GUIDANCE NOTES ON SUSPICIOUS TRANSACTIONS / ACTIVITIES

Report anything suspicious

Monitoring & Compliance

Updated August 2022
(October 2018)

Guidance

GUIDANCE NOTES ON SUSPICIOUS TRANSACTIONS / ACTIVITIES

Contents

ACRONYMS

AML	Anti-Money Laundering
AMLCO	Anti-Money Laundering Compliance Officer
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ML	Money Laundering
SA	Suspicious Activity
SAR	Suspicious Activity Report
ST	Suspicious Transaction
STR	Suspicious Transaction Report
TF	Terrorist Financing

A. PURPOSE

This guidance note is prepared to assist ICPAC's members in obtaining a practical and comprehensive approach to **recognizing** and **reporting** suspicious activity as required under "The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007", as amended from time to time (the "AML Law") and the ICPAC's Directive on the Prevention and Suppression of Money Laundering Activities (the "Directive").

The Money Laundering and Terrorist Financing (ML/TF) environment is constantly changing, and individuals involved in such activities are continually attempting to exploit services and products offered by professionals in an effort to disguise the true nature of their illicit activities and proceeds. This guidance note is a summary of non-exhaustive steps and best practices to be adopted by ICPAC's members (as obliged entities[1] / persons subject to the Law) when dealing with the execution and/or review of clients' transactions and activities and the assessment of suspicion.

[1] Definitions found in Appendix I

B. SUSPICIOUS ACTIVITY, SUSPICIOUS TRANSACTION / REPORTING REQUIREMENT

I. Suspicious Activity/ Suspicious Transaction

Suspicious activity/transaction can be identified both during the on-boarding or ongoing due diligence of a client as well as during the transaction monitoring process and may be raised by any employee of an obliged entity.

Suspicious Activity (SA)	• Arises from suspicion relating to general ***behaviour*** of the person in question which creates the knowledge or belief that he or she may be involved in illegal activities out of which revenue might be generated.
Suspicious Transaction (ST)	• Arises from the suspicion created by a specific ***transaction***, which creates the knowledge or belief that the transaction may relate to the legitimisation of proceeds from illegal activities.

II. Reporting Requirements

The reporting requirement for suspicion arises from *articles 27 and 69(d) of the AML Law* and relates to Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs).

Article 27 of the Law:

"*A person **who knows** or **reasonably suspects** that another person is engaged in laundering or financing of terrorism offences, and the information on which that knowledge or reasonable suspicion is based, comes to his attention in*

the course of his trade, profession, business or employment, shall commit an offence if he does not disclose the said information to the Unit[2] *as soon as is reasonably practicable after it comes to his attention. An offence under this section shall be punishable by imprisonment not exceeding two years or by a pecuniary penalty not exceeding five thousand euro or by both of these penalties*".

Article 69 (d) of the Law:

It is required that when obliged entities *"know or have reasonable suspicion that monetary sums, irrespective of the amount thereof, constitute proceeds from illegal activities or relate to terrorist financing, to ensure the Unit is immediately notified, on their own initiative, by submitting a relevant report and providing supplementary information after a relevant request by the Unit. It is provided that, the obligation to report to the Unit includes also the attempt to execute such suspicious transactions*".

In order for a report to be useful for analysis and processing, it needs to be a **quality report**, i.e. the information submitted must be **sufficient and complete** to enable a connection to be made between the person(s) and the suspicious activity/transaction. Investigations are often based on multiple SARs, and although you may feel that your report in isolation does not provide much information, it could be the missing piece of a much larger puzzle[3]. For further guidance on reporting, see section ***H***.

[2] MOKAS

[3] ICAEW: Suspicious Activity reporting guidance

C. COMPLIANCE OFFICER'S (CO) RESPONSIBILITIES

According to article 69 (a) of the Law, obliged entities have to *"appoint a senior staff member who has the ability, the knowledge and the expertise as a money laundering compliance officer to whom a report is to be made about any information or other matter which comes to its attention and which, in its opinion, proves or creates suspicion that another person is engaged in a money laundering offence or terrorist financing"*.

The CO is considered to be the contact point for all AML issues for internal purposes and external authorities and should have the responsibility for reporting suspicious activity/transactions to MOKAS. Each obliged entity has the responsibility to notify MOKAS about the appointment. To this effect, ICPAC has issued circular CC 31/2022 to provide further guidance on the obligation.

The CO must develop an effective suspicious activity/transaction monitoring and reporting policy and create a **culture of compliance**, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks. Such policies, controls and procedures should be proportionate to the nature and size of the obliged entities.

The CO should also establish an internal reporting procedure that enables relevant employees to disclose their knowledge or suspicions of ML/TF as soon as it is practically possible by filing an Internal Suspicion Report.

The CO has the duty to validate and consider the information received through the Internal Suspicion Report by reference to any other relevant information, including monitoring and investigating transactions and discuss the circumstances

of the case with the reporting employee concerned and, where appropriate, with the employee's superior(s). The evaluation of the information reported to the CO should be recorded and retained on file as per paragraph 9.3.8 of **ICPACs AML/CFT Directive** (see section C.3).

Should the CO assess the activity or transaction as suspicious, he/she has the obligation to file a SAR or a STR accordingly to MOKAS the soonest possible. The filing of a report is done though registering the obliged entity in the '**goAML system**', which is a sophisticated IT system used to submit SARs and STRs. To assist with the registration, MOKAS has issued a **goAML Web User's Guide – Registration Instructions.**

C.1 Staff Training

The CO is the person responsible to determine whether the firm's employees have the necessary knowledge on combating Money Laundering and Terrorist Financing or whether further training is required.

The term 'training' includes, other than formal training courses, communication that serves to educate and inform employees, such as emails, newsletters, guidance notes, periodic team meetings and anything else that facilitates the sharing of information.

Firms should firstly identify the target audience and each department/position should be trained on topics and issues that are relevant to them. After the target audience is identified, the

A successful training program should be ongoing and not only meet the standards set out in the laws and regulations that apply to the obliged entities but should also satisfy internal policies and procedures and should mitigate the risk of getting caught up in a money laundering scandal. Training is one of the most important ways to convey the importance of AML efforts, as well as educating employees about what to do if they encounter potential money laundering.

next step is selecting the training topics (e.g. general information, legal framework, penalties from AML violations, how to react, internal policies, procedure for reporting suspicious activity internally within the firm, practical case studies of suspicious activity etc.).

In addition, to achieve an effective training program, trainers need to consider and plan the timing, location and means of training.

C.2 Reporting Policy

Suspicious or unusual transaction reporting policy includes:

a) Procedures to identify suspicious or unusual transactions or activity through various channels, including employee observations or identification, inquiries from law enforcement or alerts generated by transaction monitoring systems;
b) A formal evaluation of each instance of, and/or continuous unusual transactions or activity;
c) Documentation of the suspicious transaction/activity reporting decision (i.e. irrespective of whether a report was submitted to the authorities or not);
d) Procedures to periodically notify senior management or the board of directors of suspicious transactions/activities submissions;
e) Employee training on detecting suspicious transactions or activity; and
f) Procedures to protect the person submitting an internal suspicious report.

C.3 Documenting Reporting Decisions

In order to control legal risks, it is important that adequate records of internal SARs and STRs are kept. This is usually done by the CO and would normally include details of:

a) All internal SARs / STRs made;
b) How the CO handled matters, including any requests for further information;

c) Assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek additional information;
d) The rationale for deciding whether or not to proceed with an external SAR/STR;
e) Any advice given to engagement teams about continuing the business relationship and any relevant internal approvals granted in this respect.

These records can be simple or sophisticated, depending on the size of the business and the volume of reporting, but always need to contain, broadly, the same information and be supported by the relevant working papers. The maintenance and retention of such records is important as they justify and defend the actions taken by the CO and/or other members of staff and should be made available to the Competent Authorities and MOKAS upon request.

For practicality purposes and ease of reference, a reporting index could be kept and each internal SAR/STR could be given a unique reference number.

D. RED FLAGS / EXAMPLES OF SUSPICIOUS ACTIVITY (SA) AND SUSPICIOUS TRANSACTION (ST)

Suspicion can be defined as:

- A state of mind more definite than speculation but falling short of evidence-based knowledge;
- A positive feeling of actual apprehension or mistrust;
- A slight opinion, without sufficient evidence.

Suspicion is not:

- A mere idle wondering;
- A vague feeling of unease.

Red flags/indicators[4]

ML/TF indicators are potential red flags that could initiate suspicion or indicate that something may be unusual in the absence of a reasonable explanation. Red flags typically stem from one or more factual characteristics, behaviours, patterns or other contextual factors that identify irregularities related to financial

[4] The list is not exhaustive

transactions or attempted transactions. These often present inconsistencies with what is expected of your client based on what you know about them. [5]

Suspicious Customer Behaviour

- overly secretive client
- client refuses to provide information
- client shows familiarity with process
- client has used/changed a number of advisors in short space of time
- client appears disinterested with outcome
- client is prepared to pay substantial abnormally high fees
- client shows inadequate knowledge of transactions
- client uses multiple bank accounts
- client requests an unusual short or deferred repayment schedule
- client does not want to receive correspondence to home address
- client avoids face-to-face meetings
- Evidence of untruthfulness on behalf of the client (e.g. providing false or misleading information)
- Client exhibits nervous behaviour

Suspicious Customer Identification Circumstances

- client provides counterfeit documents
- client only provides copies rather than original documents
- client only provides foreign, unverifiable identity documents
- client only acts through a third party
- Client displays a pattern of name variations from one transaction to another or uses aliases

[5] Source: Fintrac

- Client appears to be collaborating with others to avoid client identification or reporting thresholds.

Suspicious Employee Activity

- eagerness to work long hours when the office is closed or take on additional work from other colleagues
- rarely taking a vacation leave or working during Public holidays

Suspicious economic profile

- there is lack of sensible/commercial/financial or legal reason for business
- absence of documentation to support a client's claims
- business cannot be found on the internet
- creation of complicated ownership structures
- funds invested in dormant companies
- transactions involve non-profit or charitable organisations for which there appears to be no logical economic purpose
- The transactional activity far exceeds the projected activity at beginning of the relationship.

Suspicious Transactions

- large cash transactions/exchange of small bills for large ones
- multiple transactions in a short period of time
- finance is not provided by a credit institution
- transfer of large amounts of money to or from overseas locations with instructions for payments in cash
- cash deposits/withdrawals that fall consistently below the relevant transaction threshold
- mortgages are repeatedly repaid quickly
- unusual source of funds

- request for payments to third parties
- client receives high injection of capital
- back to back property transactions
- The transactional activity (level or volume) is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information (e.g. student, unemployed, social assistance, etc.).
- Client appears to be living beyond their means
- Client uses notes, monetary instruments, or products and/or services that are unusual for such a client
- Conducting transactions when the client's address or employment address is outside the local service area without a reasonable explanation
- Transactions displaying financial connections between persons or entities that are not usually connected (e.g. a food importer dealing with an automobile parts exporter).

Suspicion on terrorist financing and weapon proliferation

- Client conducts uncharacteristic purchases (camping gear, weapons, hydrogen peroxide)
- Client trades in commodities that may be dual used in chemical and biological weapons
- Client donates to a cause that is subject to derogatory publicly available information (NPO's, NGO's, charity)
- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- Person or entity's online presence supports violent extremism or radicalization.

Suspicious Customer Relations

- parties connected without an apparent business reason
- client is known to have convictions or currently under investigation
- age of parties is unusual for type of transactions
- client has known connections with criminals

E. DETERMINE WHETHER TO REPORT OR NOT

In making a decision on whether to make a report, the following factors will need to be taken into account:

a. Whether or not the activities/transactions in question consist of instances of reportable (suspected) ML/TF. For additional guidance refer to the Case Studies on fighting Money Laundering, Terrorist Financing and Economic Crime.

b. Whether the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege (Refer to *article 26(2)(a) of the Law*: if in good faith this is not treated as a breach of confidentiality; if in doubt contact your legal advisor).

c. Whether unusual activity appears during the ongoing monitoring of a client's information (i.e. the activity of the client is not in line with the initially documented economic profile).

d. A SAR may also be required when there are "reasonable grounds" to know or suspect. This is an objective test, i.e. the standard of behaviour expected of a reasonable person in the same position. Claims of ignorance or naivety does not constitute defense. Additional monitoring and investigation of transactions should be performed prior to submitting a SAR.

F. WHEN TO REPORT?

Should I report to the AMLCO?

Do I have knowledge or suspicion of criminal activity resulting in someone benefitting?

Am I aware of an activity so unusual or lacking in normal commercial rationale that it causes a suspicion of money laundering?

Do I know or suspect a person or persons of being involved in crime, or does another person who I can name, have information that might assist in identifying them?

Do I know who might have received the benefit of the criminal activity, or where the criminal property might be located, or have I got any information which might allow the property to be located?

Do I think that the person(s) involved in the activity knew or suspected that the activity was criminal?

Can I explain my suspicions coherently?

As the AMLCO, should I report externally?

Do I know or have reasonable grounds to suspect that another person is engaged in ML; and

Did the information or other matter giving rise to the knowledge or suspicion come to me in a disclosure made under the law?

Do I know the name of the other person or the whereabouts of any laundered property from the disclosure; or

Can I identify the other person or the whereabouts of any laundered property from information or other matter contained in the disclosure; or

Do I believe, or is it reasonable for me to believe, that the information or other matter contained in the disclosure will or may assist in identifying the other person or the whereabouts of any laundered property?

Does the professional privileged circumstances exemption apply?

Is consent required?

G. STEPS TO BE TAKEN EVEN IF A REPORT HAS NOT BEEN SUBMITTED TO MOKAS

1. The firm should document decisions related to investigations of unusual activity.
2. Records should be maintained as required by law, **for at least five years** from the date when the firm's relationship with the client was terminated or a transaction was completed. If an ongoing investigation is occurring, relevant CDD records should not be destroyed merely because the record retention period has expired.
3. The firm should determine the actual risk presented by a customer and take appropriate measures to mitigate the risk.
4. The firm should have sufficient controls and monitoring systems for the timely detection and reporting of potentially suspicious activity and large transaction reporting.
5. The firm should perform proper due diligence and employees should monitor the activity that may be inconsistent with a customer's source of income or regular business activities.
6. A firm's system for identifying, monitoring and reporting suspicious activity should be risk-based by directing additional resources at those areas the obliged entity has identified as higher risk such as the firm's size, the nature of its business, its location, the frequency and size of transactions and the types and geographical location of its customers.

H. REPORTING SUSPICIOUS MATTERS / ICPAC CIRCULARS / MOKAS GUIDANCE

It is the employee's responsibility to decide whether to submit an internal report, i.e. to report the incidence to its AMLCO. At the same time, it is the AMLCO's

responsibility to decide whether the information reported internally needs to be reported to the local FIU (see Sections F and G).

MOKAS implemented a procedure which is based on a sophisticated IT system, namely the "go AML Professional Edition (PE)", which requires the reporting entities to submit SARs and STRs online via the MOKAS secured systems. The main objective is to automate the analysis and investigation procedure of MOKAS. This process assists MOKAS to enhance its capabilities with better use of available information and automatic recognition of relationship between data, information and suspects. It also enhances the cooperation with the foreign FIUs, Law Enforcement Agencies, as well as with reporting entities. As a result of this, amongst others, the reporting entities should submit online the SARs/STRs, under the highest security standards.

To assist with the submission of SARs and STRs, MOKAS has issued **guidelines to all obliged entities for submitting reports**. The guidance gives a detailed description of the necessary information that needs to be collected once a decision to submit a report is made by the AMLCO so as to improve the cooperation between MOKAS and the obliged entities, as well as enhance the quality of reports submitted.

Guidance on the process of registration and reporting submission through the goAML system has been circulated by ICPAC through circular **GC 11/2015**.

I. PROTECTION

Under the AML Law, protection exists for persons submitting suspicious reports.

As per *article 69A of the Law*, disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

Additional provision is stipulated in *article 69B of the Law* where a person is protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions once that person has submitted an internal or external report to MOKAS.

Members have the right, as per paragraph 9.1.6 of the Directive, to file a complaint with ICPAC, in cases where they are exposed to threats or hostile action or adverse or discriminatory employment actions due to the fact that they submitted STR or SAR.

J. "TIPPING OFF"

A 'tipping off' offence occurs when any person discloses, either to the person who is the subject of a suspicion or any third party, that:

a) information or documentation on ML/TF has been transmitted to MOKAS;

b) a SAR/STR has been submitted internally or to MOKAS;

c) authorities are carrying out an investigation/search into allegations of ML/TF;

and such disclosures may likely prejudice the subsequent investigations – AML Directive, paragraph 1.5.3 and article 48 of the AML Law.

Tipping-off may also occur in those cases when an employee approaches the client to collect information about the internal on-going investigation, and through the intense questioning, the client becomes aware of the investigation.

The prohibition on disclosure of such information does not prevent disclosure between:

a) credit and financial institutions located in a member-state and belong to the same group or between those institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries comply with the group-wide policies and the procedures – *article 49(1) of the AML Law*.

b) persons who carry out professional auditing activities, or external accounting activities, tax advisors and independent legal counsellors or entities from third countries which impose requirements equivalent to those imposed by the EU Directive, and which carry out their professional activities, under any form of cooperation or engagement, within the same legal person or the wider structure to which the person belongs and which shares common ownership, management or compliance control – *article 49(2) of the AML Law*.

c) relevant obliged entities, provided they are from a member state or from a third country which imposes requirements equivalent to those laid down in the EU

Directive and that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection (*provided that* the case relates to the same client and the same transaction, involving two or more obliged entities) control – *article 49(3) of the AML Law*.

Other than the risk of prejudicing an investigation, the prohibition of disclosure of such information is necessary to also protect the identity of the staff involved and the reporting entity.

K. PENALTIES IN CASE OF FAILING TO REPORT / ASSISTING / FAILURE TO COMPLY WITH THE LAW AND DIRECTIVES / TIPPING-OFF

(a) Failing to report

Under *article 27 of the Law*, an offence is committed if a person does not disclose the information of suspicion to MOKAS. Failing to report is punishable by imprisonment not exceeding 2 years or by a financial penalty not exceeding €5.000 or both penalties.

(b) Assisting a person involved in the commission of a predicate offence[6]

As per *article 4 of the Law*, assisting in any way a person involved in the commission of a predicate offence, commits him/herself an offence punishable by 14 years imprisonment or by a financial penalty up to €500.000 or by both.

(c) Failing to comply with the provisions of the Law and the Directives issued by the Competent Authority

[6] Definitions found in Appendix 1

Per *article 59(6) of the Law*, the Supervisory Authority may impose various administrative sanctions and measures, the most important of which are as follows:

a) A public statement which identifies the natural or legal person and the nature of the breach.

b) To amend or suspend or withdraw the operating license of the supervised natural or legal person.

c) An order requiring the natural or legal person to cease the conduct and to desist from repetition of the conduct.

d) A temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities.

e) Maximum administrative fine of EUR 1.000.000

f) Maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined and €1.000 for each day thereafter that the breach continues.

(d) Tipping-off

According to *article 48(3) of the Law*, "Tipping Off" is a criminal offence and is punishable on conviction by a maximum of two years imprisonment or a fine not exceeding €50.000 or both penalties.

L. ICPAC CASE STUDIES: GENERAL CIRCULAR 10/2018, ISSUED IN MAY 2018

Within the framework of awareness and education, ICPAC has issued a case study pack on fighting ML/TF and Economic Crime. This was done in an attempt to raise awareness of the risks arising from the nature of activities of clients, the nature of

transactions undertaken on behalf of clients and the business activity in general associated with an international financial service centre.

The case study pack provides practical examples on how to follow the money trail, identifying red flags and understanding clients' business is an effective way of detecting the activities of fraudsters, money launderers and other organized crime networks.

M. MOKAS CONTACT DETAILS AND QUERIES

For a more effective and efficient cooperation between the obliged entities and the Unit, it is advised to follow the **guidelines** issued by MOKAS to all obliged entities for submitting reports.

Once an STR / SAR is submitted, MOKAS will contact the reporting entity through the message board of the system. Filing of a report should not be used as a means of communication with MOKAS for the purpose of obtaining advice on the treatment of specific cases. The purpose of submitting any report is to disclosure information related to suspicious transactions and/or activities to the relevant authority.

MOKAS may also make follow-up inquiries to the reporting entities to clarify or request additional information shortly after the submission of a report. Any information held by the reporting entity must be made available to MOKAS if requested and could be vital in the progress of the investigation.

Contact details:

P. O. Box 23768, 1686 Nicosia
Tel: + 357 22 446 018
fax: + 357 22 317063
e-mail: mokas@mokas.law.gov.cy

APPENDIX I - DEFINITIONS

Obliged Entities

a. Credit institution;
b. Financial institution;
c. Any of the following natural or legal persons in the exercise of their professional activities:

i. auditors, external accountants, and tax advisors, and any other person that undertakes to provide, either directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity;

ii. Independent legal professional, when it participates, whether acting on behalf of a client in a financial or real estate transaction, or by assisting in the planning or carrying out of a transaction for its client concerning the-

- buying and selling of real property or business entities;
- managing of client money, securities or other assets;
- opening or management of bank, savings or securities accounts;
- organisation of contributions necessary for the creation, operation and management of companies;
- creation, operation or management of trusts, companies, foundations or similar structures

d. Natural or legal person not already covered under paragraph (c) offering the following services to trusts or companies:

i. the formation of companies or other legal persons;

ii. 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;

iii. providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;

iv. acting as, or arranging for another person to act as, a trustee or a trustee of express trusts or a similar legal arrangement;

v. holding the shareholding capital of corporate entities and registering such shareholder in the respective registers of registered shareholders on behalf of or on account of third parties, other than a company listed on a regulated market that is subject to disclosure requirements in accordance with European Union law or subject to equivalent international standards, or ensures that other person exercises respective duties; and

vi. any of the services or activities specified in section 4 of the Regulation of Administrative Service Providers and Related Issues Law.

e. estate agents including when acting as intermediaries in the letting of immovable property, but only in relation to transactions for which the monthly rent amounts to EUR 10 000 (€10.000) or more;
f. providers of gambling services, as provided in the relevant laws of the Republic·
g. casino, which falls under the scope of the Law Regulating the operation and Supervision of casino;
h. a person trading in goods, if the payment is made or collected in cash and it concerns an amount equal to or greater than ten thousand euro (€10.000), regardless of whether the transaction is carried out in a single operation or in several operations which appear to be linked;
i. Crypto Asset Service Providers, who are registered with the register provisioned as per section 61E (1) of the AML Law;
j. persons, whose supervision is assigned to CySEC under the provisions of the Cyprus Securities and Exchange Commission or any other law;
k. persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to ten thousand Euro (€10.000) or more.
l. persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to ten thousand Euro (€10.000) or more.

Predicate Offence

Predicate offence is defined under article 5 of the AML law as '*any offence defined as a criminal offence under Cyprus Law*'.

In general, it is considered to be an offence that is part of a larger criminal offense or scheme.

A number of non-exhaustive categories of criminal offences is provided by the FATF that could be covered as predicate offences:

- participation in an organised criminal group and racketeering;

- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling; (including in relation to customs and excise duties and taxes);
- tax crimes (related to direct taxes and indirect taxes);
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

APPENDIX II - USEFUL LINKS

GC_11/2015: Submission of reports to MOKAS

GC_8/2016: Sanctions and Restrictive Measures

Directive for compliance with the provisions of un security council resolutions (sanctions) and the decisions/regulations of the council of the European union (restrictive measures).

AML Guidance on establishing Source of Wealth and Source of Funds

Case Studies on fighting Money Laundering, Terrorist Financing and Economic Crime

CC_31/2022: Notification of AMLCO to MOKAS

ICPAC's Directive on the Prevention and Suppression of Money Laundering Activities

Guidelines issued by MOKAS to all obliged entities for submitting reports

Specialized Technical Material on Anti-Money Laundering

MOKAS official web

GoAML Login