AML Tuesday's Session #27 on:

Sector-Specific STR Typologies and Red Flag Scenarios applied in Practice for Financial Institutions

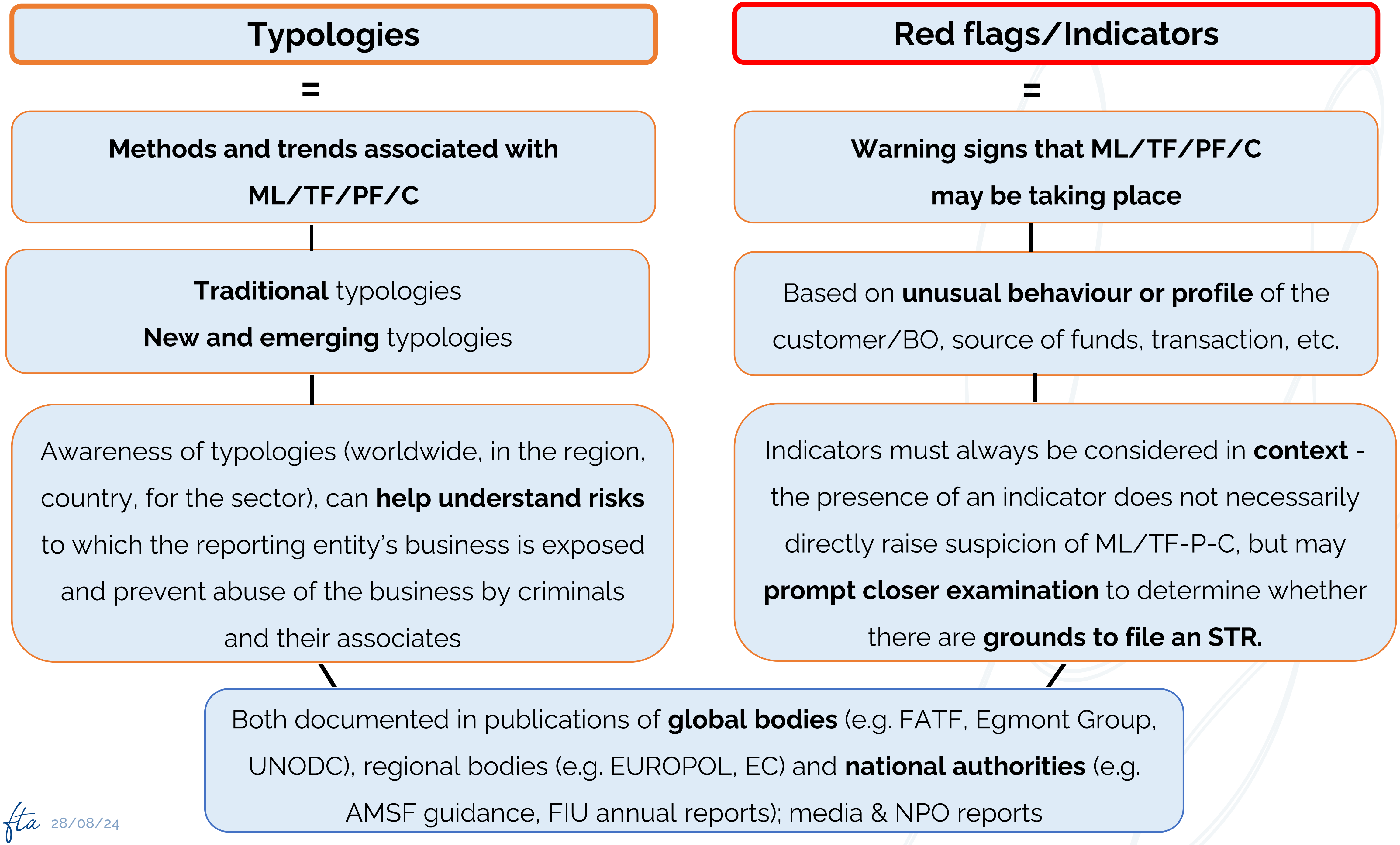
August 27, 2024

Discussion Topics

01 Reporting obligations

02 Typologies, including new and emerging typologies

03 Red flags indicators



Typologies

=

Methods and trends associated with ML/TF/PF/C

Traditional typologies

New and emerging typologies

Awareness of typologies (worldwide, in the region, country, for the sector), can **help understand risks** to which the reporting entity's business is exposed and prevent abuse of the business by criminals and their associates

Red flags/Indicators

=

Warning signs that ML/TF/PF/C may be taking place

Based on **unusual behaviour or profile** of the customer/BO, source of funds, transaction, etc.

Indicators must always be considered in **context** - the presence of an indicator does not necessarily directly raise suspicion of ML/TF-P-C, but may **prompt closer examination** to determine whether there are **grounds to file an STR.**

Both documented in publications of **global bodies** (e.g. FATF, Egmont Group, UNODC), regional bodies (e.g. EUROPOL, EC) and **national authorities** (e.g. AMSF guidance, FIU annual reports); media & NPO reports

01

Reporting obligations

FATF International standards on combating ML and TF

Recommendations 20 & 21 & interpretive note:

- If a financial institution **suspects or has reasonable grounds to suspect** that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to **report promptly** its suspicions to the financial intelligence unit (FIU).
- The reference to **criminal activity** refers to all criminal acts that would constitute a predicate offence for money laundering.
- The reference to **terrorist financing** refers to the financing of terrorist acts and also terrorist organisations or individual terrorists, even in the absence of a link to a specific terrorist act or acts.
- **All suspicious transactions, including attempted transactions**, should be reported regardless of the amount of the transaction.
- Financial institutions, their directors, officers and employees should be **prohibited by law from disclosing ("tipping-off")** the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

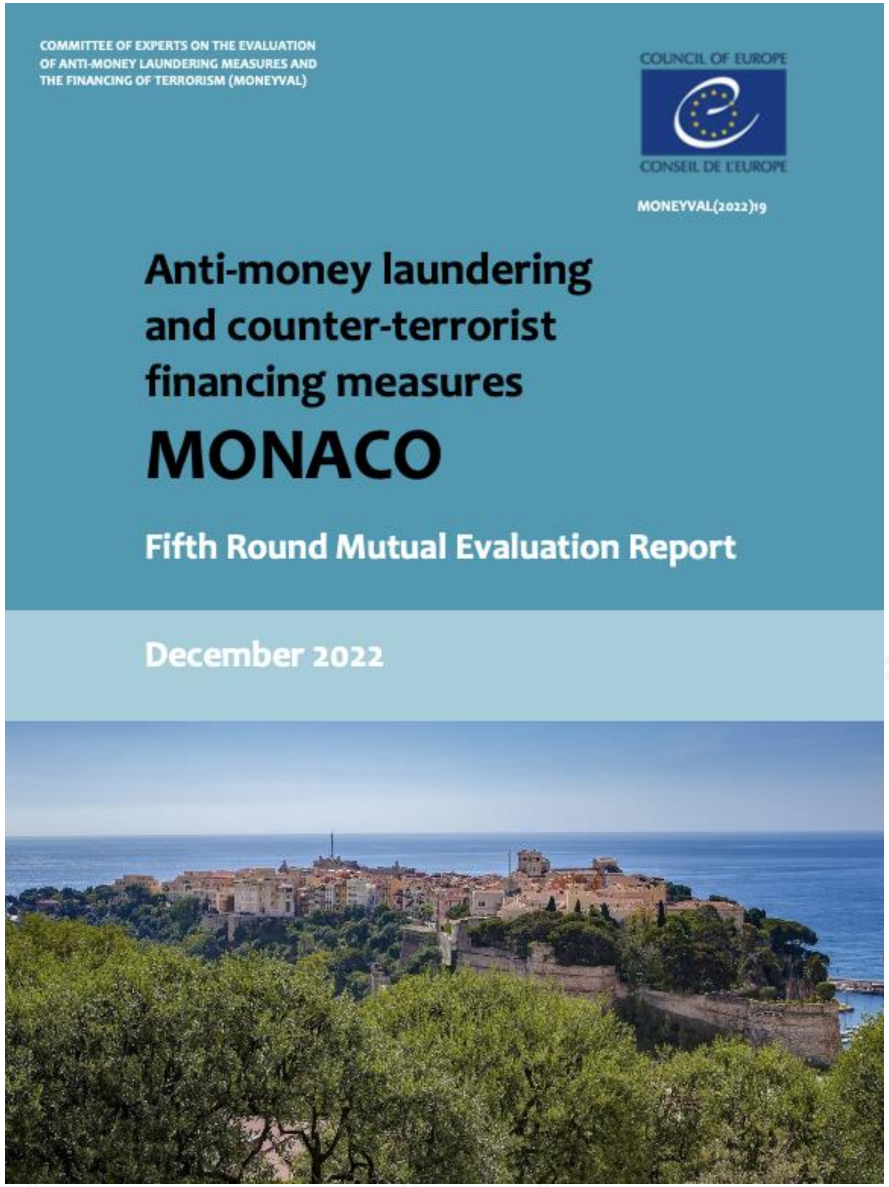
Monegasque legal framework

- The relevant legal obligations relating to the reporting of suspicious transactions for all reporting entities, are set out in:
  - **Art. 14 of the Law 1.362 (special examinations)**
  - **Chapter V (Art. 36 to Art. 45) of the Law 1.362 (STRs & mandatory reporting)**
  - **Art. 31 & Art. 36-2-1 of SO 2.318 (internal controls on reporting & form of reporting)**
- Professionals must file **<u>confidentially and without delay</u>** all transactions or attempted transactions involving sums or funds that they know or suspect to be derived from a predicate offence for money laundering or are related to terrorist financing or corruption offence, **before** the transaction is executed.

2022 MONEYVAL evaluation

Recommended action:

"The authorities should take measures to **improve the quality of STRs**, in particular by providing **guidance** and additional **red flags indicators**, by further developing the **typologies**. Ensure that the reporting entities **understand** and **timely fulfil** their STR obligations and that the internal audit and control departments **monitor** their sustainable implementation."



COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

MONEYVAL(2022)19

Anti-money laundering and counter-terrorist financing measures

MONACO

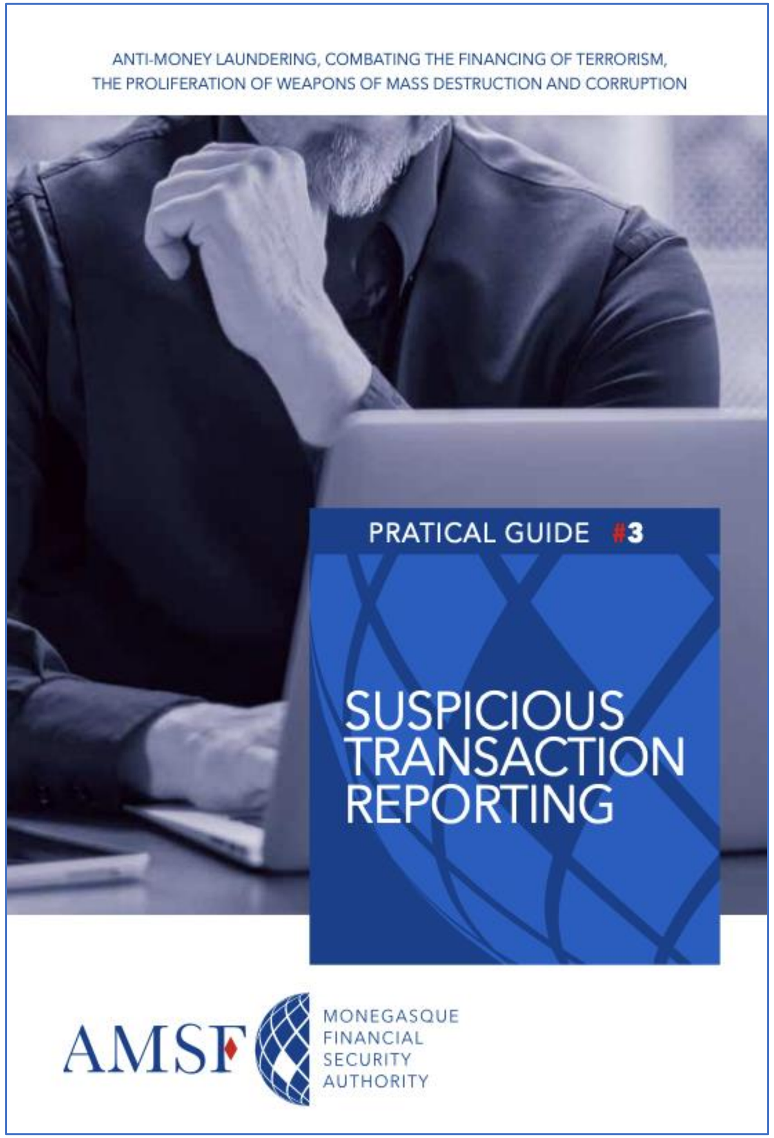
Fifth Round Mutual Evaluation Report

December 2022

Examples of actions taken pursuant to MONEYVAL Recommendation

- Implementation of **GoAML platform** for STR reporting
  - Relevant instructions and training slides on the use of GoAML are published on [this AMSF webpage]
- **AMSF publications** providing **guidance on STR obligations and red flags indicators**:
  - **Short Practical Guide** on STRs, providing a brief global overview of reporting obligations
  - **Detailed Guideline** on STRs, containing more detailed explanations of reporting obligations as well as an **Annex with Indicators** for suspicions
  - **Guidance on PEPs**, in light of exposure of Monaco to proceeds of offences of corruption and influence peddling & **Guidance on Private Banking and Wealth Management**, in light of high-risk exposure of these sectors, including specific red flags indicators related to these areas
  - All of these publications are available in French & English at [this AMSF webpage]
- **In-person training** organised by AMSF & FTA on "**Effective STR reporting**" (13-16 November 2023), covering in particular:
  - Detailed explanations of FATF standards, MONEYVAL findings & Monegasque legal framework on STRs
  - What is suspicion; How to identify and describe reasons for suspicion; Indicators
  - Elements of a good-quality STR and information to be included in STRs

Guidance on STR obligations and red flags indicators

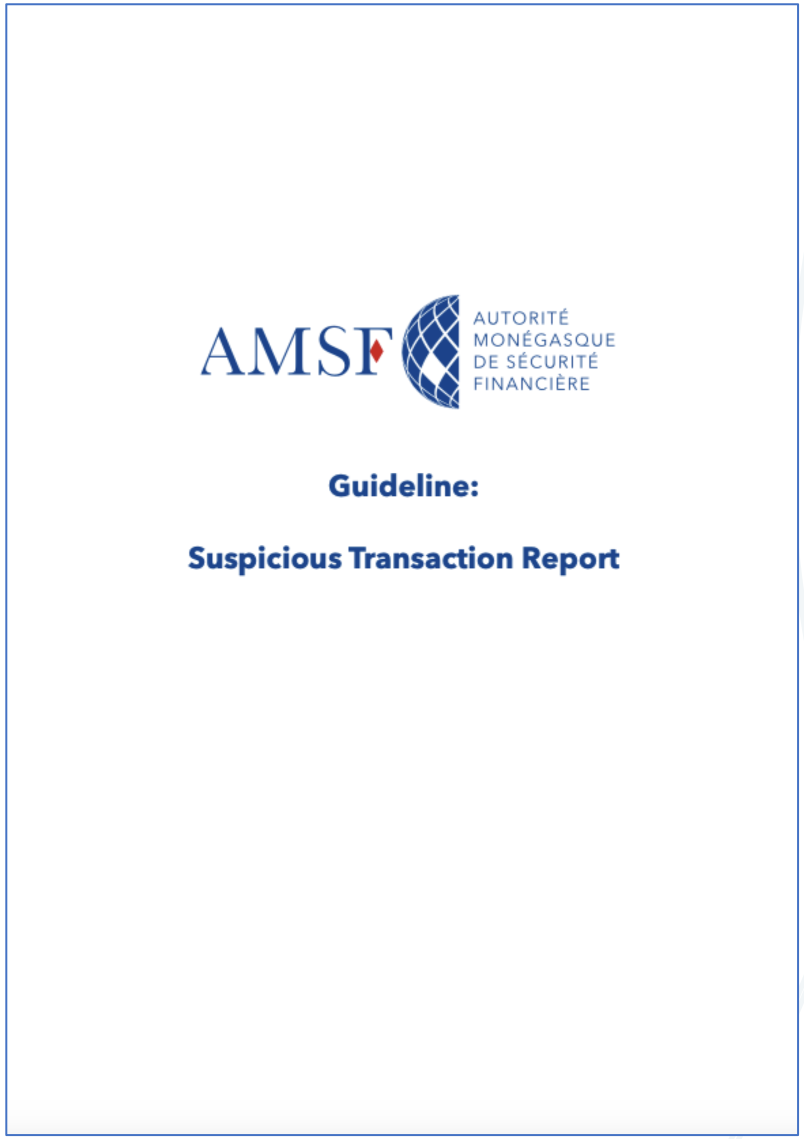


ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM,
THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND CORRUPTION

PRATICAL GUIDE #3

SUSPICIOUS TRANSACTION REPORTING

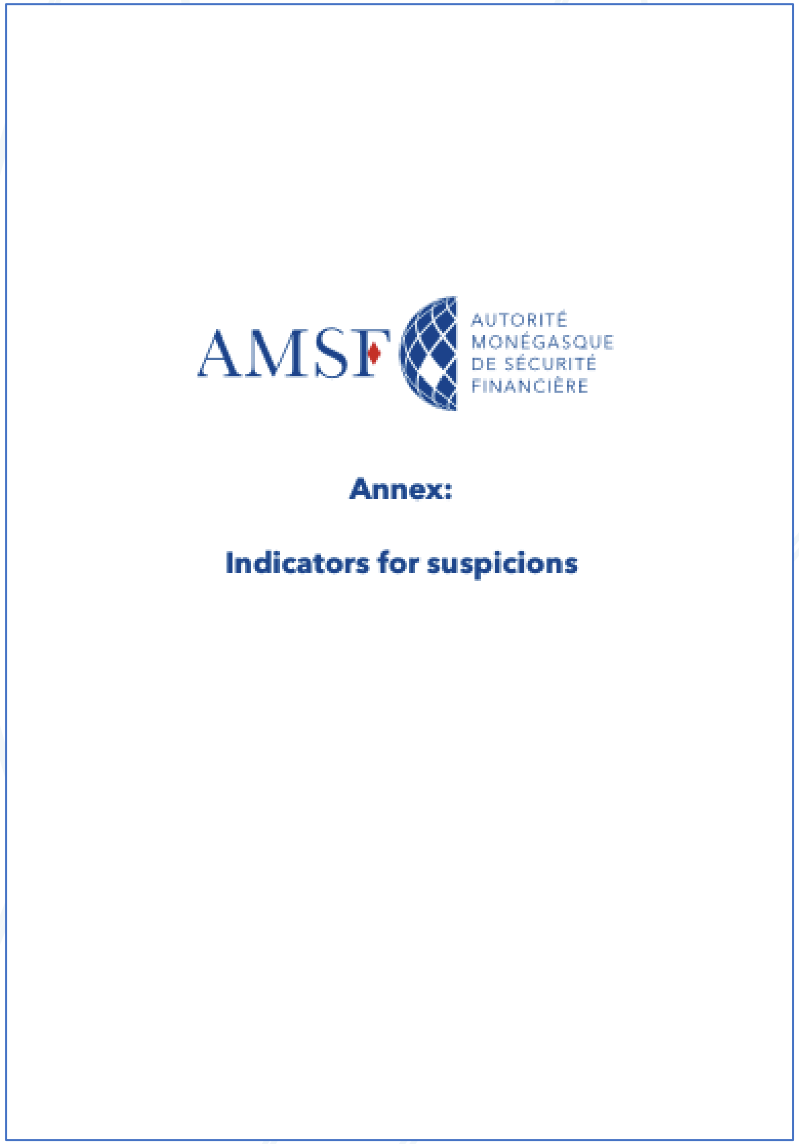
AMSF MONEGASQUE FINANCIAL SECURITY AUTHORITY



AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Guideline:

Suspicious Transaction Report

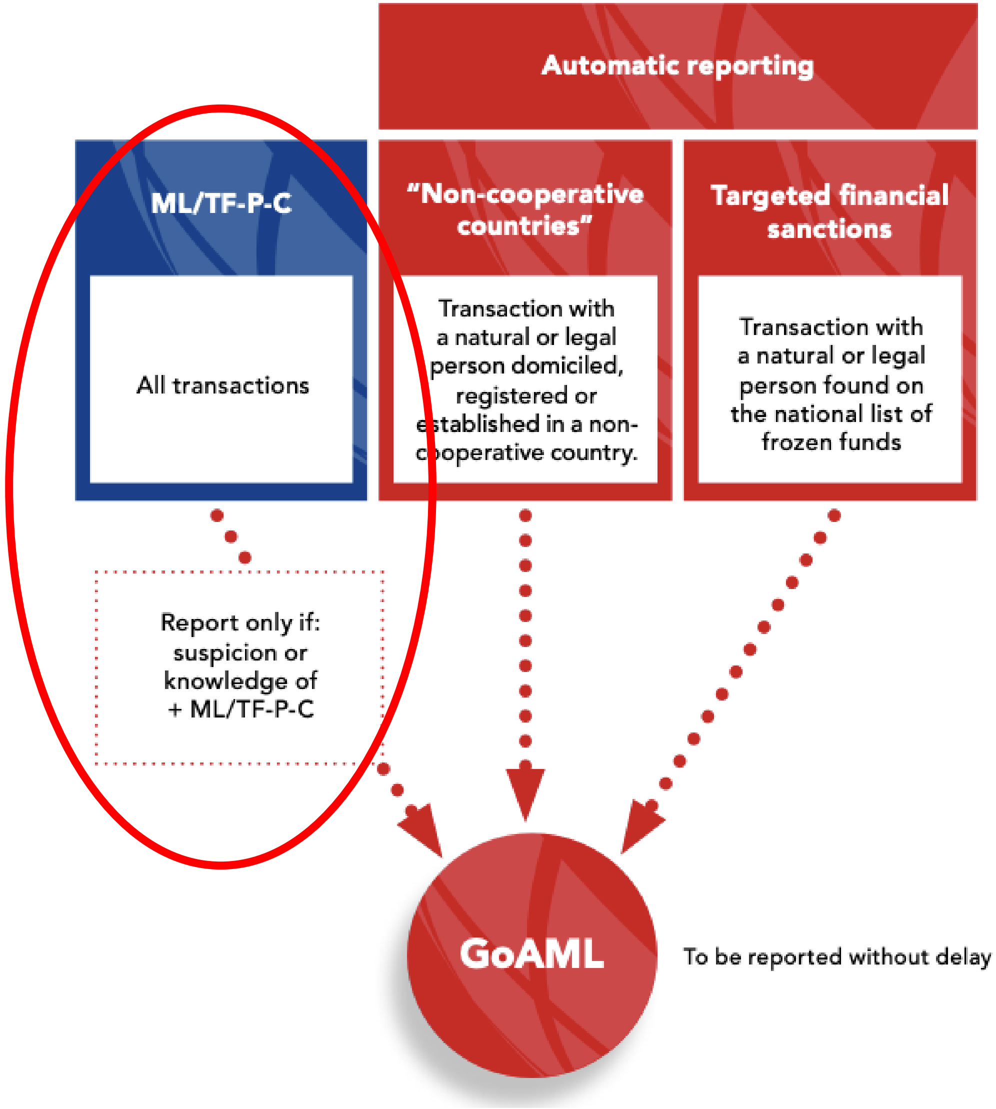


AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Annex:

Indicators for suspicions

Some key points on STR obligations



Automatic reporting

ML/TF-P-C

All transactions

Report only if:
suspicion or
knowledge of
+ ML/TF-P-C

"Non-cooperative countries"

Transaction with a natural or legal person domiciled, registered or established in a non-cooperative country.

Targeted financial sanctions

Transaction with a natural or legal person found on the national list of frozen funds

GoAML

To be reported without delay

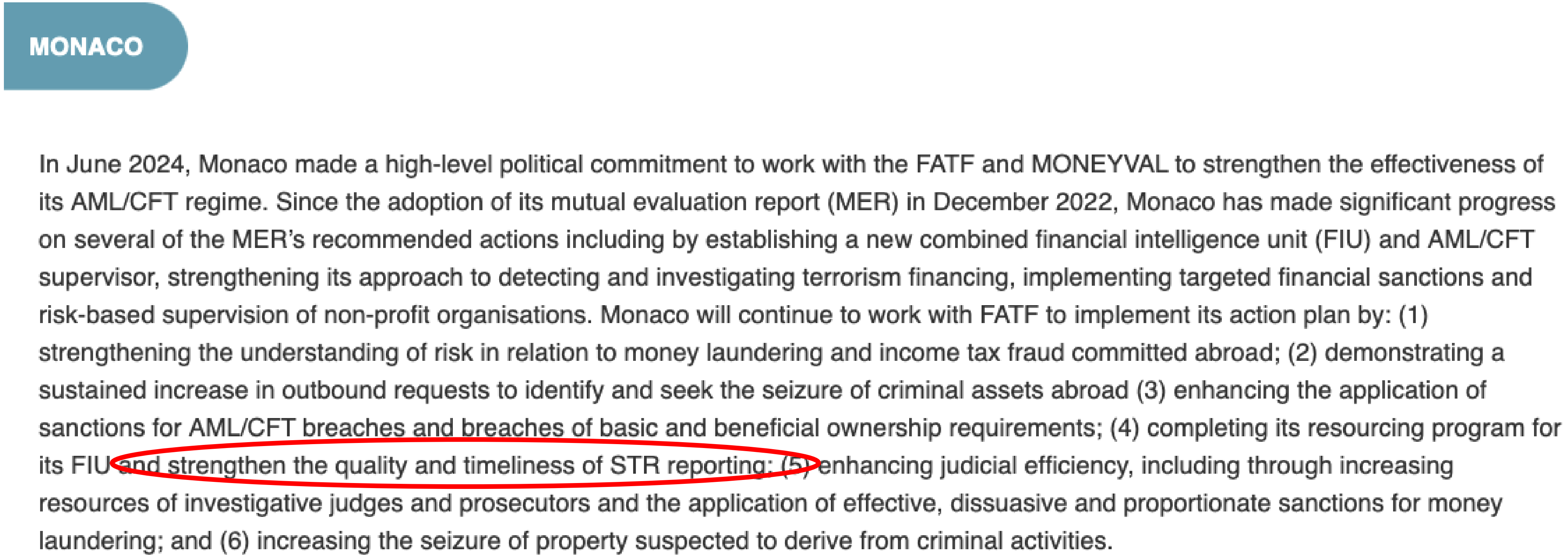
Obligations in all cases:

- supplementary report if the reporting entity gathers new information;
- confidentiality;
- respond to requests for further information;
- retention of reported elements.

NB : FIU's right to postpone

June 2024: Monaco grey-listed by FATF

To be removed from the list, the FATF expects to see the **effects of these efforts** and to note **improvements in the quality and timeliness of STRs filed in practice**:



MONACO

In June 2024, Monaco made a high-level political commitment to work with the FATF and MONEYVAL to strengthen the effectiveness of its AML/CFT regime. Since the adoption of its mutual evaluation report (MER) in December 2022, Monaco has made significant progress on several of the MER's recommended actions including by establishing a new combined financial intelligence unit (FIU) and AML/CFT supervisor, strengthening its approach to detecting and investigating terrorism financing, implementing targeted financial sanctions and risk-based supervision of non-profit organisations. Monaco will continue to work with FATF to implement its action plan by: (1) strengthening the understanding of risk in relation to money laundering and income tax fraud committed abroad; (2) demonstrating a sustained increase in outbound requests to identify and seek the seizure of criminal assets abroad (3) enhancing the application of sanctions for AML/CFT breaches and breaches of basic and beneficial ownership requirements; (4) completing its resourcing program for its FIU and strengthen the quality and timeliness of STR reporting; (5) enhancing judicial efficiency, including through increasing resources of investigative judges and prosecutors and the application of effective, dissuasive and proportionate sanctions for money laundering; and (6) increasing the seizure of property suspected to derive from criminal activities.

AML Tuesdays session of 17/09/2024 will provide further information on the FATF's decision to grey-list Monaco and the ICRG follow-up process and actions to be implemented to exit the list

02

Typologies, including new and emerging typologies

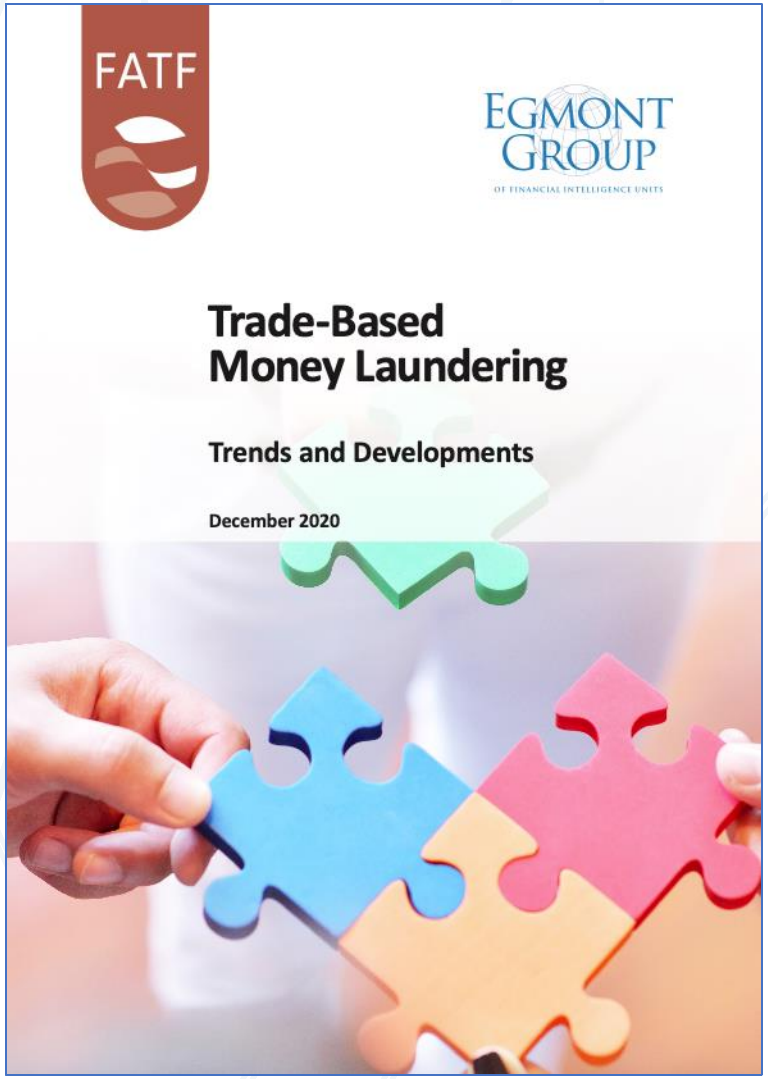
Common typologies involving FIs

Some common factors in scenarios reported worldwide whereby criminals and their associates abuse the services of FIs for ML/TF/PF/C purposes:

- **Funds being transferred across borders and between companies, e.g.:**
  - **Shell companies** with no legitimate economic rationale: for example, the StaR Initiative, a collaboration between the UNODC and the World Bank, noted in its review in 150 cases worldwide involving grand corruption that 128 involved the use of shell companies.
  - **Companies with complex ownership structures** that allows to conceal the ultimate owner of the assets held by the company, including cross-border structures, use of nominee shareholders, frontmen for people actually controlling the company, opaque structures such as trusts, etc.
- **Other types of transactions, e.g.**:
  - **Smurfing/structuring:** splitting large (cash) transactions to avoid detection/reporting; this process often involves **money mules**
  - **Transactions in context of trade-based money laundering:** over/under invoicing, ghost shipments, etc.

Example of “traditional” typologies: TBML

- **Trade-Based Money Laundering** is the process of disguising the proceeds of crime and moving value using **cross-border trade transactions** in an attempt to legitimize their illicit origins.
- TBML typically occurs through the **mis-invoicing of international trade transactions**. By fraudulently misreporting the price, quantity, or quality of goods, criminals can quickly move substantial amounts of money or value from one jurisdiction to another.
- When providing services to their **customers engaging in trade transactions**, FIs play an important role in the detection of TBML. **FIs engaged in trade finance** must be vigilant and implement TBML-specific control frameworks to protect their business from illicit activities.
- To learn more: see World Bank/IFC Open-access free course “Countering Trade-Based Money Laundering” tailored to front-line staff of FIs (available in English & French), including **TBML Typologies and red flags**



FATF

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Trade-Based Money Laundering

Trends and Developments

December 2020

New and emerging typologies

- Global and regional bodies such as FATF periodically publish **reports describing new and emerging ML/TF typologies** observed worldwide
- Financial institutions should keep themselves informed about such publications and determine which typologies can be **relevant in the context of their own geography, sector, business, customer profile and activities**
- The FI should monitor evolving risks on a continuous basis to determine whether there is a need to update its policies and procedures in order to adapt to the risks, e.g. whether there is a need to **add new red flags to its internal list of indicators** for potentially suspicious activity on the basis of such typology reports

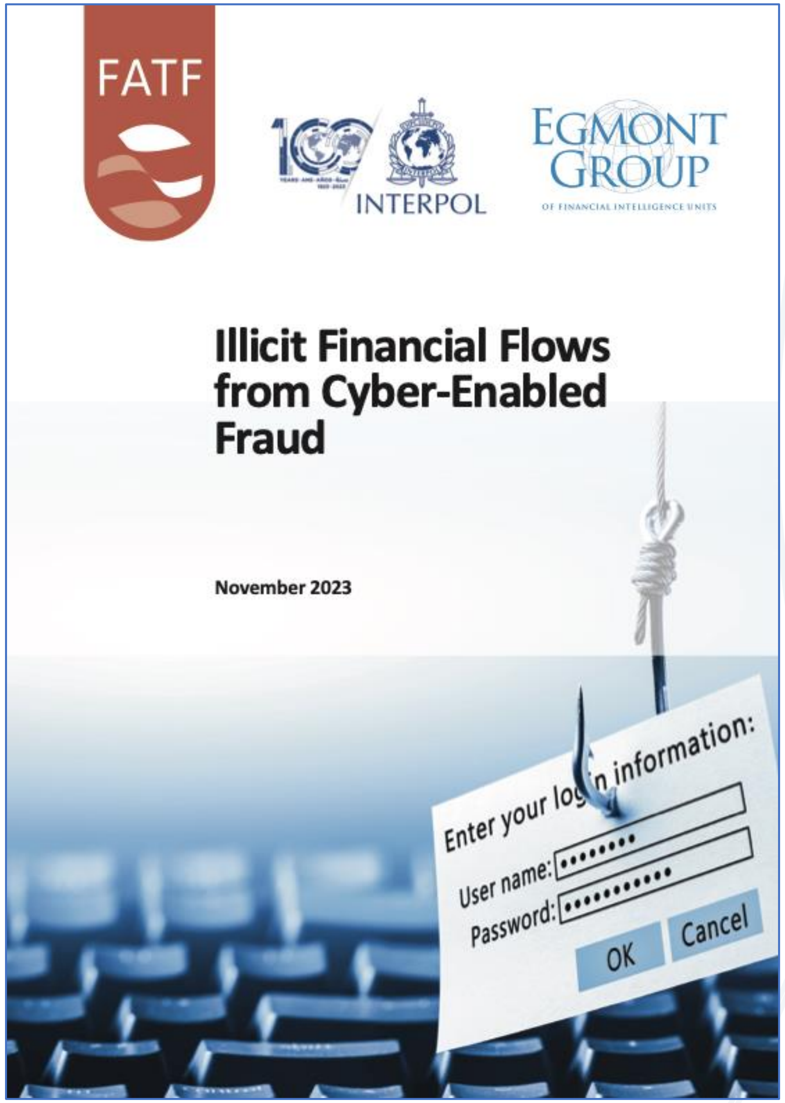
Examples of recent publications on typologies

FATF

OECD

Misuse of Citizenship and Residency by Investment Programmes

November 2023



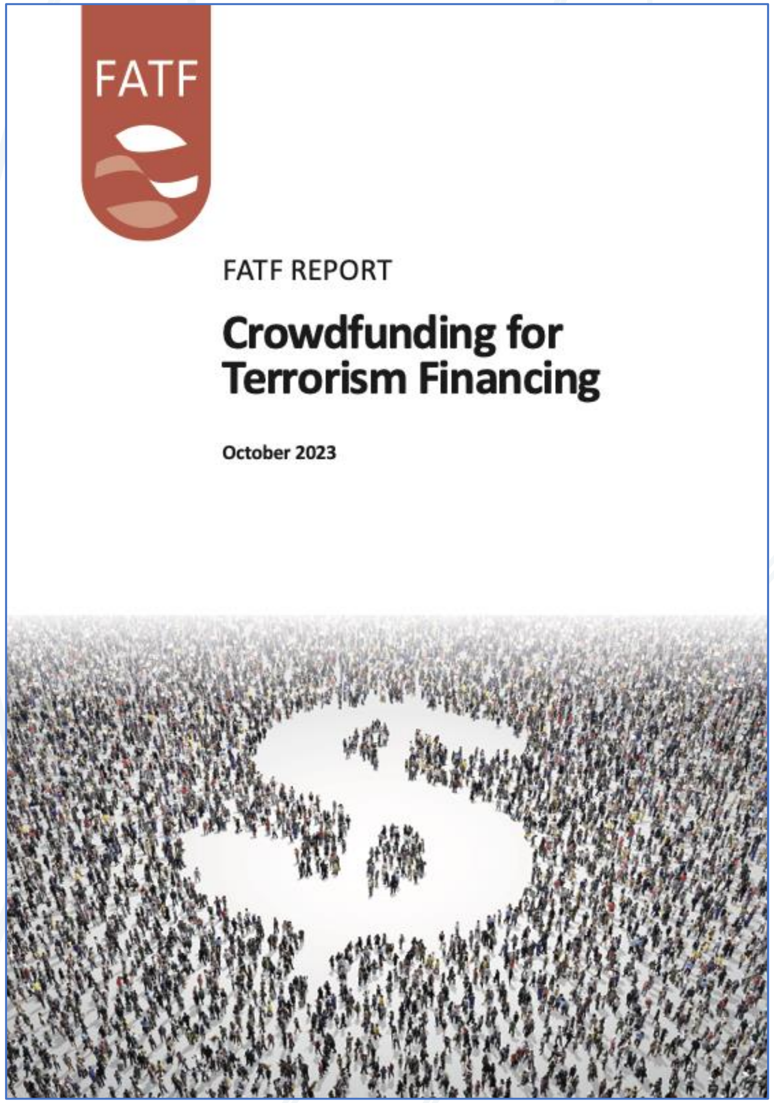
FATF

INTERPOL

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

Illicit Financial Flows from Cyber-Enabled Fraud

November 2023



FATF

FATF REPORT

Crowdfunding for Terrorism Financing

October 2023

Misuse of citizenship- and residency-by-investment programmes (CBI/RBI) – global context

From **2023 FATF report on misuse of CBI/RBI**:

- CBI/RBI programmes attract an array of clients, many of whom have gained their assets legitimately and have benign intentions. However, they can also be **abused by criminals** who seek to **launder and conceal proceeds of crime or commit new offences**, including financial crimes, undermining these programmes' intended objectives.
- As the popularity of investment migration programmes has grown, the **risk of illicit actors** utilising these programmes to their advantage **has also increased.**
- **CBI programmes are particularly vulnerable** because they allow illicit actors more global mobility, the ability to open bank accounts and establish shell companies in other jurisdictions, and to disguise their identity or conceal where they may owe taxes or other liabilities by using new ID documents.
- It is common for **high-risk individuals to gift wealth to their spouse or other family members** who will make the lead application for CBI/RBI, with the high-risk individual then applying as a family dependent. This typology can be particularly common in the case of **PEPs/corrupt actors**.

Misuse of CBI/RBI - observed typologies in Europe

From **European Commission's 2022 supra-national risk assessment (sNRA) for ML/TF**, chapter on CBI/RBI risks:

- The sNRA cites numerous examples of jurisdictions with **CBI schemes that have attracted wealthy people known or suspected to be involved in money laundering schemes**, including Malta, Cyprus, and Caribbean jurisdictions. In the EU, **only Malta still operates investor citizenship schemes.**
- Since the imposition of EU and U.S. economic sanctions, visa bans and asset freezes on Russia following its invasion of Ukraine in 2014, there has been **a surge in Russian applications for investor citizenship schemes worldwide;** this has given rise to the risk of **sanctions evasion in addition to the potential laundering of illicit funds.** Malta suspended its scheme for Russians & Belarussians in March 2022, but many Russians are known to have benefitted from the scheme before that date. A journalist investigation into the Cypriot investor citizenship scheme revealed several Russian nationals on US or EU sanctions lists who allegedly obtained Cypriot citizenship before the programme was suspended/abolished.
- **North Korean nationals** have also previously managed to **obtain alternative passports** (notably in Caribbean countries), which they then used to conduct business outside of North Korea.
- The EC concludes that the estimated risk level of ML for CBI/RBI schemes is **VERY HIGH**.

Misuse of CBI/RBI programmes – enhanced vigilance and red flags

- The OECD maintains an overview of jurisdictions with high-risk CBI/RBI schemes

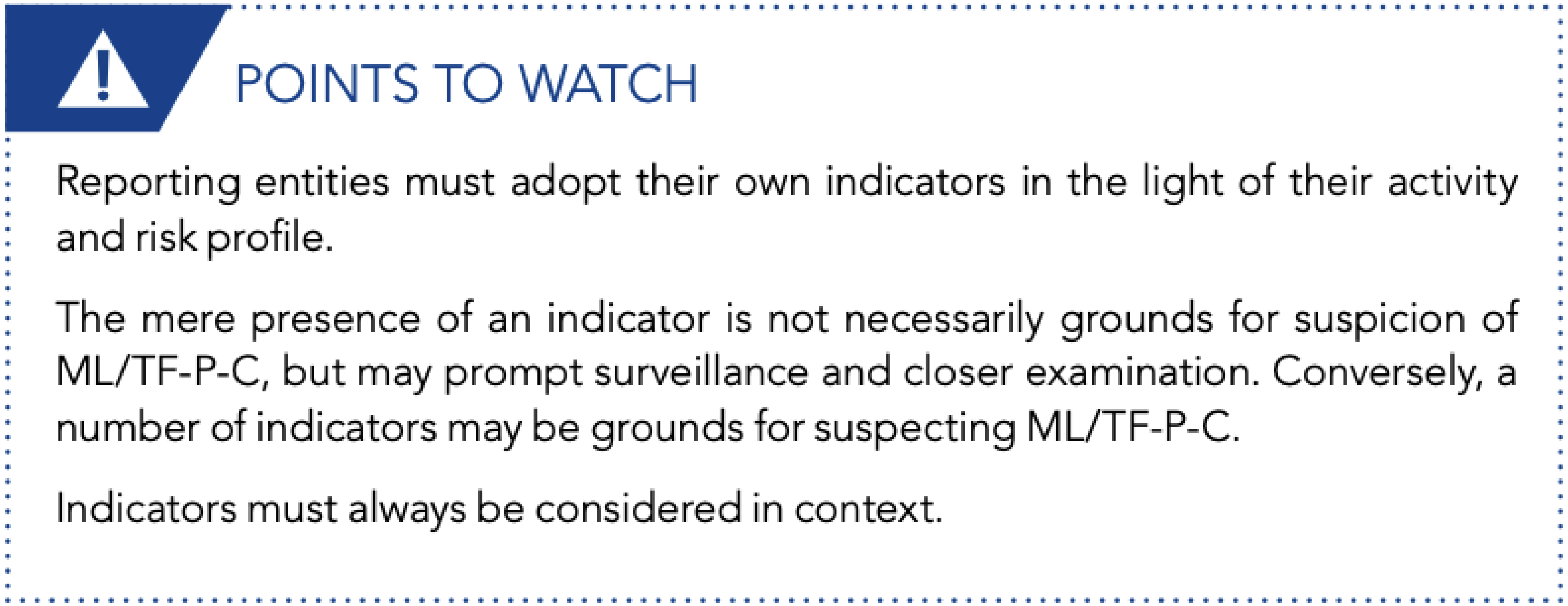
- The EU sNRA also provides examples of jurisdictions with schemes that are controversial or known to be exploited (see previous sheet)

- FIs should consider subjecting customers with citizenship/residency from jurisdictions with high-risk CBI/RBI schemes to **enhanced checks**, e.g. to determine:
  - whether they benefited from CBI/RBI schemes;
  - whether they have changed their identity in the course of the CBI process;
  - ensure that all their names, nationalities and passports are disclosed as part of CDD etc.,

  and **closely monitor/scrutinize the transactions of persons who benefited from such schemes** on a risk-sensitive basis

⚑ A customer benefited from a foreign CBI scheme, or a RBI scheme in a foreign jurisdiction with limited transparency, screening and monitoring measures for investors

03 Red flags indicators

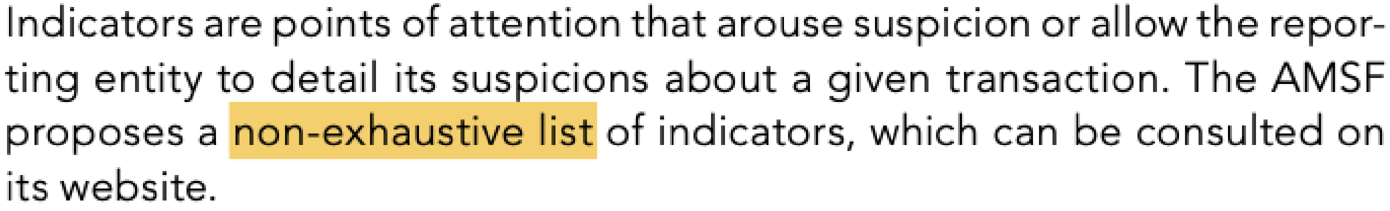


POINTS TO WATCH

Reporting entities must adopt their own indicators in the light of their activity and risk profile.

The mere presence of an indicator is not necessarily grounds for suspicion of ML/TF-P-C, but may prompt surveillance and closer examination. Conversely, a number of indicators may be grounds for suspecting ML/TF-P-C.

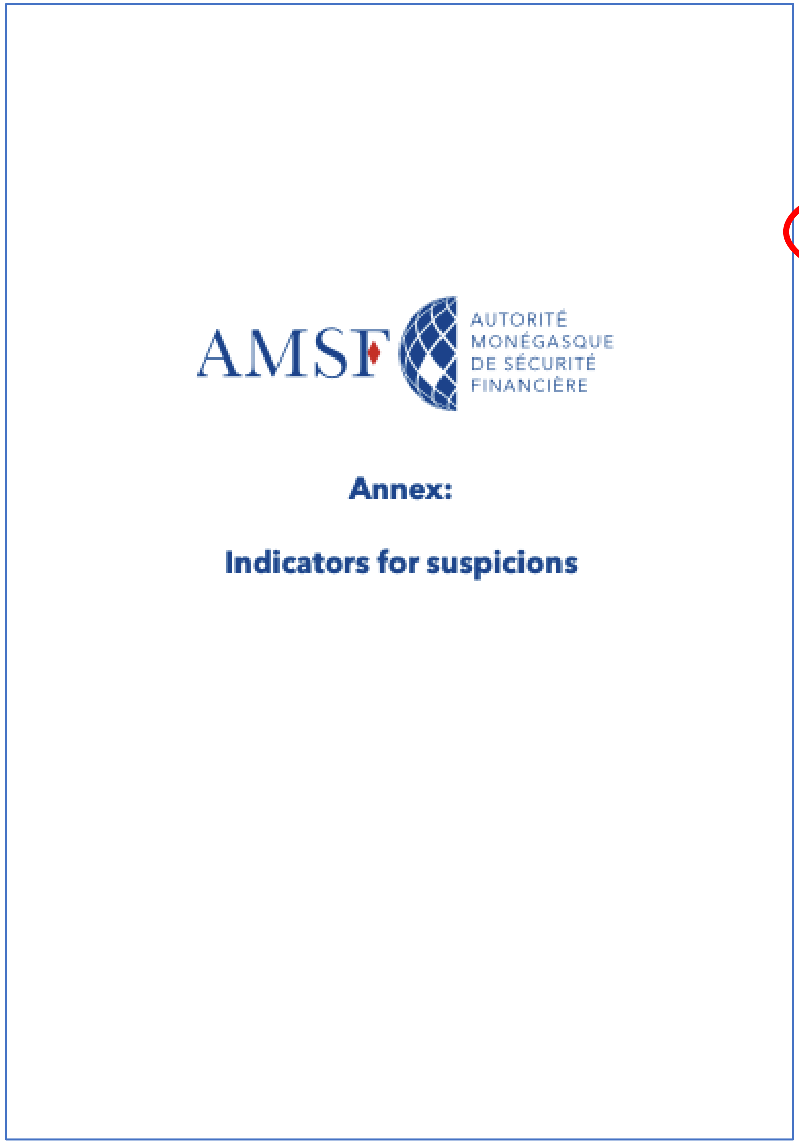
Indicators must always be considered in context.



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

The next slides contain **non-exhaustive examples of indicators**

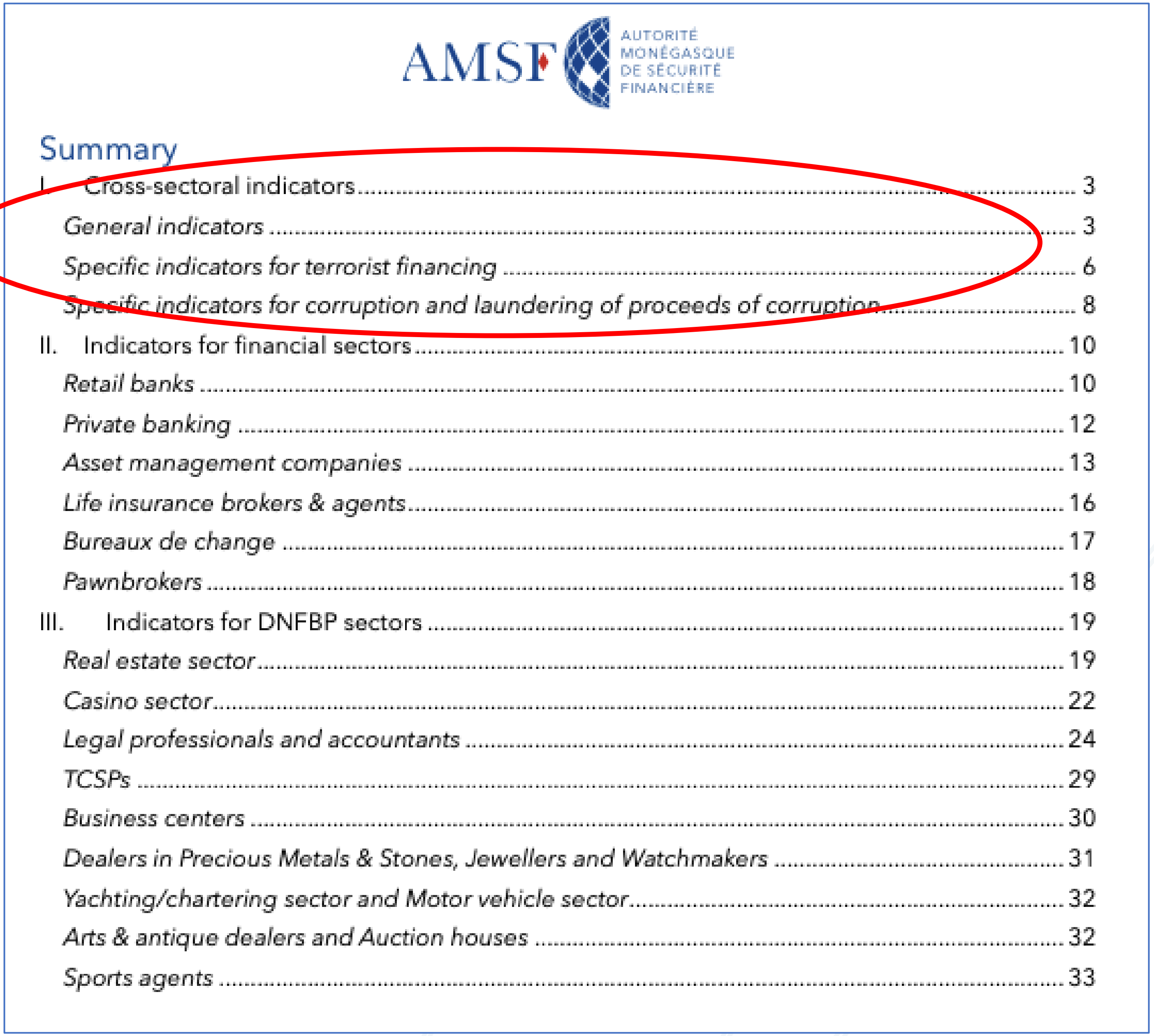
FIs should develop their own internal lists of red flags, tailored to their **<u>own activities and profile:</u>** products and services, customer base, transaction sizes, etc.



AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Annex:

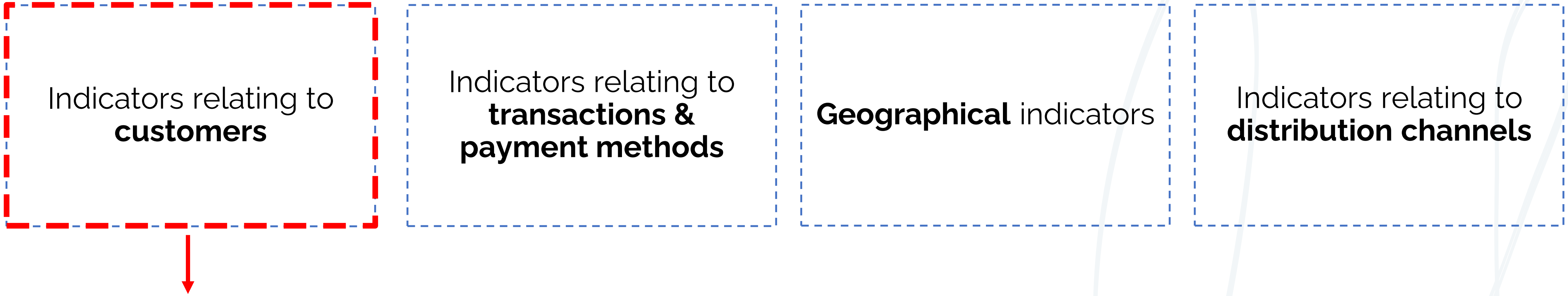
Indicators for suspicions



AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

General red flags indicators across sectors



Indicators relating to **customers**

Indicators relating to **transactions & payment methods**

Geographical indicators

Indicators relating to **distribution channels**

Examples of indicators relating to customers. particularly **customer behaviour:**

- 🚩 The customer offers to pay a higher price for unusual services or in exchange for more discretion
- 🚩 The customer is highly reluctant, refuses to provide information, or provides minimal, unclear or inconsistent information, or seemingly fictitious information, in relation to his/her identity, the identity of BOs, their business activities, etc.
- 🚩 The customer tries to persuade the (representative or employee of the) FI to not keep records of any documents that it has shared

TF red flags indicators

Indicators relating to (ab)use of **NPOs** for terrorist financing

Indicators relating to **wire transfers and remittances**

Indicators relating to **travel** for terrorist purposes

Other indicators for terrorist financing

Examples of indicators relating to **other TF indicators**:

- 🚩 Transaction patterns inconsistent with customer's age/employment/income
- 🚩 Customer's online presence supports violent extremism or radicalization
- 🚩 Reactivation of bank accounts after long period of inactivity, by depositing cash, receiving funds from family members, or using debit card to withdraw cash in ATMs in countries of bordering zones with armed conflicts/known presence of terrorist organizations

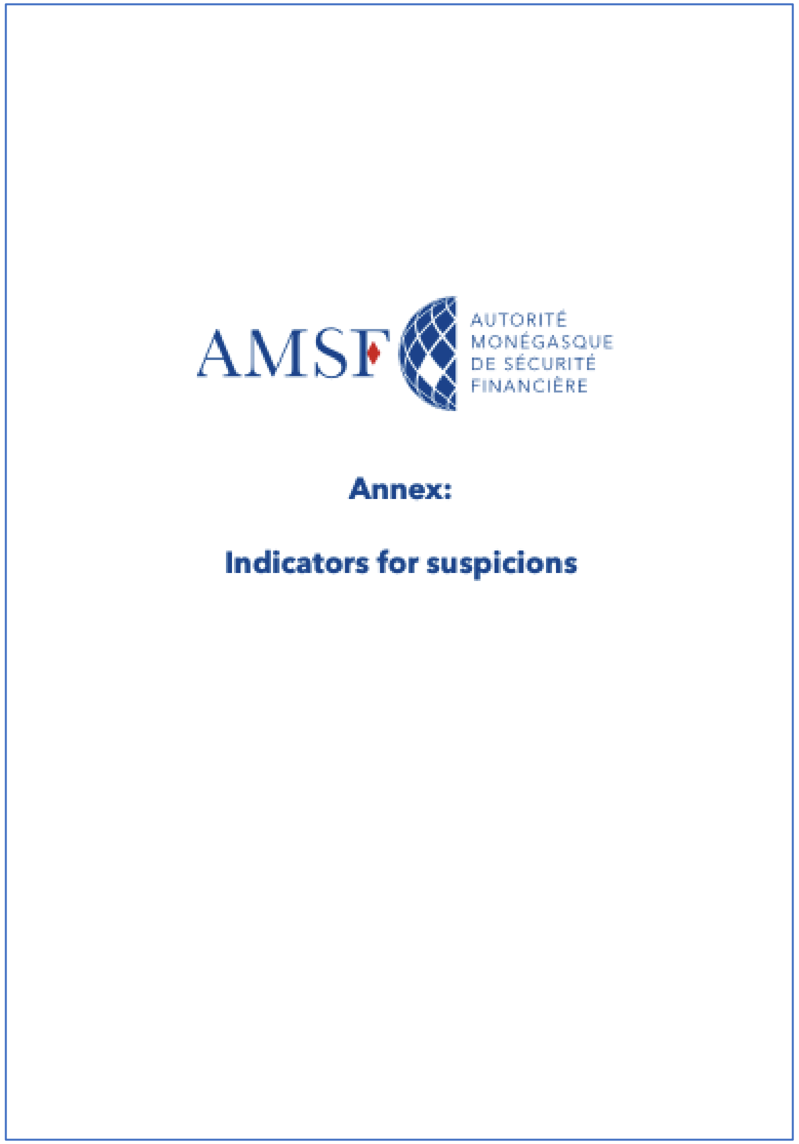
Corruption red flags indicators

Indicators relating to **PEPs** *(see also the indicators in the PEP guidance)*

Other indicators relating to corruption

Examples of indicators relating to **public procurement:**

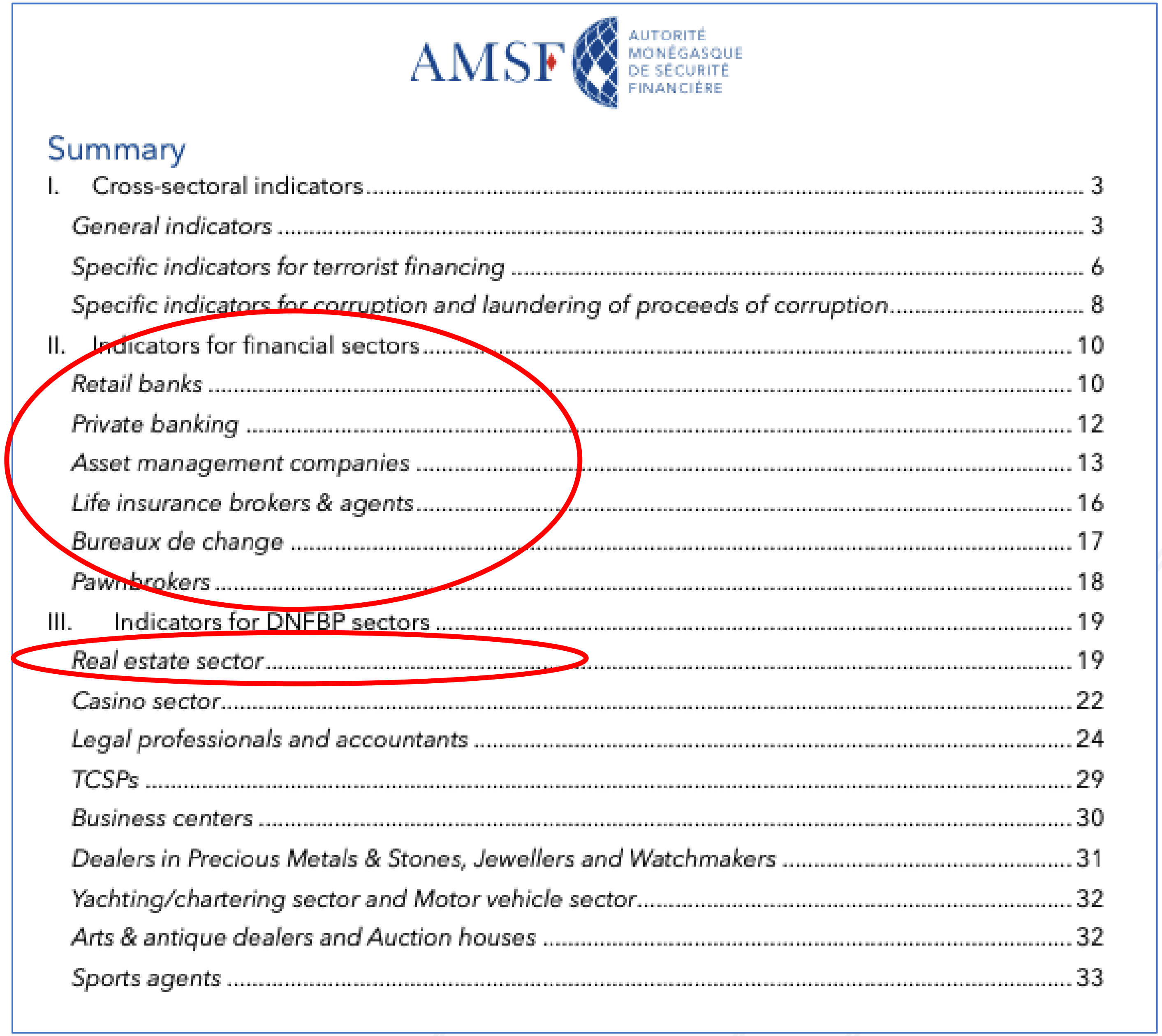
- Recently established companies are awarded major public contracts
- Long-term government contracts are consistently awarded to the same entity or entities that share similar beneficial ownership structures or the same responsible persons
- Documents corroborating transactions involving government contracts that include charges at substantially higher prices than market rates or that include overly simple documentation or lack traditional details (e.g., valuations for good and services)



AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Annex:

Indicators for suspicions



AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

Indicators for retail banking

Indicators relating to cash deposits and withdrawals

Indicators relating to loans

Indicators relating to bank accounts

Indicators relating to wire transfers

Indicators relating to credit card transactions

Other indicators

See also:
Indicators for financial transactions involving real estate (in Annex to the STR Guideline, under Real estate sector)

Example of indicators relating to loans

Indicators relating to **loan applications**:

- There is no apparent economic sense for a loan application
- The customer appears indifferent to the terms/costs/fees associated with the loan
- The customer cites foreign income on the loan application without providing further details, especially where higher-risk jurisdictions or territories are involved
- The customer is unwilling or unable to provide documentation to support the loan application, or the documentation is provided by a third party with no apparent reason to be involved in the loan

Indicators relating to **loan repayments**:

- Loan repayments that appear to be inconsistent with a customer's declared income or turnover
- Repayment of a long-term loan within a relatively short period, potentially followed by an application for another loan
- Repayment of instalments by unrelated third parties
- Large, unexpected loan repayments with funds from unknown sources or from sources which are inconsistent with previous information on the customer's source of funds

Indicators for private banking

Indicators relating to private banking customers

Indicators relating to source of wealth or source of funds

Indicators relating to transactions

See also:
Indicators for financial transactions involving real estate (in Annex to the STR Guideline, under Real estate sector)

Examples of indicators relating to **SoW/SoF**:

- Customer cannot provide clear information on the SoF/SoW
- The customer's funds originate from or are sent to, an entity that is not registered in the jurisdiction where either the customer or exchange is located
- Customer whose bulk of source of wealth is derived from investments in virtual assets

See also:
Indicators in the AMSF Guideline for Private Banking & Wealth Management

Indicators for asset management companies

Indicators related to investment/trading behaviour

Indicators related to customer accounts

Other indicators

Indicators related to payments/payment methods

Geographic indicators

See also:
Indicators in the AMSF Guideline for Private Banking & Wealth Management

Example of indicators relating to investment/trading

Indicators relating to **investment behaviour:**

- The customer wishes to engage in transactions/investment activity that are inconsistent with the customer's stated investment goals, investment profile/practice/history or their financial ability and there is no reasonable explanation
- The customer does not exhibit any concern with the cost of transactions or investment losses, or is willing to deposit or invest at rates that are not advantageous or competitive
- The customer wants to purchase investments in the name of another party or the customer wants to use shell companies to purchase investments or wants to acquire bearer shares

Indicators relating to **transfers in securities/funds**:

- Transfers of securities are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation
- "Deposit, sale, and withdrawal activity": the customer has a pattern of depositing funds for purchase of a (long-term) investment or depositing shares followed shortly by the request to liquidate the position or by the sale of the shares, and subsequently transfers the proceeds out of the account
- Mirror trades or a pattern of securities transactions indicating the customer is using securities trades to engage in currency conversion for illegitimate or no apparent business purposes

Fictionalized case study: Application of red flag scenario in practice

- An existing customer of Bank ABC, resident in Monaco, Mr. X, introduces a “business acquittance” as a potential interesting new customer to the bank: Mr. Y. The association between Mr. X and Mr. Y is not further specified.
- Mr. Y is a non-resident to Monaco, who lives in Malta and who is the director of healthcare company DEF based in Malta. He requests to apply for a loan from Bank ABC for DEF, to contribute to the funding of the development of DEF’s projects in Malta.
- Through a Google search, the loan officer finds out that Mr. Y appears to be a Indian businessman with Maltese citizenship and that company DEF is subject to adverse media in Malta.
- There are no immediate apparent links between Mr Y and the Principality, except for the introduction by Mr. X. Neither of them immediately offers a reason to the banker as to why Mr. Y would be applying for such services in Monaco rather than in Malta.

Case study: Application of red flag scenario in practice *(continued)*

Red flags immediately identified by the front-line loan officer:

- No clear apparent link between the introducing client and the prospective new client
- No clear apparent link between Monaco and the location of residency/citizenship/activities of the prospective customer
- Adverse media on the prospective customer
- The director of the customer may have benefited from Malta's citizenship-by-investment programme

Hence, on the basis of the bank's internal procedures, the loan officer decides to quickly escalate the request to the compliance department for a **special examination into Mr. Y, based on an unusual attempted transaction,** without tipping off either Mr. X or Mr. Y.

(NB: a **special examination** should also be launched into the past and ongoing transactions of **Mr X** on the basis of the fact that he served as the introducer for an unusual prospective customer, but this remains outside of scope of rest of the case study)

Case study: Special examination into Mr. Y

The compliance department instructs the loan officer to **collect further CDD information**, resulting inter alia in the following findings:

- Mr. Y has hostile responses in respect of sensitive questions from the loan officer, e.g. as to whether he benefited from the Maltese CBI programme and whether he has connections to PEPs.
- DEF was formed recently and the information provided by the company representatives on prior experience in healthcare of its main shareholders and directors (CV's) cannot be corroborated through open source information.
- The applicant maintains that DEF also has lenders in Malta, but that this is not yet enough to fund its ambitious projects, which is why they are now also looking for foreign lenders. However, DEF fails to provide any details or documentation on its financial position/current debts/outstanding loans of other FIs, within the requested timeframe.

Case study: Special examination into Mr. Y *(continued)*

At the same time, a **detailed analysis of the adverse open-source media information** is carried out on the company.

Through this analysis, it is determined that DEF is subject to several accusations by Maltese journalists of being implicated in bribery, misappropriation of funds and mismanagement, including for:

- having been awarded contracts for the private operation of three Maltese hospitals under suspicious circumstances, notably allegations of collusion between public officials deciding on the privatisation and the winning company's shareholders;
- having accumulated high debts in the years since obtaining the contracts, combined with failures to deliver on any of the intended improvements of the hospitals foreseen in the privatisation plans.

Case study: Special examination into Mr. Y *(continued)*

Additional red flags identified through the special examination:

- ⚑ The customer is reluctant or unable to provide standard CDD information
- ⚑ The customer is unwilling or unable to provide documentation to support the loan application
- ⚑ The customer is a recently established company which has been awarded a major public contract
- ⚑ Extensive adverse media on the company including in relation to corruption and embezzlement

Hence, following the special examination, the Bank decides to **file an STR with the FIU,** for an attempted transaction, setting out all of the red flags identified, on the basis of the suspicion that the funds that may be disbursed as part of the loan may become subject to **embezzlement** rather than be invested in healthcare projects, and that the funds intended to be used to repay the loan may derive from **ML/corruption offences** committed by DEF/its directors/its associates.

FINANCIAL
TRANSPARENCY
ADVISORS

Thank you for your time

Financial Transparency Advisors GmbH
Zieglergasse 38/7/1070 Vienna, Austria

Phone: +43 1 890 8717 11

www.ft-advisors.com

http://www.ft-advisors.com

Next Session:

17.09.2024

Topic:

ICRG Discussion

Today's Host: Suzanna van Es

Today's Presenter: Suzanna van Es