FIAU

Guidance Document on

Reporting through goAML

CONTENTS

GLOSSARY

AML	Anti-Money Laundering
PMLA	Prevention of Money Laundering Act
PMLFTR	Prevention of Money Laundering and Funding of Terrorism Regulations
FIAU	Financial Intelligence Analysis Unit
SP	Subject Persons
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
PEPR	Politically Exposed Person Report
PEPTR	Politically Exposed Person Transaction Report
TFR	Terrorism Financing Report
TFTR	Terrorism Financing Transaction Report
AIF	Additional Information File
TRN	Transaction Report

1. REPORTING TRANSACTIONS CONNECTED TO IRAN THROUGH goAML

The Financial Intelligence Analysis Unit (FIAU) is issuing this guidance note to Subject Persons (SP) to clarify and assist with the reporting of transactions connected to Iran by means of the goAML platform.

The FIAU issued a Directive on 17 December 2019 in terms of Article 30C of the Prevention of Money Laundering Act (PMLA), which applies to all SPs as defined by Regulation 2(1) of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR), in their dealings with natural or legal persons having connections with Iran. Given that the FATF had proceeded to lift the suspension of countermeasures and called upon jurisdictions to apply effective countermeasures, this Directive no longer applies and has been replaced by the Notice the FIAU had issued on 25 February 2020, whereby the provisions of Regulation 11(11) of the PMLFTR, have now come into force instead.

Due to this and until further notice from the FIAU, Iran is now to be considered as a jurisdiction for which there has been an international call for countermeasures (i.e., an FATF 'Category 1' jurisdiction in terms of Chapter 8 of the Implementing Procedures Part I).

Under the same regulations mentioned above, SPs must also take note of the EU's consolidated list of high risk third countries.

Subject Persons should be aware that the Implementing Procedures Part 1 state that the natural or legal person should be 'established' in the jurisdiction in question. Guidance has been provided as to how 'established' should be interpreted under Section 4.9.1 of the Implementing Procedures – Part I. Note that the section refers to numerous factors that 'establish' the person to the non-reputable jurisdiction, such as where the main activities of the person generating his wealth are located or where the person is residing or operating. The guidance also makes reference to personal connecting factors like place of birth and citizenship, but this section also provides that:

[h]aving citizenship on its own need not be automatically equated with the natural person being established in the non-reputable jurisdiction if the individual has no other links with the jurisdiction concerned'

This aspect is also highlighted under Section 8.1.3 of the Implementing Procedures – Part 1 wherein it is stated that:

'not every form of connection to a non-reputable/high-risk jurisdiction will give rise to the requirement to apply EDD. By way of example, when a business relationship or an occasional transaction involves a customer who is a citizen of a non-reputable/high-risk jurisdiction but does not reside in that jurisdiction and the business/economic activity and/or the source of wealth/funds involved are not in any way connected with that jurisdiction, the requirement to apply EDD does not arise'

In a nutshell, if any of the persons in question only happen to either have been born in a non-reputable jurisdiction or have citizenship from that country but no other connections, it would follow that neither the reporting obligations under Regulation 11(10) and (11) nor the PMLFTR would need to be applied.

Example 1:

A Casino is faced with a customer that has deposited EUR 2,000.00 in cash. Source of wealth documentation has been provided which shows that he is employed with a reputable Maltese company earning a sufficient salary to cover his gaming activity. However, upon verifying the customer's identity, the gaming operator notes that he was born in Iran and holds an Iranian Passport. When questioned about this, the customer points out that he has been living in Malta for the past 20 years, which is clearly evidenced by the contract of employment and his proof of address, and that he has no ties with Iran as he left at a very young age. Additionally, he has dual citizenship and holds a Maltese passport. In this regard, under the regulations and notices in question, the casino is not obliged to report the individual. As a further mitigating measure, the remote gaming company will continue monitoring the activity of the customer to ensure that, throughout the course of the business relationship, the customer does not disclose any links with Iran (such as the use of an Iranian bank account to deposit or withdraw funds).

Example 2:

A Maltese registered Company ultimately owned by a UK national is going to be onboarded by a Company Service Provider (CSP). Upon taking closer look at its structure chart, the CSP notes that the UK national ultimately owns the company through an Iranian registered company. Moreover, the CSP is informed that the objective of the company is to sell grain in Iran. Therefore, since most of the source of wealth of the company originates from Iran and 25%+1 shares are owned by an Iranian registered company, the CSP is obliged to report the company under the mentioned regulations.

6

In order to comply with Regulation 11(11) of the PMLFTR, SP should:

1. Inform the FIAU of:
    a. Any existing business relationships connected with Category 1 jurisdictions
    b. Any pending transactions connected with a Category 1 jurisdiction
    c. Any requests to establish a business relationship or carry out a transaction (whether occasional or otherwise) connected with a Category 1 jurisdiction.

In addition, any transaction(s) connected with Iran, should include the provision of the following details:

    i. Full name and details of the customer and, where applicable, the beneficial owner, who has a business relationship or is carrying out an occasional transaction in the context of which transactions connected with Iran are to take place;
    ii. Details of any other known parties to those transactions;
    iii. The manner/channel through which the transaction is to be made;
    iv. The exact value of the transaction;
    v. A description of the transaction, including its purpose and scope.

2. To inform the FIAU about Iranian registered companies or those companies having branches or subsidiaries in Iran and to:
    a. identify who exercises control over such companies, branches, and subsidiaries
    b. carry out increased external audits on the application of the group-wide AML/CFT policies and procedures by such companies, branches, or subsidiaries

3. SP may only execute transactions connected with Iran if there is no written opposition by the FIAU within five (5) working days from when the notification is sent to the FIAU. Provided that where it is not possible to refrain from carrying out the transaction, prior to informing the FIAU, the SP must inform the FIAU immediately following the transaction.

Due to the introduction of the goAML platform, as of 18 June 2020, SP are to submit the required information/notification to the FIAU through the goAML platform, in line with Regulation 11(2) of the PMLFTR using the appropriate report type (Refer to Section 2 of this Guidance Document). Notifications under the Regulations must therefore be made irrespective of whether there is a suspicion of money laundering, funding of terrorism or proceeds of crime.

Furthermore, it is also important to mention that SP outline the previously highlighted details included in the FIAU's Iranian Nationals Notice (Dated 25 February 2020) through the goAML platform's designated fields accordingly.

Another requirement for SPs is to highlight the reporting indicator in line with the nature of the transaction being reported. The FIAU has now made available to SPs an additional report indicator dedicated to transactions in connection to Iran namely: "High- Risk Jurisdictions subject to a Call for Action". SPs are required to select the related report indicator within the report in conjunction with any other relevant indicators.

+41.87

+32.69%

-24.98%

-34.87%
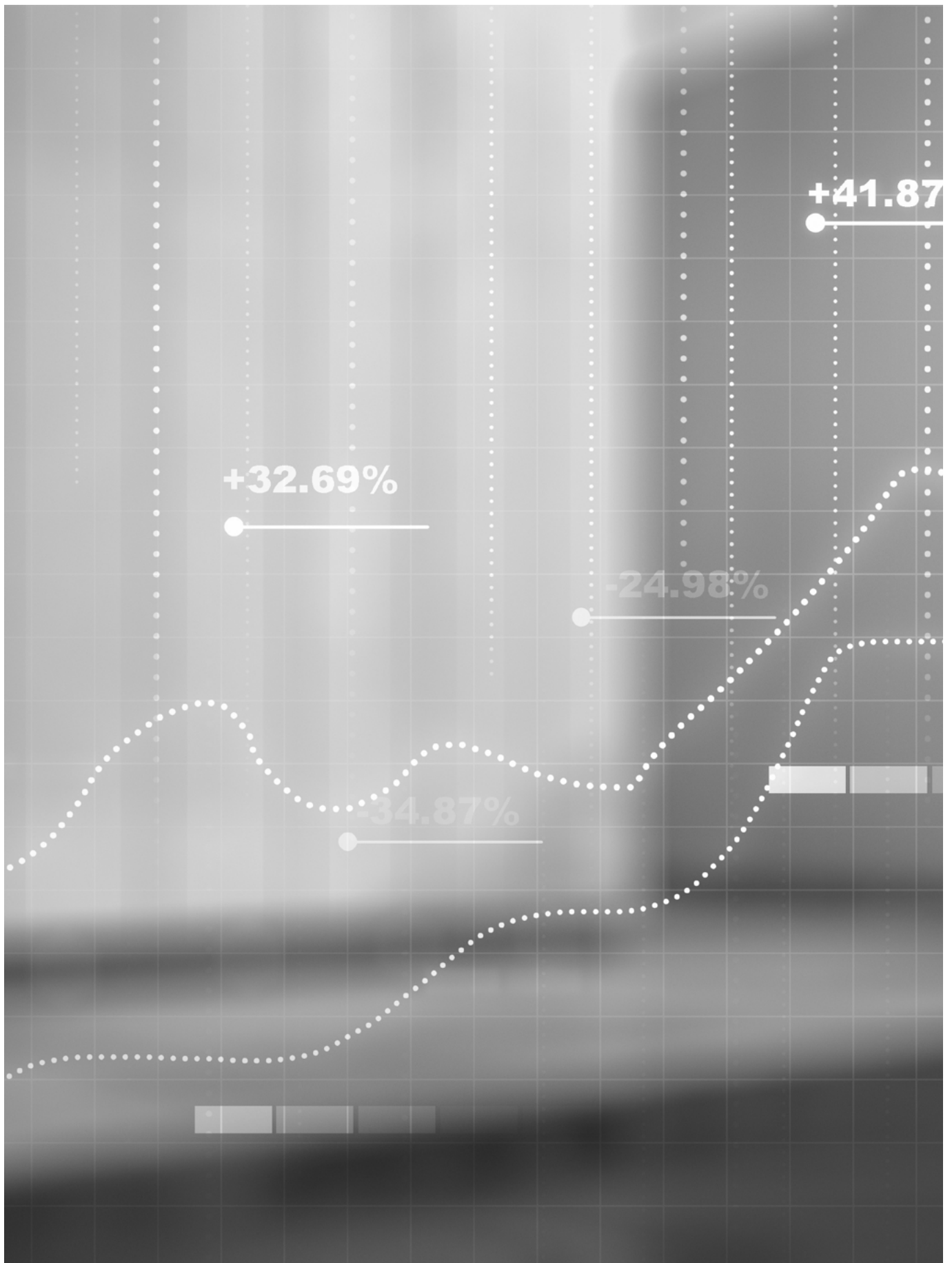
2. THE DIFFERENCE IN REPORT TYPES

Since going live with goAML in June 2020, the FIAU has been approached on various occasions to clarify the difference in report types.

The report types used in goAML consist of STR, SAR, PEPR, PEPTR, TFR, TFTR, AIF and TRN.

The different report types allow the FIAU to collate more detailed statistical information. This assists the Unit in the prioritising and timelier execution of its functions and allows for more detailed information to be sourced. This helps fine tune the various outreach initiatives undertaken by the Unit. In addition, the Unit has, on various occasions, been asked to provide very detailed statistical information. Without the introduction of these multiple report types and the more detailed reporting criteria, it would not be possible to respond to these requests effectively.

When to submit a STR?

The main components of an STR are 'Suspicion and Transaction'. An STR consists of a transaction or series of transactions which are deemed to be suspicious due to not being in line with the customer's known or expected transactional profile.

Ex 1. Customer deposits a onetime cash payment of €20K which is not observed to be in line with their known profile and offers no reasonable explanation for this deposit. All other transactions made by the customer are in line with their expected activity. In this case, the SP should report only the suspicious transaction to the FIAU by submitting an STR regarding the €20K transaction. The remaining transactions should be submitted as an additional information file (AIF).

Ex 2. Customer has an expected turnover of €20K per year. However, the transactional activity shows that the turnover of the customer adds up to €50K per year. In this case, the reporting entity should submit an STR with the FIAU, highlighting all the transactions carried out by the customer which total to the €50K.

Ex 3. Customer carries out a series of deposits which are not in line with their usual or expected activity. No explanation for this was provided. In this case, the reporting entity should submit an STR containing all the transactions made by the customer which gave rise to the SP's ML/FT suspicion. All other transactions made by the customer which do not give rise to suspicion of ML/FT should be submitted as an AIF.

When to submit a SAR?

The main components of an SAR are 'Suspicion and Activity'. An SAR consists of transactional activity which is in line with the known or expected profile, but the customer displays behaviours which raise suspicion. Examples of this include but are not necessarily limited to;

- Adverse information through open sources
- Refusal to provide requested documentation
- Uncooperative behaviour
- Becoming uncommunicative
- Refused onboarding

If such suspicious activity is identified during the initial stages of a business relationship (including during the on boarding stage), SPs are to evaluate the information obtained and consider submitting a SAR.

When to submit a AIF?

```
                        ┌─────────────────────────┐
                        │  Initial report - Submitted │
                        │  with necessary documents   │
                        └─────────────────────────┘
                                    │
                                    ▼
                              ◇ Do I have more
                  Yes ◄───────  information to add?  ───────► No
                    │
                    ▼
              ◇ Is the information
                transactional?        ── No ──►  ┌──────────────────────┐
                    │                            │ Submit via message board │
                    ▼ Yes                        └──────────────────────┘
              ◇ Is the transaction
                suspicious?           ── No ──►  ┌──────────────┐
                    │                            │ Submit as AIF │
                    ▼ Yes                        └──────────────┘
              ◇ Does it change
                the suspicion of      ── No ──►  ┌──────────────┐
                the initial report?              │ Submit as AIF │
                    │                            └──────────────┘
                    ▼ Yes
        ┌─────────────────────────┐
        │  Submit as STR with       │
        │  reference to initial report │
        └─────────────────────────┘
```
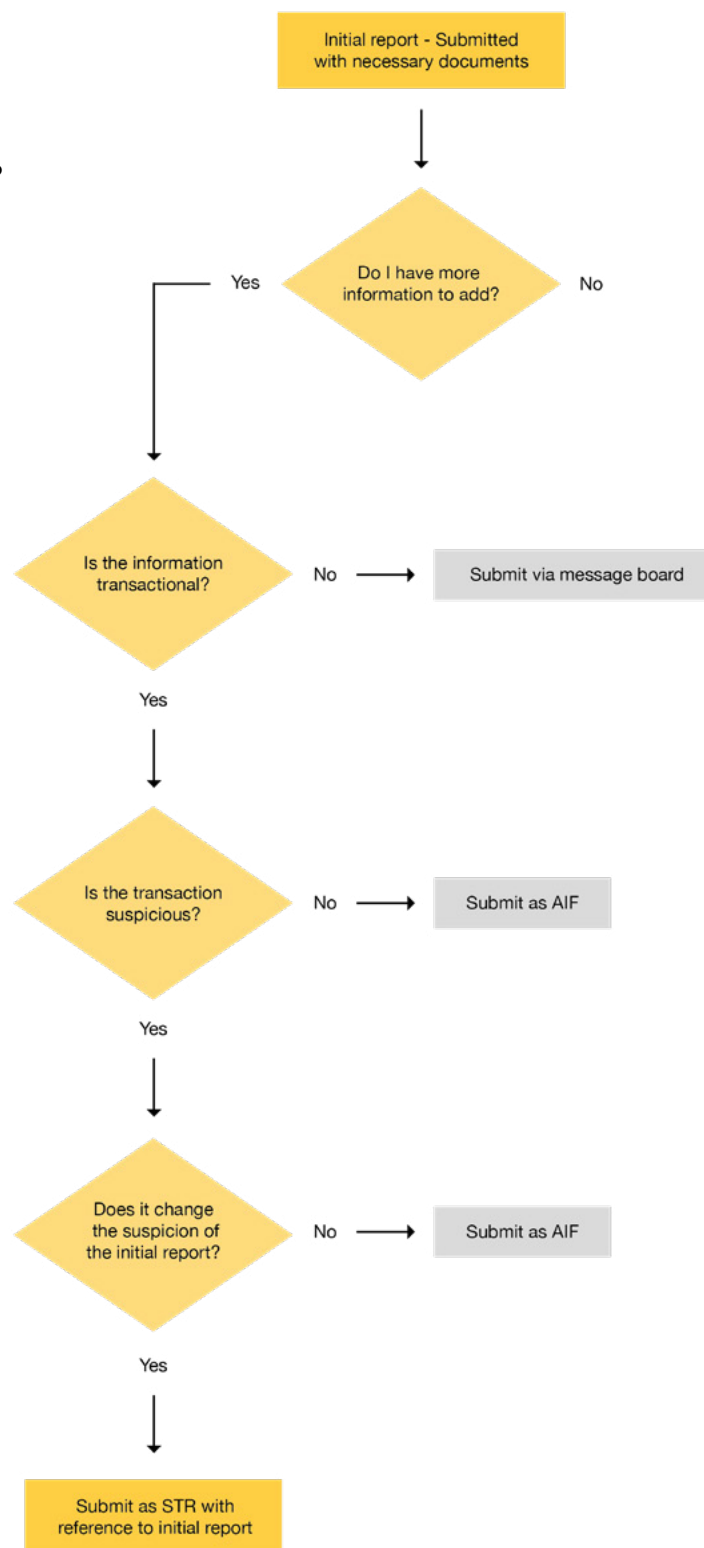
Ex 1. Customer's account activity is in line with their established profile however, adverse information was discovered through open sources. Although there is no transactional activity that is evidently linked to the adverse information found the SP should evaluate all the information held and obtained and consider submitting an SAR. In this case, the transactional activity, although not suspicious, should be submitted as an AIF.

Ex 2. Adverse information on a potential customer was identified at on boarding stage. As a result of this, the client was not on boarded. Although the business relationship was not established and no transactions took place, a SAR should be submitted, due to the fact that the decision not to onboard was based on the knowledge or suspicion of ML/FT and not as a result of a suspicious transaction.

Ex 3. In January 2020, a SP submitted an STR about a company on tax evasion suspicions since a discrepancy was identified between the financial statements and the respective company's bank account(s). All the relative documentation was submitted at this stage. Fast forward November 2020 and the SP was informed that the company's UBO is adversely known for being involved in an organised crime group. In this circumstance, the suspicion has now changed and thus, a new SAR is to be submitted referring to the previous report in the narrative. Despite submitting a SAR, transactions for the past five years are required to be submitted as an AIF even though the transactions seem to be in line with the company's objectives.

When to submit a PEPR/PEPTR?
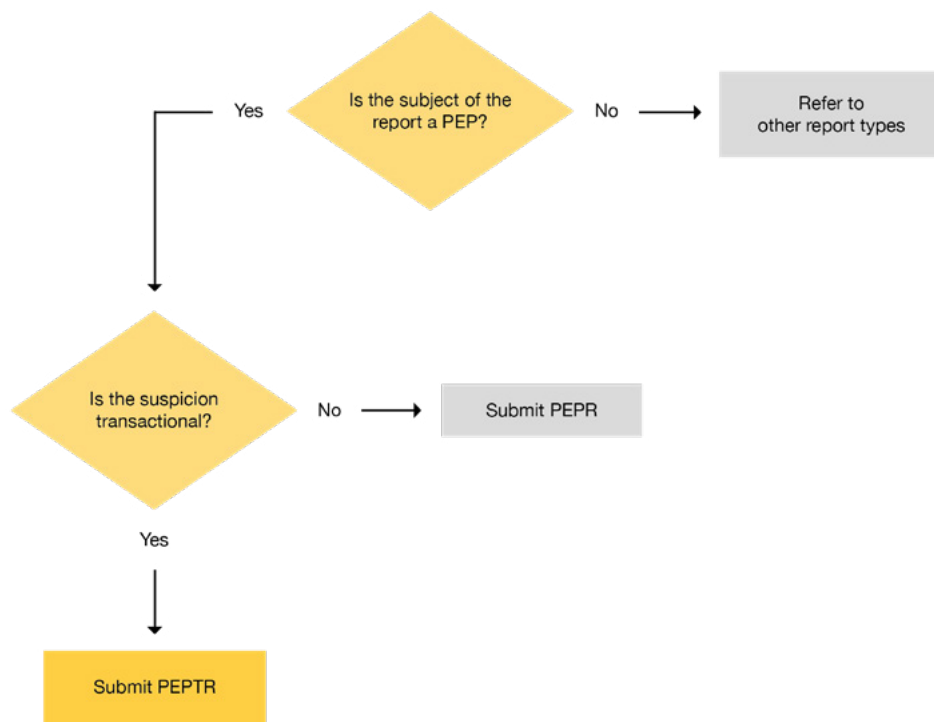
Ex 1. A foreign PEP set up a company in Malta. Although the transactional activity carried out within the accounts of this company were deemed to be in line with the expected business activity of the company, open-source information indicated that the PEP was subject to an investigation on charges of corruption in his respective country. In this case a PEPR is to be submitted which is an activity-based report and contains no transactional information. An AIF including all transactional activity is to be submitted in conjunction with the PEPR.

When to submit a TFR?

Terrorism Financing Reports are to be submitted when there is suspicion of terrorist financing activities. This report is predominantly activity based and the suspicion does not arise from the actual transaction(s). This report type does not allow for the inclusion of suspicious transaction reporting.

When to submit a TFTR?

This report is to be submitted when there is a clear suspicion of terrorist financing, however the suspicion emanated from a transaction or series of transactions carried out by the reported natural or legal persons.

3. SUBMITTING REPORTS VIA goAML IN LINE WITH REGULATION 15(4) OF THE PMLFTR

The Financial Intelligence Analysis Unit (FIAU) is issuing this guidance note to SP to advise them on the best practice to be adopted when submitting reports via goAML in line with Regulation 15(4).

Transaction Report (TRN) Category on goAML

The TRN category also prompts a pending transaction but such category shall be adopted in the following circumstances:

1. Where the SP has already submitted a report with the FIAU, however at a later stage, the SP was informed that the subject of the report wanted to move the funds. Thus, at this point the SP would currently be refraining from carrying out a transaction.

   In these circumstances, SPs who have already submitted a report, need only submit a TRN report. This TRN would be subsequently linked to the previous report and considered by the FIAU altogether. Additional documentation can also be submitted through the TRN report. In which case, there is no need to submit an AIF.

2. Where the SP is faced with a pending transaction or alternatively as commonly referred to a transaction in line with Regulation 15(4) of the PMLFTR, then at that point in time the SP is to submit a report (i.e., PEPR, TFR, SAR, STR), choosing from one of the above categories. In turn, the SP must also highlight the said pending transaction within the narrative of the report as well as part of the reporting indicators.

   In addition to the above, apart from submitting a report, a SP must also submit a TRN report highlighting the amount of each pending transaction, the details to where the funds are moving to and include an indicator. Once again, the said TRN would then be linked to the report and considered by the FIAU altogether. Additional

documentation can also be submitted through the TRN report. In which case, there is no need to submit an AIF.

It is imperative to highlight that when faced with more than one suspicious transaction for the same client, the SP should take note of the guidance note published by the FIAU on 24/03/2022 titled 'Update: Submitting reports via goAML in line with regulation 15(4) of the PMLFTR'.

By way of Example: A client wants to carry out 2 transactions which are being considered as suspicious. Upon reviewing the account, other suspicious transactional activity is identified. In such case the SP should report the STR detailing the suspicious activity which already took place, an AIF with details of the account activity which was not suspicious and a TRN.

Important
- It is important to mention that SPs refraining from carrying out a transaction in line with Regulation 15(4) of the PMLFTR, must upon submission provide the FIAU with the respective transactional details to where the funds are moving to, the suspicion identified in relation to the transaction being reported and any related supporting documentation.
- A report indicator needs to be created on all report types to be able to identify a pending transaction in the report in line with Regulation 15(4) of the PMLFTR.
- For additional guidance on TRN reporting, kindly also refer to the Guidance Document issued on 24th March 2022.

4. FURTHER CLARIFICATIONS IN RELATION TO XML UPLOADS

The main focus of this section will be primarily on the following criteria and field types:

- Source party (from) types and Destination party types (account, entity and person)
- Transaction modes (ATM, Electronic transaction, In-Branch/ Office, Other, Remittance)
- Beneficiary (to) Details (credit card number, account number, IBAN)
- Remote Gaming Accounts

Party Types: Source Party Types and Destination Party Types

Kindly find below examples of when "Account", "Entity" and "Person" are to be used in the party type:

Transaction Mode	Source Funds Type	Source Party Type	Destination Party Type	Destination Funds Type	Transaction Description
ATM	CASH	PERSON	ACCOUNT	DEPOSIT	Cash deposit
ATM	WITHDRAWAL	ACCOUNT	PERSON	CASH	Cash Withdrawal
POS	ELECTRONIC FUNDS TRANSFER	ACCOUNT	ACCOUNT	ELECTRONIC FUNDS TRANSFER	POS Payments
ONLINE	ELECTRONIC FUNDS TRANSFER	ACCOUNT	ACCOUNT	ELECTRONIC FUNDS TRANSFER	Online Payments
IN-BRANCH/OFFICE	CHEQUE	ACCOUNT	ACCOUNT	DEPOSIT	In house cheque deposit
IN-BRANCH/OFFICE	CHEQUE	PERSON	ACCOUNT	DEPOSIT	Other cheque deposit
IN-BRANCH/OFFICE	CHEQUE	ACCOUNT	PERSON	CASH	In house encashing of cheques
IN-BRANCH/OFFICE	CHEQUE	PERSON	PERSON	CASH	Other encashing of cheques
IN-BRANCH/OFFICE	CASH	PERSON	ACCOUNT	CASH	Other encashing of cheques
IN-BRANCH/OFFICE	WITHDRAWAL	ACCOUNT	PERSON	CASH	Branch Cash Withdrawal
REMITTANCE	MONEY ORDER	PERSON	ENTITY	ELECTRONIC FUNDS TRANSFER	Remittance not involving a bank, involving a money order to a company
REMITTANCE	MONEY ORDER	PERSON	PERSON	ELECTRONIC FUNDS TRANSFER	Remittance not involving a bank, involving a money order to a company
REMITTANCE	MONEY ORDER	ENTITY	PERSON	ELECTRONIC FUNDS TRANSFER	Remittance not involving a bank, involving a money order to a company
REMITTANCE	MONEY ORDER	ENTITY	ENTITY	ELECTRONIC FUNDS TRANSFER	Remittance not involving a bank, involving a money order to a company
ELECTRONIC TRANSACTION	ELECTRONIC FUNDS TRANSFER	ACCOUNT	ACCOUNT	ELECTRONIC FUNDS TRANSFER	Account to Account wire transfer such as a SWIFT payment – SP to include respective narrative

FIAU | Financial Intelligence Analysis Unit

Important: Kindly note that following this guidance note a new value will be added to funds code "from_funds_code" and "to_funds_code" as indicated hereunder.

Value	Description
W	Withdrawal

Also, please note that the following will be added to transaction mode code ("transmode_code"):

Value	Description
G	POS
H	Online

The above can be used to specify POS and online transactions.

Counterparty Details

In cases of credit card payments:

- The Source Party Type and Destination Party Type should always be account to account.
- If the reporting entity is the credit card issuer, and the linked bank account is known, then all the details linked to the credit card should be included in the transaction details.
- If the reporting entity is not the credit card issuer, then the account details should only include the credit card number and any additional details on the merchant, if available. One must keep in mind that any available data which could add value to the analysis would be appreciated.
- The Source Party Name or Destination Party Name should always reflect the name of the Card or Account Holder.

It is pertinent to also highlight, that no field should be filled in with a constant value such as "000" or "N/A" as this does not represent any information and would not add value to the analysis. Furthermore, the data inputting in such fields will be incorrect. If for instance five different accounts have "N/A" as source party name, than when a search is carried out by "N/A" from an analyst's perspective, more than one account will be linked to the person "N/A". As a result, the inputted data is invalid, incorrect, and useless given that it will ultimately portray the wrong classification and aggregation of data.

In relation to account details, if the reporting entity is the account issuer, then all details related to the account should be updated thus, account name, primary account holder, signatories, dates, balances, account type etc.

Remote Gaming Accounts

Although transactions which are carried out in remote gaming accounts differ from credit/financial institutions, fields should not be filled up as follows: "unknown", "N/A" and "000". A remote gaming account should still be considered as an "account" party type, with the details being the remote gaming account number. Source or Destination Party Types should reflect the account, wallet or credit card from where funds are being deposited or otherwise withdrawn respectively.

The gaming history/betting history, must be sent in excel format and transactional data for deposits/withdrawals in the gaming account is to submitted only in XML.

What is the difference between currency_code_local in report_node and currency_code in t_account node. And when do we use the foreign currency node? This question refers to the difference between the currency at the top of the report vs the account currency.

The currency_code_local is stored in the c_application_ defaults table serves as the base currency of the country. It is auto populated in a web report at the time of report creation. The currency code at the account level is the currency of the account. One can open a USD account at any bank in Europe so the currency code at account level serves that purpose. The foreign currency node is used when a transaction for example, is carried out in another currency compared to the currency of the account's currency. In this case, the reporting entity (RE) must report the transaction with its actual details including the use of foreign currency along with the rate of conversion on that particular day.

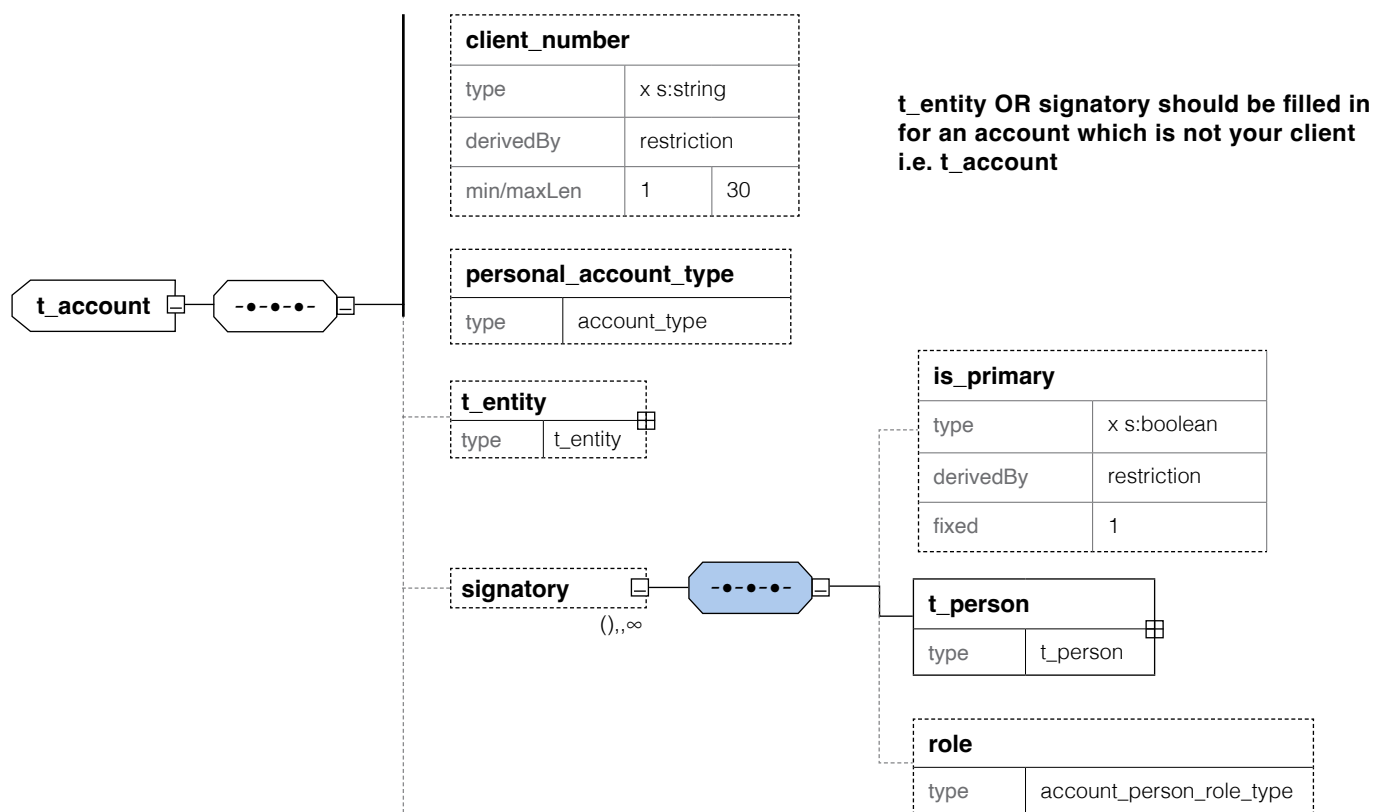**Rejection Rules**

Local Currency Code ("currency_code_local")
It is important to note that as also highlighted in the technical documentation provided on the goAML portal, the field named "currency_code_local" should always be Euro, in the case this is provided as another currency via XML than the report will be marked for rejection automatically.
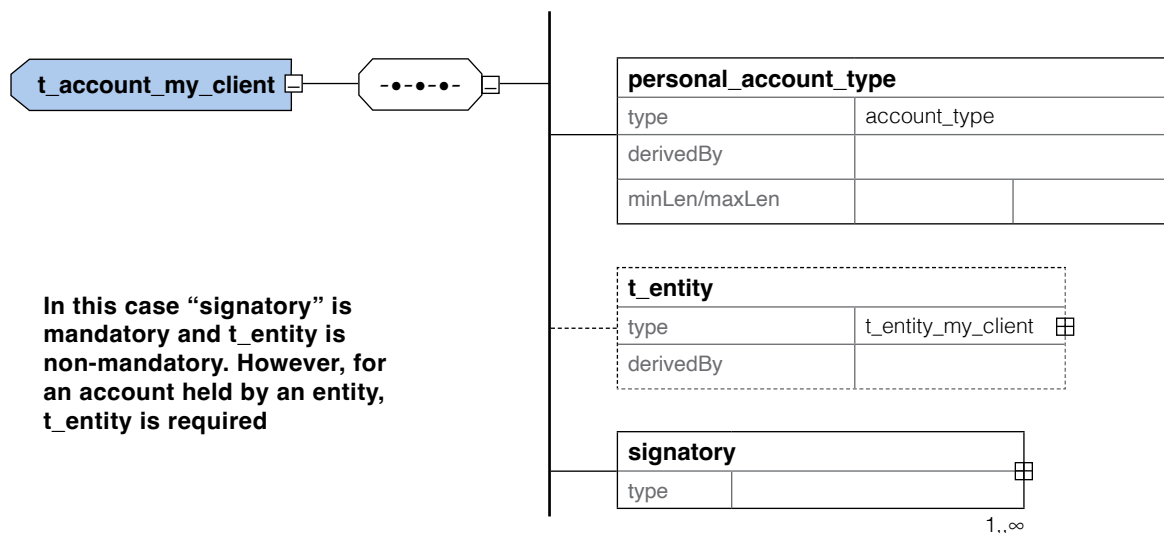
Banks and Financial Institutions Issuing IBANs
In case of transactions involving the "Account" party type either for destination or source should always include the account holder of the account. In the case of an entity holding the account "t_entity" should be filled with at least the mandatory fields which depend on whether the account pertains to the reporting entity's client or not.

If the account is held in the name of a natural person then "signatory" should be filled in as indicated in the charts hereunder. For accounts which are listed as not the reporting entity's client (i.e., t_account) then a signatory or an entity is required on submission.

For accounts of a client of the reporting entity (t_ account_ my_client), signatory is a mandatory field, however if the account is held by an entity, "t_entity" would be required.

t_entity OR signatory should be filled in for an account which is not your client i.e. t_account

client_number	
type	x s:string
derivedBy	restriction
min/maxLen	1	30

personal_account_type	
type	account_type

t_entity	
type	t_entity

signatory	
()., ∞	

is_primary	
type	x s:boolean
derivedBy	restriction
fixed	1

t_person	
type	t_person

role	
type	account_person_role_type

In this case "signatory" is mandatory and t_entity is non-mandatory. However, for an account held by an entity, t_entity is required

personal_account_type		
type	account_type	
derivedBy		
minLen/maxLen		

t_entity		
type	t_entity_my_client	
derivedBy		

signatory	
type	

1,,∞

Report Indicators

In case of reports with no indicators (node: "report_indicators"), the FIAU will automatically mark this report for rejection. Report indicators are extremely important in order to prioritise reports, identify particular typologies and for statistical purposes amongst many other reasons.

This rejection rule will be applied to all report types **except** AIFs.

Other Remarks

- Apart from what was highlighted earlier on, further distinction needs to be made between the details provided in terms of 'Not My Client' and the 'My Client'. It is a known fact that the details and transactional data available for 'My Client' should be more in comparison to the details and transactional data pertaining to the 'Not My Client'.

- It is also pertinent to highlight that when submitting an AIF via the XML Schema, SP have to make sure to include the FIAUs reference number pertaining to the initial request for information or otherwise report.

- The goAML XML Upload has an embedded feature which allows more than one XML file to be uploaded together. This is possible by attaching and compressing each XML file into one ZIP file.

ZIP files are used to group together XML reports and attachments to upload as one file. The files inside the zip file must be structured in a specific way to be accepted by the goAML Web application. The zip file must contain one of the following file arrangements

- A single XML file with zero or more non-XML attachments
- Multiple XML files with no attachments
- One or more folders that each contain;
  One XML file with zero or more non-XML attachments

It is pertinent to also point out, that zipping multiple XML files is allowed and recommended ONLY in those instances where more than one XML file relates to the same FIAU reference.

In the case of any additional queries in terms of transactional activity reporting or otherwise XML Schema submissions, kindly refer to:

1. The Technical Documentation on the FIAUs website: **https://fiaumalta.org/report-a-suspicion/** or
2. Send the FIAU an email on: **goAMLsupport@fiumalta.org**, **goAMLtechnical@fiumalta.org** or **technical@fiumalta.org**