AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Guideline:

Suspicious Transaction Report

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

I. Purpose and Scope

The purpose of this guideline is to assist financial institutions (FIs) and designated non-financial business and professions (DNFBPs) in Monaco, together referred to as "reporting entities", in understanding and complying with their obligations relating to the reporting of suspicious transactions under the AML/CFT Law 1.362 as amended, and Sovereign Ordonnance 2.318 as amended. The guideline sets out the expectations of the AMSF Financial Intelligence Unit (hereafter the "FIU") regarding indicators that reporting entities should take into account and the measures that they should take in the context of suspicious transaction reports (STRs).

This guideline does not intend to replace the AMSF "Generic AML/CFT Guidelines for Monegasque Businesses" (2021) but rather to complement it by raising further awareness and understanding of reporting obligations and by providing specific indicators for reporting as applicable across sectors and on a sector-by-sector basis (see Annex to the Guidance). For comprehensive guidance on overall AML/CFT obligations in Monaco, entities should continue to refer to the Generic Guidelines.

The measures and indicators described in this guideline are not exhaustive and this guideline does not set limitations on the steps to be taken by reporting entities in order to meet their legal and regulatory obligations. In devising internal processes, establishing indicators, and taking decisions to file STRs, reporting entities should consider any other factors and indicators and take any other measures as appropriate to their business.

II. Applicable legal and regulatory framework[1]

The relevant legal provisions relating to the reporting of suspicious transactions are set out in Chapter V of the Law 1.362 as amended on countering ML, TF and corruption ("**the AML/CFT Law**"):

- **Article 36** sets out the fundamental principles of the reporting obligation, determining in particular that all reporting entities, with the exception of lawyers (having a distinction legal regime, as described further below), , must report **confidentially** and **without delay** to the FIU all transactions or attempted transactions involving sums or funds that they know or suspect to be derived from a money laundering, terrorist financing or corruption offence, before the transaction is executed**.**
- **Article 36-1** specifies that auditors, accountants, fiscal and legal advisors are not bound to reporting obligations when they assess the legal situation of their client, when providing legal advice.
- **Article 37 § 1** asserts that as soon as the report is received, the FIU shall acknowledge receipt, unless the reporting person has expressly indicated not being willing to have it.
- **Articles 37 and 38** regulate the possibility for the FIU to postpone the execution of any transaction on behalf of the client concerned by the declaration.
- **Article 39** describes that, the suspicious transaction report may be transmitted after the transaction has been carried out in two cases :
  - either postponement of the execution of the operation is not possible ;
  - either postponing execution of the operation would be likely to prevent prosecution of the beneficiaries of the offence of ML/TF.

  In these cases, the declaration must indicate the reason why the declaration was not sent before the transaction happened, and must be sent without delay.
- **Article 40** sets the reporting obligation for lawyers, who are required to inform the "Conseil de l'Ordre des avocats-défenseurs et avocats" (who forwards the declaration to the FIU upon determination that no legal conditions apply that would avoid to do so without delay). The article further specifies a limited number of exemptions for lawyers, bailiffs and notaries, in line with the FATF Standards. .
- **Articles 41 and 42** regulate reporting obligations in the case of transactions linked to non-cooperative jurisdictions or to entities subject to asset freezing sanctions. The report must be transmitted **automatically**, which means, regardless of whether the reporting entity suspects, has reasonable grounds to suspect or knows that a transaction involves funds linked to a TF/PF offence.
- **Article 43** determines that STRs shall be submitted by the person within the entity who is responsible for AML/CFT matters.
- **Article 44** sets out the causes of non-liability of reporting entities.
- **Article 45** provides derogations of the principle of confidentiality of STRs to permit information-sharing on STRs between certain entities in specific and limited cases.

[1] This overview is a summary of the legal framework for information, intended to help reporting entities understand the nature and scope of their legal and regulatory obligations, and to direct them to the texts where they can find a full description of these obligations. This summary does not replace or supersede any legal or regulatory requirements. In the event of any discrepancy between the guideline and the law or ordinance relating to the fight against money laundering and terrorist financing, the latter shall prevail.

The Sovereign Order 2.318 as amended laying down the conditions for application of the AML/CFT Law further contains the following provisions on reporting:

- **Article 36-2-1** determines that FIU shall determine the method of transmission of STRs for all reporting entities except for lawyers, which shall be indicated on the AMSF website. Any declaration or information transmitted by any other means is reputed not to have been communicated to the FIU, with the exception of suspicious reports sent to the FIU pursuant to paragraph 1 of Article 37 of Law 1.362 as amended.
- **Article 38-2** determines that lawyers submit their STRs to the "Conseil de l'Ordre des avocats-défenseurs et avocats" by registered letter with request for an acknowledgement of receipt or by depositing the STR at the Secretariat of the "Conseil de l'Ordre des avocats-défenseurs et avocats" in return for a receipt.

III. The importance of reporting suspicious transactions

STRs play a pivotal role in the fight against money laundering (ML), associated predicate offences, terrorist financing (TF), and corruption. Information provided in STRs assist Monegasque Law Enforcement Authorities in their investigations, resulting in the disruption of criminal and terrorist activities. STRs also provide authorities with valuable market intelligence on trends and typologies in ML/TF methods, including new and emerging risks.

IV. Meaning of suspicious operations

Pursuant to the Monegasque legal framework in place, there are **three types of suspicious operations** that must be reported:

1. Suspicious operations
2. Operations or facts concerning persons linked to so-called "non-cooperative jurisdictions[2]"
3. Operations or facts concerning persons subject to international financial sanctions

Type 1. Suspicious operations

As defined in **article 36 of Law 1.362** as amended, a suspicious operation refers to any transaction, attempted transaction involving sums or funds which a reporting entity knows, suspects, or has reasonable grounds to suspect as being in whole or in part, **related to money laundering, terrorist financing or corruption**, e.g. by:

- Being the proceeds of crime or misdemeanour (these include all offenses punishable in the Principality by a prison sentence of more than one year, as well as other offences listed exhaustively in article 218-3 of the Criminal Code);
- Being intended to be used in an activity related to such crimes.

Reporting entities should note that there is **no minimum monetary threshold** for reporting and no amount should be considered too low for suspicion. This is particularly important when considering potential terrorist financing transactions which often involve very small amounts of money.

Reporting entities should also note that **transactions need not be completed**, in progress or pending completion in order to be considered as suspicious. Attempted transactions, transactions cancelled by the customer, transactions that are not executed and past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must also be reported in accordance with the relevant requirements.

Furthermore, reporting entities should ensure to always apply the right order of actions when identifying suspicions. It is unacceptable for example for a bank in case of suspicions to close accounts and remit funds back to the customers on their own initiative and prior to submitting STRs, thereby making it impossible for the FIU to exercise their right to postpone the transaction. We draw your attention to the specific case of Terrorist Financing, in which the account must never be closed, and the suspicious transaction report must be sent to the AMSF without delay.

[2] As determined in Arrêtés Ministériels n°2018-926 and n°2018-927 dated September 28, 2018.

Type 2. Non-cooperative jurisdictions

As defined in **article 41 of Law 1.362** as amended, every operation or fact concerning natural or legal person linked to a non-cooperative jurisdiction must be reported **automatically**, that means immediately.

The decision to appoint a country as non-cooperative jurisdiction is taken by the **Financial Action Task Force (FATF)** and endorsed by Ministerial Order in Monaco (see footnote 2). The list of "non-cooperative countries" can be consulted on the AMSF's website, but only Monaco's "Journal Officiel" prevails.
A person is considered to be linked to such jurisdiction whenever they are **resident, registered or established** in that jurisdiction.

This applies to **all counterparties** of operations, e.g. existing customers as well as potential customers, beneficial owners, or intermediaries or persons acting on behalf of customers.

Again, there is no minimum monetary threshold for reporting, and attempted transactions involving persons linked to non-cooperative jurisdictions should be reported as well.

Type 3. Persons under targeted financial sanctions

As defined in **article 42 of Law 1.362** as amended, any operation or fact concerning natural or legal persons targeted by asset freezing measures under international targeted financial sanctions should also be reported **automatically**, that means immediately.

The reporting entity should ensure that the relevant funds and economic resources are **frozen without delay** and without prior notice to the persons involved. Where links to sanctioned persons are established, reporting entities should further **immediately** freeze their assets and economic resources, and any transaction that the sanctioned person intended to execute should be blocked to avoid any movement, transfer, modification, use or manipulation of funds.
This applies to **all counterparties** of operations, e.g. existing customers as well as potential customers, beneficial owners, or intermediaries or persons acting on behalf of customers, as well as to entities fully or partially owned or controlled by persons subject to sanctions.

The reporting entities should also report all relevant information concerning this fact/operation to the **Budget and Treasury Department**.

Further detailed information on reporting obligations related to targeted financial sanctions is contained in the Generic Guidelines (refer to p. 75-76).

V. Timing of suspicious transaction reports

As a matter of principle, under the AML/CFT legal and regulatory framework of Monaco, all reporting entities are obliged to report STRs to the FIU (or, in the case of lawyers, to the "Conseil de l'Ordre des avocats-défenseurs et avocats"), **before the transaction is executed, in accordance with article 36 of the Law 1.362** as amended. In the STR, the reporting entity should indicate the deadline by which the transaction must be executed.

By exception, the STRs may be transmitted after the transaction has been carried out in two cases, in accordance with article 39 of the Law 1.362, as amended:

- either postponement of the execution of the operation is not possible ;
- either postponing execution of the operation would be likely to prevent prosecution of the recipient of the offence of AML/CFT.

In both aforementioned cases, STRs must include a justification as to why the declaration was not sent before the transaction, and must be sent without delay. With the exception of these last 2 cases, the law does not grant the reporting entity the right to file a suspicious transaction report after the transaction happened. Thus, submitting an STR following the execution of a transaction remains a strictly exceptional case and duly justified.

In all cases, the **immediate filing** of an STR to the FIU (or the "Conseil de l'Ordre des avocats-défenseurs et avocats") is one of the key elements of the AML/CFT process. Suspicions must be reported **without delay** to the FIU (or to the "Conseil de l'Ordre des avocats-défenseurs et avocats") when they know, suspect or have good reason to suspect that transactions or attempted transactions involve sums or funds that originate from an ML/CFT offence (Type 1), or are linked to non-cooperative jurisdictions (Type 2) or sanctioned persons (Type 3).

The same applies to cases where a transaction meeting at least one of the conditions set out in article 14 of Law 1.362 as amended gives rise to a special examination which does not remove any doubt about the transaction and which degenerates into suspicion. Investigations into potentially suspicious transactions must be completed rapidly once they have been identified. Reporting entities must submit an initial suspicious transaction report, followed by a supplementary report.

Anyway, all Information that is collected by the reporting entity after the STR has been filed and which may change the scope of the report should be communicated to the FIU (or to the "Conseil de l'Ordre des avocats-défenseurs et avocats") **without delay**. This refers to any element likely to invalidate, confirm or

modify the content of the STR. Failure to submit a complementary STR is equivalent to a failure to submit an STR.
Furthermore, when filing an STR, reporting entities must indicate the date that the (request for the) transaction or other form of interaction with the customer took place, the date that unusual or potentially suspicious activity was identified.

In practice, the obligation to report an STR **prior** to execution of a transaction is crucial especially where the execution of the transaction may lead to funds or assets disappearing. This will generally be the case for example for outgoing transactions of funds held by the reporting entity for the customer. In particular, where the customer seeks to send funds abroad, the FIU will not be able to oppose the transaction, and the Monegasque law enforcement authorities will not be able to seize and confiscate the proceeds of crime or other funds linked to money laundering and terrorist financing. Also, where there are multiple and different suspicion indicators in conjunction with large amounts of money involved in the transaction, there is a high risk that a reporting entity helps to facilitate large-scale money laundering or other criminal activities if they go ahead with the transaction.

VI. The postponement of a transaction by the FIU

The suspicious report must be made before the operation happens, without delay, so as not to deprive the FIU of the right to oppose the planned operation.

Indeed, if the FIU deems it necessary, it may oppose the execution of the transaction, before the expiry of this period, as well as any other operation on behalf of the customer subject to the STR, for a maximum period of 5 working days in order to carry out additional analyses. A judicial extension of this period is possible.

This right of opposition may be exercised during the period in which the operation is to be carried out. Objections are communicated in writing or by appropriate electronic means. If no objection is notified, the reporting entity is free to carry out the transaction (unless asset freezing measures apply as indicated above). The term "free" means that the reporting entity is authorized to carry out the transaction within the meaning of Law 1.362 as amended. Nevertheless, it still remains responsible for the legality of the transaction.

VII. Identification of suspicious transactions

The suspicious nature of a transaction may be deduced from **a plurality of indicators, patterns of behaviour or information relating to customer due diligence.** It does not depend on obtaining evidence that an offence has actually taken place or proof of the illicit source of the proceeds concerned. Reporting entities are not required to have knowledge of the underlying criminal or delictual activity or to have reasonable grounds for suspecting that the proceeds originate from criminal and delictual activity. Reasonable grounds for suspicion are sufficient to trigger reporting obligations.

For further clarity, these three concepts should be understood as follows:

1. Knowledge – it is an objective criterion, either a person knows something or does not. If the MLRO or any other employee of the reporting entity if aware or detains information indicating that any of the aforementioned criminal activity may, is or will be taking place, the MLRO should immediately file an STR with the FIU (or, for lawyers, with the "Conseil de l'Ordre des avocats-défenseurs et des avocats").

2. Suspicion – is more subjective than knowledge. In order to ascertain a suspicion, the MLRO must take into account the varying circumstances. In order to guide entities, indicators can be consulted on the AMSF website.

A transaction that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So, the unusual is, in the first instance, only a basis for further enquiry that may in turn require judgment as to whether it is suspicious.

3. Reasonable Grounds to Suspect – the requirement to file an STR goes beyond "suspicion" and also includes the obligation to report when "reasonable grounds to suspect" exist. This implies that a further obligation to report arises where, on the basis of objective facts or circumstances, a reasonable person would have inferred knowledge or formed the suspicion that ML/FT existed or that funds were the proceeds of criminal activity.

When making a determination of suspicion, reporting entities should consider their specific products, and services and the customers in the context of their **risk profile**, as what might be considered suspicious for one product, service or customer may not be for another. For this reason, clear internal policies and procedures including alert escalation and investigation, and internal suspicious transaction reporting are critical to an effective ML/TF risk-mitigation programme. This includes an adequate training program that will allow staff to detect possible unusual or suspicious transactions.

It is essential to formalize the steps taken. The same applies to unsuccessful searches or diligence. Reporting entities must be able to justify that their searches have been carried out even when no results have been obtained (formalizing the search may, for example, take the form of a dated screen capture). This formalization therefore constitutes protection for the reporting entities, enabling them to demonstrate that each step of the procedure has been fully completed. This written record is the only means of proving that the reporting entity has complied with its obligations.

Reporting entities should note that the presence of an **indicator or red flag** may not always mean that a transaction is suspicious, however, it does require that a transaction is immediately assessed to determine whether the transaction needs to be reported to the FIU (or the "Conseil de l'Ordre des avocats-défenseurs ou avocats"). The investigations needs to cover customer's earlier and related transactions.

Special examinations carried out in accordance **with article 14 of Law 1.362, as amended, are an important means of identifying a suspicious transaction if any of the following criteria are present:**

- the transaction is complex;
- the amount of the transaction is abnormally high;
- it follows an unusual pattern;
- it has no apparent economic or lawful purpose;
- transactions involving a counterparty with links to high-risk jurisdictions or territories.

To determine whether a high-risk jurisdiction is involved in a business relationship or transaction, reporting entities should apply Monaco's official list of states or territories with strategic deficiencies in their AML/CFT systems. This list is maintained by Monaco at the national level and published in the "Journal Officiel" by Ministerial Order. Updates are also communicated on the AMSF website. The list is based on the FATF's list of jurisdictions under increased monitoring (the so-called "grey list") as well as the EU's list of high-risk third countries.

The importance of an effective monitoring system to detect unusual transactions

To be able to detect and report suspicious transactions when they occur, it is crucial that reporting entities have an effective transaction monitoring system in place, tailored to the nature, size and risk exposure of their business, client base and operations.

An effective transaction monitoring system should allow the entity to detect any **unusual transactions**. When an unusual transaction is identified, this should lead to a **Special Examination** by the entity in order to determine whether it gives rises to suspicions to be reported.

The required features of the transaction monitoring system are listed in article 28 of the Sovereign Ordinance 2.318, as amended. The AMSF Generic Guidelines (part 2 - section 2.3.1) elaborate on transaction monitoring and special examinations of unusual transactions (part 2 – section 2.3.1.1).

Links with non-cooperative jurisdictions are generally established on the basis of CDD information collected by reporting entities regarding the residences, registered addresses and place of incorporation of customers, beneficial owners, customer representatives, counterparties in transactions and generally any person connected with the customer. Therefore, in order to comply with the reporting obligations, it is important that reporting entities adequately collect and assess information on the **geographical components of business relationships and transactions.**

As for links to sanctioned persons, they are established based on **continuous** sanctions screening that is to be carried out by the reporting entity on all counterparties involved in new and existing business relationships and transactions. The reporting entity can use a specialised automated monitoring tool for this purpose and must ensure that any updates to the sanctions lists are incorporated immediately into the internal screening system. Contrary to transaction monitoring in order to identify any potential ML/TF suspicions, the requirement of **compliance with sanctions cannot be fulfilled on a risk basis**. An entity must at all times be able to detect whether any of its counterparties are subject to sanctions.

As part of their overall AML/CFT framework, reporting entities should determine the **internal policies, procedures and controls** they apply in connection with the identification and evaluation of potentially suspicious transactions (see next section). This includes an adequate process and dedicated **experienced employees** for the investigation of and dealing with alerts. The investigation of alerts and the conclusion of the investigation should be **documented**, including the decision to close the alert or to immediately report the transaction as suspicious.

VIII. Internal procedures for the reporting of suspicious transactions

As part of their overall risk-based AML/CFT framework, and commensurate with the nature and size of their businesses, reporting entities should establish clear and appropriate policies, procedures and internal controls (including staff training programmes) pertaining to the identification, investigation and suspicious reports (including attempted transactions) in accordance with all the obligations imposed by Law 1.362, as amended. These procedures must be documented, approved by senior management, and communicated to all employees. The internal reporting procedures should also include information on the procedures employees of the subject person are to follow when the MLRO is absent from duties.

With regard to internal procedures, they should determine the degree and extent of appropriate investigations. AML/CFT compliance monitoring procedures should be in place and should cover the provision by front-line staff of the necessary records and data to the designated AML/CFT compliance officer for further analysis and reporting decisions. These procedures have to clearly set out the steps to be followed when an employee of the subject person becomes aware of any information or matter that in his opinion gives rise to knowledge or suspicion that a person or a transaction is connected to ML/FT. These policies and procedures should include operational guidance on the core systems used for case management and notifications, as well as secure information flows. Training on reporting obligations should be provided to all staff. This advice and training are particularly important for front-line staff who are in contact with customers. It is essential that these employees know when there may be cases of suspicious transactions, what questions they should ask the customer and what information they should never disclose to the customer, particularly when there is a delay in the transaction, and how to manage the relationship without putting the customer on the spot.

The decision to file or not to file an STR must always be taken by the MLRO's/designated employee's and should not be subject to the direction or approval of other parties within the subject person. This is not to say that a determination on whether an internal report gives rise to knowledge or suspicion of ML/FT shall always be made by the MLRO or the designated employee and may not be delegated by the MLRO to other employees under his/her supervision, or that the MLRO cannot seek assistance, including from internal staff of the subject person or external advisors. Where the MLRO seeks the assistance of other internal members of staff or external advisors, due consideration ought to be given to the sensitivity and confidentiality of information that may be disclosed and the non-disclosure obligations that subject persons have to adhere to.

The relevant policies, procedures and controls should take into consideration such factors as:

- Roles and responsibilities of the organisation in implementing and reviewing/updating relevant indicators for unusual and suspicious transactions;
- The organisation's roles and responsibilities for conducting and evaluating special examinations that may give rise to suspicion;
- Operational and IT systems procedures and controls in relation to the application of relevant indicators to process such as transaction processing and monitoring, customer due diligence and review, and alert escalation;
- Employee training on special reviews, the identification and reporting of suspicious transactions (including attempted transactions), the appropriate use and evaluation of relevant indicators, the degree and extent of appropriate internal investigation, and the management of the customer relationship in the event of transaction delays due to internal investigations and/or the filing of STRs;
- Operational procedures for the monitoring and follow-up of transactions;
- Requirements relating to the content and format of potentially suspicious internal transactions;
- Appropriate controls for ensuring confidentiality and the protection of data from unauthorized access;
- Policies and procedures for the analysis and decision-making around suspicious transactions by the AML/CFT responsible person in regard to reporting to the FIU (or the "Conseil de l'Ordre des avocats-défenseurs et avocats");
- Procedures related to the provision of additional information, follow-up actions pertaining to the transactions, and the handling of Business Relationships after the filing of STRs;
- Other provisions deemed appropriate by the AML/CFT responsible person.

IX. Form and content of suspicious transaction reports

In all cases, the STR must contain the facts that constitute the suspicion on which the professional relies, and the deadline by which the transaction must be completed, if applicable, in accordance with article 36 of the Law 1.362, as amended.

In addition, STRs should include all relevant information, documents and records relating to the customer, as well as to the operations, accounts concerned and counterparties, if applicable. To fulfill these obligations, reporting entities should implement adequate internal policies, procedures and controls in relation to the identification and the immediate reporting of suspicious transactions as outlined in Section 8.

Reporting entities are advised to include references to the applicable indicators when they describe the facts and reasons for filing an STR (see Section 16 & Annex of this Guideline).
In accordance with article 36-2-1 of Sovereign Ordinance 2.318, as amended, the method of transmission of STR is indicated on the AMSF website and established by the department exercising the financial intelligence function. **Since January 1, 2024, goAML became the sole means of transmitting STR**. If a report is transmitted by any means other than the goAML solution (or not in the good way in goAML), it is deemed not to have been transmitted to the FIU. Transmitting a STR by any other means, with the exception of goAML, is equivalent to failing to report a STR, with the exception of suspicious reports sent to the FIU pursuant to paragraph 1 of Article 37 of Law 1.362 as amended. A goAML user manual is available on the AMSF website. The steps of the registration process are detailed. The STR is considered as transmitted by the reporting entity to the FIU when the reporting entity receives the official notification from the FIU that the STR has been accepted.

In accordance with article 38-2 of Sovereign Ordinance 2.318, as amended, lawyers must transmit their suspicious transaction reports to the "Conseil de l'Ordre des avocats-défenseurs et avocats", without delay, by registered letter with acknowledgement of receipt or by delivery to the Secretariat of the "Conseil de l'Ordre des avocats-défenseurs et avocats" against receipt.

Lawyers must mention all relevant information relating to the transaction, the client or the account. This includes but is not limited to :

- reason for filing an STR (type 1, type 2, type 3 - section 4)
- information on whether the transaction concerned has been carried out:
  - if not, information on the period during which the transaction is to be carried out;
  - if so, and only in accordance with the conditions set out in article 39 of the Law 1.362, as amended, the reason why the STR is being filed after the transaction has been carried out and the date on which the transaction or other interaction with the customer took place.
- date on which the suspicion arose;
- information on the persons involved in the report, including, but not limited to, the identification details of natural persons, the registration details of legal persons or legal arrangements, and the identification details of natural persons involved in the legal person (shareholders, beneficial owners, representatives, etc.) or legal arrangement (BO, trustee, etc.). In the specific case where the suspicion relates to a transaction, the lawyer must ensure that all information relating to the suspicious transaction is provided (IBAN, identification of the counterparty, bank details, etc.).
- description of the facts and results of the internal investigations.

Lawyers are also asked to provide any relevant documentation and records to support the information should be annexed to the report.

X. Prohibition against "Tipping off"

When reporting suspicious transactions to the FIU (or the "Conseil de l'Ordre des avocats-défenseurs et avocats") reporting entities are obliged to maintain confidentiality with regard to both the existence, content and follow-up of a suspicious transaction report and must ensure that the information and data reported are protected from access by any unauthorized person.

As a matter of principle, the exchange of information between professionals is not permitted in STR.

The exchange of information is only permitted between entities in the same profession under certain conditions, in accordance with article 45 of the Law 1.362, as amended. It concerns only the list below:

- by way of exception, credit institutions, insurance companies and insurance intermediaries, insofar that they belong to the same group, may inform each other of the existence and content of a declaration, under certain conditions.
- by way of exception, auditors, tax consultants, legal advisors and chartered accountants, insofar they belong to the same professional structure, of the existence and content of a declaration, under certain conditions.
- by way of exception, credit institutions, insurance companies, insurance intermediaries, auditors, tax consultants, legal advisors, chartered accountants, notaries, lawyers and bailiffs, when acting on behalf of the same customer and in the same transaction, or when they have knowledge, for the same customer, of the same transaction, may inform each other.

It is acknowledged that it can be challenging for reporting entities to manage the customer relationship while a transaction is delayed due to the filing of an STR or an opposition of the FIU.

Therefore, as mentioned in point 8 of these guidelines, it is essential that procedures and training courses provide detailed and practical information on how confidentiality is to be managed by the all team, particularly by the front office.
In any cases, it is an offence for reporting entities or their managers, employees or representatives, to inform a customer, beneficial owner or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction.

XI. Protection against liability for reporting entities

The liability of reporting entities is protected in whole or in part by Law 1.362, as amended as follows:

- cause of criminal irresponsibility: in accordance with article 44, paragraph 1, of Law 1.362, as amended, a person who makes a declaration in good faith may not be prosecuted for slanderous denunciation (article 307 CP) or violation of professional secrecy (article 308 CP),
- cause of civil and disciplinary irresponsibility: in accordance with article 44, paragraph 2 of Law 1.362, as amended, a person who makes a declaration in good faith may not be subject to
  - a civil liability action;
  - a professional sanction or prejudicial or discriminatory measure in the field of employment against himself, his directors or authorized agents.

The aforementioned grounds for non-liability are applicable even:

- when the person who filed the report did not have accurate knowledge of the facts that were the subject of the report;
- when the activity or transaction that is the subject of the suspicious transaction report has not taken place; and
- when the facts giving rise to the report have not been proven to be criminal in nature or when these facts have been dismissed, relaxed or acquitted.

In any case, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

XII. Internal follow-up measures after filing an STR

Following the reporting of a suspicious report to the FIU (or "Conseil de l'Ordre des avocats-défenseurs, et des avocats" in case of lawyers), reporting entities are expected to implement additional measures in relation to the customer and business relationship to mitigate the associated ML/TF risks. Examples of such measures include but are not limited to:

- Review and reassess the business relationship and its risk classification in order to modify the risk profile accordingly;
- Obtain approval from senior management before entering into certain transactions;
- Implement enhanced risk-based continuous monitoring measures;
- Any other reasonable measure, proportionate to the nature and size of the business, bearing in mind the prohibition on informing the customer.

XIII. Record-keeping requirements

Reporting entities are required to retain all records and documents pertaining to STRs and the results of all analysis or investigations performed in the context of suspicions. Such records relate to both internal reports on suspicions and reviews thereof, and STRs filed with FIU (or the "Conseil de l'Ordre des avocats-défenseurs, et des avocats"), and include but are not limited to:

- Suspicious transaction indicator alert sheets, logs, investigations, recommendations and decisions, together with all related correspondence;
- CDD and business relationship monitoring records, documents and information obtained in the course of the analysis or investigation of potentially suspicious transactions, and all related internal or external correspondence or communication records;
- STR records and statistics, as well as the corresponding analyses, recommendations and decisions (including the justification for reporting or non-reporting), and all related correspondence;
- Requests for information from the competent authorities, requests for assistance from the corresponding banks, and the related investigation files and correspondence;
- All documents and information used as part of an internal assessment of a customer following the filing of an STR;
- Notes relating to feedback provided by the authorities in respect of reported STRs, together with notes or records relating to any other action taken by or required by FIU.

In accordance with Article 23 of the Law 1.362 as amended, the record-keeping is 5 years.
By exception, the record-keeping may be extended for a further maximum period of 5 years:

- at the professional out of necessity;
- at the request of the AMSF;
- at the request of the Public Prosecutor, the examining magistrate or judicial police officers acting at the request of the Public Prosecutor or the examining magistrate in the investigation.

XIV. Responding to FIU requests for information

Reporting entities are also obliged to communicate to the AMSF **without undue delay**, all information that is explicitly requested by the FIU in the context of its intelligence activities. It is frequently the case that the FIU sends such requests following the filing of an STR. However, such requests may be sent even in the absence of the reporting entity having filed an STR.

XV. Supervision of compliance with reporting obligations

The AMSF supervisory department (or the "Conseil de l'Ordre des avocats-défenseurs et avocats"), as responsible AML/CFT supervisors in Monaco, supervise the reporting entities' compliance with the AML/CFT law and related regulations, including the provisions on suspicious transaction reporting. In this context, while conducting inspections, the supervisors may request, STRs files, and request further information on examinations and STRs (timing, reasons, roles, etc.).

XVI. Penalties

A reporting entity that contravenes the provisions of the Law is liable to the following penalties:

Penalties for failure to declare:

In accordance with article 71-2 of Law 1.362, as amended, penalties may be imposed on natural or legal persons who:

- knowingly fail to make the suspicious transaction report referred to in article 36 of Law 1.362, as amended (prior report);
- fail to make the suspicious transaction report referred to in article 39 of Law 1.362, as amended (subsequent report);
- fail to file a suspicious transaction report in accordance with Article 39 of Law 1.362, as amended (ex-post report);
- not file a suspicious transaction report in accordance with article 41, paragraph 1 of Law 1.362, as amended ("Non-cooperative countries" report);
- fail to file a suspicious transaction report as referred to in Article 42 of Law 1.362, as amended ("Targeted financial sanctions" report); or "Targeted financial sanctions" report);
- knowingly omit to make the declaration of suspicion referred to in paragraph 1 of article 40 of Law 1.362, as amended (lawyer-defensor, lawyers and trainee lawyers are required to inform the "Conseil de l'Ordre des avocats-défenseurs et avocats" without delay).

Penalties for failure to maintain confidentiality:

Pursuant to article 73 of Law 1.362, as amended, any natural or legal person that fails to comply with the prohibition on disclosing the contents of a suspicious transaction report or the consequences thereof shall be liable to criminal prosecution.

Penalties for failure to Record-keeping

Pursuant to article 71-1 of Law 1.362, as amended, any person referred to in articles 1 and 2 who fail to comply with their obligation to keep the documents and information referred to in article 23 incur a penal sanction.

XVII. Indicators for suspicions

The Annex to this Guideline contains a non-exhaustive list of cross-sectoral and sectoral indicators of suspicious transactions or activities, to enable reporting entities to better understand the facts and situations that might warrant the filing of a suspicious transaction report.

Indicators are points of attention that enable a reporting entity to awaken or detail its suspicions about a given transaction. The AMSF proposes a non-exhaustive list of indicators, which can be consulted on its website.

The reporting entity must develop its own indicators in the light of its activity and risk profile. The simple presence of an indicator does not necessarily constitute grounds for suspicion of BC/FT-P-C, but may prompt closer monitoring and examination. Conversely, a number of indicators may be grounds for suspicion of BC/FT-P-C. Indicators should always be considered in context.

Reporting entities are further expected to keep an eye on new relevant publications that may contain additional indicators, by checking updates on the website of AMSF as well as by checking directly the websites of relevant international and regional bodies, such as the Financial Action Task Force, MONEYVAL and the Egmont Group.

In any case, the presence of a High-Risk jurisdiction should also be considered as an indicator.