISK

Clients usually include PEPs or persons closely associated with or related to PEPs.

SHELL V.S. SHELF COMPANIES

Used to conceal beneficial ownership, enhance the perception of legitimacy, reputation and add complexity to structure.

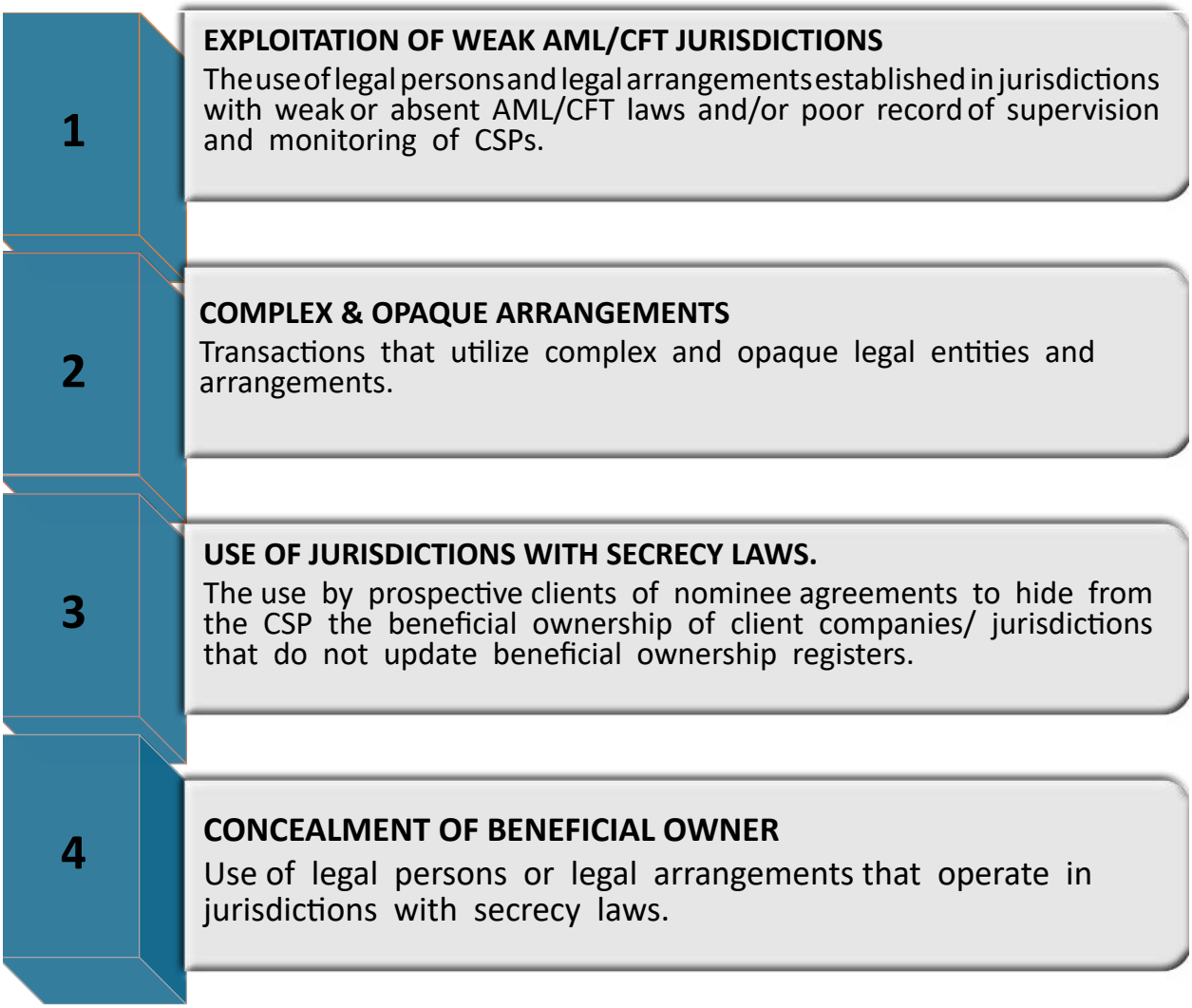
CONFIDENTIALITY EXPECTATION

Legitimate expectations of privacy and business confidentiality are held.

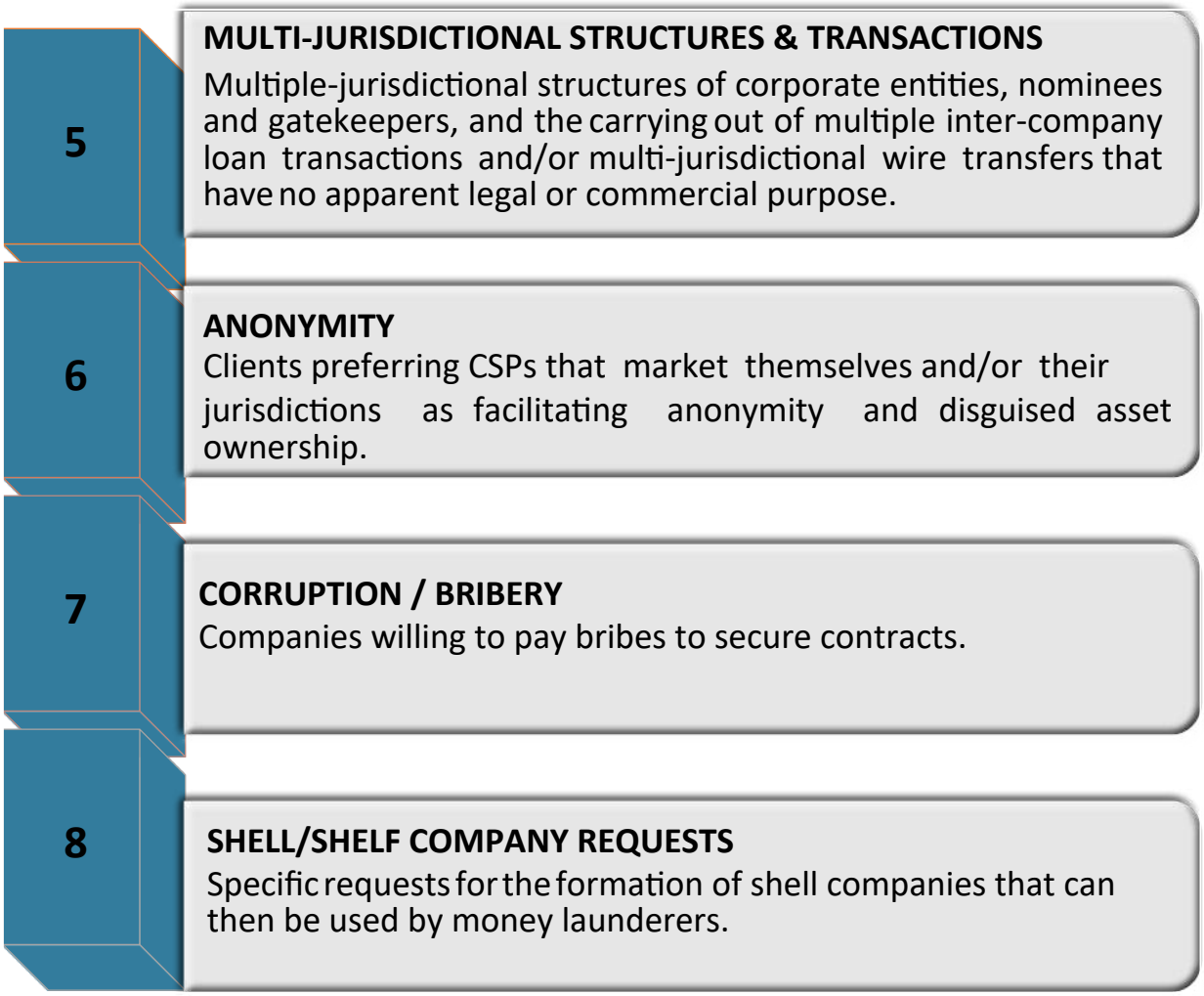
7.12.3 Mitigating CSPs/CSMs Risks

Staff AML/CFT Training	• Ensure that staff is exposed to AML/CFT training, so they easily recognize, and report attempted or completed suspicious financial transactions.
Risk Based Assessments	• Identify, manage and assess risks given the environment and implement policies to monitor any changes.
Maintain Accurate Records	• Maintain an accurate company register and document all beneficial owners, shareholders and directors.

7.12.4 CSPs/CSMs Industry Indicators



7.12.4 CSPs/CSMs Industry Indicators (cont'd)



8.0 HOW TO MAKE A SUSPICIOUS ACTIVITY/TRANSACTION REPORT

Reports of suspicious activities and transactions relating to money laundering and terrorist financing must be reported by a person or the MLRO (where applicable) to the FIA within twenty-four hours[8] after the information comes to their attention on the Suspicious Activity/Transaction Report SAR/STR form (see Appendix A), electronically via email to **submissions@fia.tc.** A copy of the SAR/STR form is available on the FIA website: www.fia.tc Additionally the form can be provided to you by contacting the FIA directly at 649-941-7691 or email **submissions@fia.tc.** If submitted by hand, your report should be sealed in an envelope, marked 'Confidential' and addressed to:

The Director
Financial Intelligence Agency
202 Cabot House, Graceway Plaza
Leeward Highway
Providenciales
Turks & Caicos Islands

Business hours are Monday – Thursday 8:00AM to 4:30PM, Friday 8:00AM – 4:00PM. Closed - Saturday, Sunday and Public Holidays.

8.1 CONTENTS OF THE SAR/STR

The quality of the information within the SAR/STR report is vital to the FIA in its analysis of the reports received. Care must be taken to ensure relevant information is included. The relevant information will include:

- Full details of the customer and as complete a statement as possible of the information giving rise to knowledge, suspicion or reasonable grounds for suspicion of money laundering and terrorist financing or both.
- If a particular type of criminal conduct is suspected, provide a statement of this conduct;
- Where a financial business has additional relevant evidence that could be made available, provide the nature of this evidence;
- Any data the FIA may require.

8. Sec. 29 (1) (e) AML- CFT Code 2011

It is pertinent that when preparing the report, have all relevant information at hand so that all information is available for analysis. This is particularly relevant for the descriptive or narrative component of the report.

The Money Laundering Reporting Officer or the Compliance Officer or Designate person when creating the report may need to give consideration to the following:

- **WHO:** There will be an entity or natural person who is conducting or conducted the suspicious activity. In this case all relevant factors of description of the customer or client (occupation, nationality, business connection, identification document, place of incorporation, date of incorporation, beneficial owners, address etc.) must be recorded. All other person connected to the suspicious activity should be included.

- **WHAT:** Describe what the activity was that occurred.

- **WHEN:** Refers to the date of the suspicious activity. If it was a sequence of events, describe the suspicions in a chronological order.

- **WHERE:** Refers to the location of the suspicious activity. This includes the address of the office or branch of the entity reporting, origination of the activity especially if another jurisdiction is involved.

- **WHY:** Indicates why the activity is considered suspicious? Provide reasons in terms of what is different or inconsistent with the client or customer's history or different to the activities of other customers.

- **HOW:** How was the suspicious transaction/activity was executed. This can include the use of internet, telephone, emails or other devices; mechanisms, business services and instruments used to conduct or attempt the suspicious activity.

8.2 SUPPORTING DOCUMENTS

If supporting documents are submitted with the report briefly describe what the documents are. Note that all documents related to the filing of a SAR/STR must be retained for minimum of 5 years.[9]

9. Anti-Money Laundering and Prevention of Terrorist Financing Code, Regulation 37

8.3 CONSIDERATION FOR ENTITIES ON SUBMISSION OF A REPORT TO THE FIA

There is nothing in the law to indicate that a business ought to continue or terminate the relationship or transaction with a customer after a SAR is submitted to the FIA. However, there must be consideration by the Reporting entity as to whether there can be an issue of tipping off if they choose to terminate any relationship where an investigation has commenced. Notwithstanding the above, it is very important that attention be paid to certain stipulations in the Regulations[10] regarding the requirements to cease transaction or terminate a business relationship.

9.0 PROCEDURES UPON THE RECEIPT OF SUSPICIOUS ACTIVITY REPORTS BY THE FIA

1. A SAR/STR acknowledgement is prepared and sent to the MLRO who submitted the report.
2. The report is assigned to a Financial Intelligence Analyst for analysis.
3. Further information may be requested by the FIA from the reporting entity for clarification, provide additional details and develop the intelligence.
4. A sanitised version of the report may be disseminated to a foreign counterpart or relevant law enforcement agency as permitted by POCO and POTO to further develop intelligence or to assist in international AML/CFT investigations.
5. When the FIA concludes its analysis of a suspicious activity, transaction or series of transactions with findings of criminal activity or regulatory breaches, the result of that analysis is disseminated to the relevant local authorities for further investigation or prosecution.

Additional feedback may be provided to the reporting entity on a case-by-case basis.

Note that submission of a report to the FIA is not an automatic indication of criminal activity, money laundering or a terrorist financing offence.

10. Anti-Money Laundering and Prevention of Terrorist Financing Regulations, Regulation 12

10.0 FILLING OUT THE SAR/STR FORM

All sections on the form should be completed where applicable. In cases where a section is not relevant to you, please insert words "Not Applicable" or simply "N/A."

All dates can be entered using the following format: dd/mm/yyyy or dd/mmm/yyyy. (E.g. 10/02/2015 or 10/Feb/2015).

If there is no available information on the subject to the suspicious activity/transaction report, the person making the report or the MLRO should indicate this with the words "No details available on the subject" in the space allocated where the subject's name should be.

The form can also be appended by making copies of the relevant section (s) if you have additional information or need to provide details on multiple subjects.

10.1 DEFINITIONS AND EXPLANATIONS OF SECTIONS ON THE SAR/STR FORM.

Section 1: Form Administrative Details		
1	**Report Date**	The date when the report is completed by the Money Laundering Reporting Officer. The dates shall be inputted in the date field and shall be in the format day, month, year (dd/mm/yyyy). This format applies to all date fields.
2	**Activity / Transaction Date**	The date when the actual suspicious activity or transaction or attempt occurred.
3	**Type of Report:** **New:** **Supplementary:** **Example:**	Tick this box if the report is of a new suspicion about a client or customer. Tick this box if the report is of a nature where you have additional or other information about a previously submitted suspicious activity/ transaction report on a subject. Explain the additional details in the narrative at Section 6 on the form and reference which previous report it pertains to. Note that a supplementary report does not relate to a new activity or transaction though similar, if it is not related to the subject of the initial report referenced. Initial Report - A financial institution reports to the FIA that a dormant account containing X dollars saw funds suddenly liquidated over a period of a few days to several persons or entities in countries with association to the illegal drug trade. Then... a similar series of transactions occurs at the institution under a different account. While the transactions have followed a similar.
4	**Location Where Activity Occurred**	Give the location of the reporting entity's office or branch where the suspicious activity or attempted transaction occurred. Some MLRO's operate out of different locations to where a SAR/STR took place. This is especially so in relation to larger entities which may have different operational offices or branches**.**
Subject 2: Details of Reporting Activity		
5	**Name of Reporting Entity**	This refers to the name under which the reporting entity is registered or incorporated.
6	**Category:**	This refers to the classification of the reporting entity for example Attorney, Bank, Casino, Insurance Company, Trust. Make your selection from the drop-down list.
7	**Telephone Number**	The telephone number at which the FIA can contact a competent person within the institution in relation to the SAR/STR filed.
8	**Email Address:**	Email address of the MLRO who submitted the report.
9	**Fax Number:**	Reporting entity's fax number.

Definitions and Explanations of Sections on the SAR/STR form (cont'd)

Section 3: Subject of the Report		
(This section should be completed if the subject is a stand-alone customer or natural person with no connection to a business entity; however, if connected this section must be completed along with Section 4)		
10	**Title**:	If a natural person enter as applies. (Example: Dr., Sir, Mr., Mrs. etc.)
11	**Last Name:**	Subject's last name.
12	**First Name:**	Subject's first name
13	**Middle Name:**	Subject's middle name if available**.**
14	**Other Names**:	Aliases which the subject is known by or answers to.
15	**Date of Birth (DOB)**:	Subject's date of birth.
16	**Place of Birth:**	Enter all details regarding the place or country of birth of the subject.
17	**Nationality**:	Enter the nationality of the subject.
18	**Address:**	Some subjects may have more than one address, particularly those which are multi-jurisdictional. All known addresses for the subject should be inputted to the form. The address details should include where available, the unit, apartment, house or other number, street, area location, state and country or in which ever format it was obtained.
19	**Occupation**:	Fully identify the occupation, profession or business of the person who conducted the transaction or attempted transaction. If the subject is self-employed, it is advisable that the specific field of his or her self-employment be stated for e.g., construction labourer, carpenter, fisherman, artist and so on.
20	**Telephone Number:**	Enter all telephone numbers on record for the subject; the number should be inclusive of the country code and area code to avoid any confusion.
21	**Forms of Identification Available:**	Enter the type of identification received from the subject during the CDD process. For example, passport, driver's license and so on.
22	**Identification Document Number:**	The identifying number for the form of identification described at item 21.
23	**Date of Issue/ Expiration:**	This is the date on the form of ID showing when it was issued and the date of expiration.
24	**Place of Issue:**	The place of issue on the ID. In some instances, this may be shown as the country of issue.
25	**Business Relationship:**	Enter the date when the relationship between the reporting entity and the subject (natural person) began and if applicable when ended.
26	**Account Number if applicable:**	Where applicable, the subject's bank account number should be placed in the allotted space. This applies if the said account(s) forms part of the suspicion or is connected to the individual(s) reported on**.**

Definitions and Explanations of Sections on the SAR/STR form (cont'd)

Section 4: Details of the Subject		
(If subject is a legal entity)		
27	**Legal Entity's Name**	The full name of the legal entity should be entered in this field.
28	**Country Registered/Incorporated:**	Enter the country where the company is registered or incorporated.
29	**Date Registered or Incorporated:**	This is the date when the legal entity or customer was registered or incorporated.
30	**Address of the Registered Office:**	Registered address or registered office for the legal entity whether local or overseas. This includes the address of the trustee.
31	**Business Address:**	This applies if the business address is different to that of registered office. Some legal entities business address and registered office will be the same.
32	**Trade or Business Activity:**	State the type of trade or activity the legal entity is engaged in. For example - holding company, trust, restaurant etc.State the type of trade or activity the legal entity is engaged in. For example - holding company, trust, restaurant etc.
33	**Business Relationship (Commenced/ Finished):**	Enter the date when the relationship between the reporting entity and the subject (other legal entity) began and ended.
34 & 35	**Was the subject introduced?**	If the business is introduced by a third party who conducted the due diligence, select the relevant option. If yes, enter the details in the allotted space at item 35 regarding the natural person or legal entity that introduced the subject to your entity.
36 & 37	**Shareholders and Directors:**	Enter the name(s) of the shareholders and directors of the legal entity. If needed additional names can be appended to the report.
38	**Ultimate Beneficial Owner(s):**	Enter the name and address of the Ultimate beneficial owner(s) (whether natural person or other legal entity/s) if different from 36 and 37 above. Also, should there be more than one beneficial owner, a list of their names and addresses can be appended to the report.
39	**Account Number if Applicable:**	Where applicable, the subject's bank account number should be placed in the allotted space. This applies if the said account(s) forms part of the suspicion or is connected to the legal entity reported on.
Section 5: Instruments/Mechanisms Used or Attempted		
40	**Instrument and Mechanism**	Chose by selecting all types that apply to the instruments/ mechanism used. (Note that this list is not exhaustive and is only for quick referencing; select other and state where applicable.)
41	**Currency/ Value:**	If a financial transaction is involved, enter the currency and the amount in which the transaction or attempt is conducted. (Example USD5,000.00, £500.00, €700.00.)
42	**Transaction Type:**	**Kindly indicate whether the transaction was successfully completed or not.**

Definitions and Explanations of Sections on the SAR/STR form (cont'd)

Section 6: SAR/ STR Narrative
Note that the allotted space will expand as you type.
This section of the report is critical. Provide a chronological and complete account of the activity/ transaction detailing what caused your suspicion (i.e.) what is unusual, irregular or suspicious. The field provided for the narrative increases as you type allowing you to provide as much information as needed. Note: It is useful to state your reason for suspicion as a caption at the beginning of the narrative or at the end. For example: • *Customer account activity is inconsistent with customer profile.* • *Customer income inconsistent with the customer's profile.* • *Declined business.* • *Adverse Media Reports or "Indirect Reports"*
Section 7: Report Preparation
This report was prepared by_____ *This section pertains to the person who prepared the Suspicious Activity/ Transaction Report.*

11.0 LEGAL CONSIDERATIONS

11.1 RECORD KEEPING

Financial businesses are required to keep records/ details[11] of any report made to the FIA for a period of 5 years. This also applies to all supporting documents submitted to the FIA.

11.2 PROTECTION OF DISCLOSURE

The Proceeds of Crime Ordinance Chapter 3.15 (POCO) and the Prevention of Terrorism Ordinance 2014 (POTO) contain specific provisions that provide protection[12] from liability for damages in relation to compliance with disclosure requirements under both Ordinances.

11. See Part 7 of the AML-CFT Code 2011

12. The POCO Section 131 & POTO Section 19

11.3. FAILURE TO DISCLOSE

The Failure to disclose[13] to the FIA knowledge or suspicion of proceeds of crime and terrorist property is a criminal offence under the POCO and POTO. Under the POCO, failure to report knowledge or suspicion of money laundering results in the person being liable on summary conviction to imprisonment for the term of twelve months or a fine of $100,000 or to both; or on conviction on indictment, to imprisonment for a term of five years or a fine without limit or to both.

Under the POTO, a person who fails to report knowledge or suspicion of terrorist property shall be liable on conviction on indictment to a fine or to imprisonment for a term of seven years, or to both.

11.4 CONFIDENTIALITY OF INFORMATION

The FIA is required to treat SARs/STRs with confidentially. Where the decision is made by the FIA to further disclose or disseminate information received by way of a SAR/STR, the FIA ensures that the identity of the originator (e.g., reporting entity or MLRO) of such report is protected or not disclosed.

11.5: PREJUDICING INVESTIGATION AND TIPPING OFF

A person commits an offence if he knows or suspects that an authorised or protection disclosure has been made and makes a disclosure which is likely to prejudice any investigation[14]. Under the POCO a person who commits an offence is liable on summary conviction to imprisonment for a term of twelve months or a fine of $50,000 or to both or on conviction on indictment, to imprisonment for a term of five years or a fine without limit or to both. Under the POTO a person who commits an offence is liable on conviction on indictment to a fine or to imprisonment for a term of ten years, or to both.

13. The POCO Section 127 & the POTO Section.

14. Attention should be given to Section 129 and of POCO & Section 32 of the POTO

12.0: CONCLUSION

This document provided general guidance to assist persons and various categories of reporting entities to understand their AML/CFT responsibilities and requirements under various connected legislation. Information was also provided on some general indicators for money laundering and in some cases those specific to various categories of businesses and entities. It also provided guidance on how to complete SARs and how to report them to the FIA.

It is important to recognise that it is not the function of the reporting entities to investigate suspicious transactions beyond assembling the basic facts necessary to establish that a transaction is suspicious. It is thus expected that upon analysis by the FIA, a large proportion of reports received by the FIA may not be linked to criminal activity. (IMF/World Bank FIUs: An Overview,2004: 42).

It is anticipated that you would have found this guidance to be a useful guide to having a better understanding of the AM/CFT regime and specifically your role and that of the FIA regarding the submission, receipt, analysis and dissemination of suspicious activity reports. Comments and feedback which would help you to improve your understanding of SAR requirements are welcome and can be submitted to administration@fia.tc or you can call us at (649) 941-7691.

- END -

13.0 APPENDIX A

FIA SUSPICIOUS ACTIVITY / SUSPICIOUS TRANSACTION (SAR/STR) FORM (AMENDED 2022)

FINANCIAL INTELLIGENCE AGENCY
TURKS AND CAICOS ISLANDS

SUSPICIOUS ACTIVITY/ TRANSACTION REPORT

11.20145127-8-SARSTRF-0122-1.3

FOR OFFICIAL USE ONLY

Save and Print | Start Over

SECTION 1	
1. Report Date (dd/mm/yyyy):	2. Activity/Transaction Date(dd/mm/yyyy):
3. Type: ☐ New ☐ Supplementary	4. Location where activity occurred:

SECTION 2: DETAILS OF REPORTING ENTITY	
5. Name of Reporting Entity:	
6. Category:	7. Tel. Number:
8. Email Address:	9. Fax Number:

SECTION 3: SUBJECT OF THE REPORT *(this section should be completed if the subject is a stand-alone customer or natural person with no connection to a business entity; however if connected, this section must be completed along with Section 4).*	
10. Title:	11. Last Name:
12. First Name:	13. Middle Name:
14. Other Names:	15. DOB:
16. Place of Birth:	17. Nationality:
18. Address:	
19. Occupation:	20. Tel. Number:
21. Forms of Identification Available(i.e. Passport, Driver's License and others):	
22. Identification Document Number:	
23. Date of Issue/Expiration:	24. Place of Issue:
Business Relationship: 25. Commenced (dd/mm/yyyy):	Finished (dd/mm/yyyy):
26. Account Number if Applicable:	

Suspicious Activity/ Transaction Report Form for the Reporting of Unusual /Suspicious Activities/ Transactions in Accordance With Sections 127 & 128 Of The Proceeds Of Crime Ordinance and Sections 13&16 of the Prevention of Terrorism Ordinance.

Completed reports should be submitted electronically to submissions@fia.tc. **The document FIA-SARGUIDE-0222-2.0** provides details on the completion of this form. To view this document, click HERE.
Contact the FIA at **1-649-941-7691/3692/8429** for any queries

Page **1** of **3**

FIA Suspicious Activity / Suspicious Transaction (SAR/STR) Form (cont'd)

SECTION 4: DETAILS OF SUBJECT *(if subject is a legal entity)*	
27. Legal Entity's Name:	
28. Country Registered/ Incorporated:	29. Date Registered/ Incorporated (dd/mm/yyyy):
30. Address of the Registered Office:	
31. Business Address:	
32. Trade or Business Activity:	
33. Business Relationship: Commenced (dd/mm/yyyy):	Finished (dd/mm/yyyy):
34. Was the subject introduced? ☐ Yes ☐ No	
35. **If Yes, state full details and address of introducer in the space below:** Name: Address:	Tel. Number:
36. **Shareholders**: Name:	Name:
37. **Directors**: Name:	Name:
38. **Ultimate Beneficial Owner (s):** Name: Name:	Address: Address:
39. **Account Number if Applicable**:	

SECTION 5: INSTRUMENTS/MECHANISMS USED/ATTEMPTED *(Choose by ticking all that apply to the instrument/mechanism used)*			
40. Instruments and Mechanisms ☐ Notes/ Currency ☐ Credit/ Debit Card ☐ Other :	☐ Cheque ☐ Wire / Money transfer	☐ Letter of credit ☐ Insurance policy	☐ Mutual fund ☐ Gaming chips
41. Currency &Value:			

42. Transaction Type: ☐ Completed ☐ Attempted

Suspicious Activity/ Transaction Report Form for the Reporting of Unusual /Suspicious Activities/ Transactions in Accordance with Sections 127 & 128 of The Proceeds Of Crime Ordinance and Sections 13 & 16 of the Prevention of Terrorism Ordinance.

Completed reports should be submitted electronically to submissions@fia.tc. The document FIA-SARGUIDE-0222-2.0 provides details on the completion of this form. To view this document, click HERE.
Contact the FIA at **1-649-941-7691/3692/8429** for any queries

Page 2 of 3

FIA Suspicious Activity / Suspicious Transaction (SAR/STR) Form (cont'd)

SECTION 6: SAR/ STR NARRATIVE: This section of the report is critical. Provide a chronological and complete account of the transaction/activity detailing what caused your suspicion i.e. what is unusual, irregular or suspicious. *The field provided for the narrative increases as you type allowing you to provide as much information as needed.*

SECTION7: This report was prepared by	
Last name:	
First name:	
Title/ Post:	
Phone number:	
Date report was prepared:	

Suspicious Activity/ Transaction Report Form for the Reporting of Unusual /Suspicious Activities/ Transactions in Accordance with Sections 127 & 128 of The Proceeds Of Crime Ordinance and Sections 13 & 16 of the Prevention of Terrorism Ordinance.

Completed reports should be submitted electronically to submissions@fia.tc. The document **FIA-SARGUIDE-0222-2.0** provides details about the completion of this form. To view this document, click HERE.
Contact the FIA at **1-649-941-7691/3692/8429** for any queries

Page **3** of **3**

14.0 APPENDIX B

FIA TERRORIST PROPERTY REPORT (TPR) FORM

FOR OFFICIAL USE ONLY

ORD92014-TERREPF-0515-1.0

FINANCIAL INTELLIGENCE AGENCY
TURKS AND CAICOS ISLANDS

Save and Print | Start Over

Terrorist Property Report Form

SECTION 1- DETAILS OF REPORTING ENTITY	
Name of Reporting Entity:	
Address of Reporting Entity:	
Category:	**Tel. Number:**

SECTION 2- DESIGNATED INDIVIDUAL *(individual(s) listed as a terrorist; connected to terrorism or part of a terrorist group/organization or owned or in control of or dealing in property for the benefit of a designated organisation or individual)*	
Last Name(s):	**First Name:**
Middle Name(s):	**Other Name(s):**
DOB:	**POB:**
Apt. No.:	**Street Address:**
Town/City:	**Country:**
Forms of Identification Available *(for e.g. passport, driver's license and others)*:	
Identification Document Number:	
Nationality:	**Occupation/place of employment:**
Contact Number:	**Email Address:**

SECTION 2B- DESIGNATED GROUP OR ORGANISATION *(listed as a terrorist group or organization, connected to terrorist financing or terrorist group, owned or in control of terrorist property for the benefit of designated group/organization or individual.)*	
Name of Group or Organization:	
Street Address:	**Town/City:**
Country:	**Contact Number:**
Email Address:	**Website:**

SECTION 3- ENTITY(includes incorporated or unincorporated entities or businesses which you believed to be in control of or undertaken transaction(s) regarding terrorist property for the benefit of a terrorist oranisation/group or individual.	
Entity's Name:	
Registered Office:	
Business Address:	
Trade or Business Activity:	
Tel. Number:	**Email Address:**

Reporting of Terrorist Property in accordance with Sections 13 - 16 of the Prevention of Terrorism Ordinance 2014.

Page 1

FIA Terrorist Property Report Form (cont'd)

ORD92014-TERREPF-0515-1.0

SECTION 4- DETAILS OF PROPERTY(refers to property you know or suspect to be terrorist property whether owned; under the control of or that you believe will be used for terrorist acts.	
Type of Property:	**Value of Property:**
Location of Property:	
Property Number:	**Account Number:**
Type of Account:	**Account Holder:**

SECTION 5- REASON FOR KNOWLEDGE OR SUSPICION OF TERRORIST PROPERTY(give details of how you came to know or suspect that the property is terrorist property, any completed or potential transactions regarding the property, transaction conducted by whom and on whose behalf, the date of such transaction etc. See Guidance Note for more details.)
States:

SECTION 6- THIS REPORT WAS PREPARED BY	
Last Name:	First Name:
Title/Post:	
Phone Number:	Date Report Prepared:

Reporting of Terrorist Property in accordance with Sections 13 - 16 of the Prevention of Terrorism Ordinance 2014.

Page 2