POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

# Regulation on the Technical Form and Substance of Report Submission

**Financial Intelligence Unit (FIU) Finland**

Operative issues: rahanpesu.krp@poliisi.fi / +358 295 486 822

Techinical issues: rahanpesuilmoitukset@poliisi.fi / +358 295 486 833

# Contents

# 1 Introduction

This Regulation specifies requirements for the obliged entities defined in the Act on Preventing Money Laundering and Terrorist Financing (444/2017) concerning reporting to the Financial Intelligence Unit Finland (Rahanpesun selvittelykeskus, hereafter “FIU”).

This regulation is based on the Act on Preventing Money Laundering and Terrorist Financing (chapter 4 section 2 subsection 4), and therefore affects all obliged entities.

The correct technical form and requirements regarding sufficient substance of reports submitted by obliged entities are vital to the FIU in performing its legislative duties. Therefore, the obliged entities will be mandated by law to fill out and submit their reports to the FIU in a specific format specified in this Regulation.

In the following chapters, detailed requirements and instructions regarding the technical form and substance of the reports submitted to the FIU are specified. Failure in complying with this regulation will result in an automatic rejection of the report in question.

Depending on the scale and recurrence, failure in complying with this Regulation may lead to supervisory measures.

This Regulation will enter into force on 11.08.2025.

# 2 General Reporting Procedure

All reporting must be conducted through the goAML Financial Intelligence Unit - Web Application (hereafter “reporting application”), unless the obliged entity is able to demonstrate specific reasons for not utilizing the reporting application, in which case reports may also be submitted by using another encrypted connection or secure procedure. The requirements specified in this document apply to all submitted reports unless stated otherwise by FIU Finland.

The reporting application is available at https://ilmoitus.rahanpesu.fi/Home. Specific instructions for submitting reports are available for all registered reporting entities after logging in to the reporting application.

## 2.1 Registration

To create a report, the obliged entity has to be registered as an organization on the reporting application. Only the obliged entities defined in the Act on Preventing Money Laundering and Terrorist Financing (444/2017), chapter 1 section 2 can be approved as reporting entities.

After an approved registration, the user can log in to the reporting application.

Each reporting entity must have at least one reporting person as a user. Reporting credentials are for personal use only, and shared credentials are strictly prohibited.

Each organization with a unique incorporation number must be registered as separate entities. However, it is possible to delegate a reporting entity to conduct all reporting of a corporation’s different companies. The delegated organization may create delegating entities on the reporting application.

## 2.2 Reporting Methods

There are two different reporting methods.

1. **Manual (web) reporting:**
   The report is filled out manually on the reporting application.

2. **XML submission:**
   A complete XML file is uploaded on the reporting application.

Typically, filling out a web report manually takes more time than creating an XML report. It is advisable for entities submitting extensive amount of reports to use a tailored XML report to significantly reduce workload. Please note that in order to begin XML reporting, an XML implementation process must first be initiated with the FIU.

All requirements specified in this regulation apply to both manual and XML reports.

Detailed instruction manuals for both manual and XML reporting are available on the report application site. FIU Finland provides user support via phone and email, see details on the title page.

## 2.3 Rejection of insufficient or erroneous reports

With this regulation, FIU Finland reserves the right to reject insufficient or erroneous reports. The requirements specified in this document are reasons for rejection.

Reports can be rejected in two different stages:

1. The report is missing information required in the reporting application and cannot be submitted;

2. The report is successfully submitted but rejected upon integration (when parsing of the incoming report and integrating into the FIU database) due to FIU rejection rule(s).

Submitted reports are pending approval before FIU integration.

A report submission is successful once the reporting entity receives a notification stating “Report Fully Accepted”. Before this, a submitted report may still be unaccepted and rejected.

Once a report is rejected, “Report Rejected” notification with the specified reason for rejection is sent. The report status will change to “Rejected” on the reporting application.

Reporting entities utilizing the manual web reporting may edit the rejected report to make the required changes and complements. After the corrections, the report can be resubmitted.

If the rejected report is in an XML file form, the required changes need to be made in the file itself. The initial report is not reversible and a completely new report has to be submitted.

# 3 Report Attributes (Nodes)

There are some basic concepts and report attributes (later: nodes) that are useful to understand before initiating the reporting process. All report types are presented in chapter 4.

## 3.1 Party, My Client and Unknown

All reports, whichever type or category, include at least one party: person, entity or account. In most cases, at least one of the reported parties is a client of the reporting entity (later: my client). As the reporting entity is legally obligated to know their customer, certain information about the client must be disclosed to the FIU upon reporting. The required minimum information for each party is specified later (starting from chapter 5) in this document.

For entities that are not clients of the reporting entity (later: non-client), the requirements are less strict. Note that it is not allowed to report a party as non-client if the party factually is a client. Failure to report a client as non-client is a reason to reject a submitted report. However, some exceptions on this rule apply when submitting entities that are not, de-facto, suspicious counter-parties of the report. Please check these exceptions in Chapter 8.1.3 Entity.

If the reporting entity has basic information about a non-client party, the party is known and it should be reported. The minimum information for each non-client party is:

**Person**: first name, last name. The default birthdate of non-client is “1.1.1900”.

**Entity**: name.

**Account**: account number and BIC/SWIFT

If there is less information about a party available, the party is technically unknown and should not be reported as a party. Instead, a reporting entity may provide the relevant information in the Reason node (see Chapter 5). Please note that it is not allowed to use dummy values (“- “, “un-known”, “x” etc.) to replace these parties. A report with dummy values will be rejected.

## 3.2 Transaction-based and Activity-based reports

As the XML scheme is in a specific form, all report types follow the same basic structure. De-pending on the report type, there are differences between which nodes are required or even available for filling out.

A suspicious activity report can either be transaction-based or activity-based. If there are trans-actions or attempted transactions involved in the suspicious behavior, they must be reported. However, there may also be suspicious behavior which does not include any transactions, but for example a suspicious request regarding an assignment. Therefore, report parties (person, entity, account) are reported either as part of a transaction(s) or as part of suspicious activity, depending on the report substance.

Whenever there is a monetary transaction or an attempt of monetary transaction involved, the reporting should always be conducted as transaction-based. The transaction in question is the

main substance of a transaction-based report. The report should also include all relevant information regarding the parties involved. In general, a transaction contains information about the party roles, amount and status.

The majority of data received by the FIU via reports from obliged entities is transaction-based. High quality transaction data is vitally important for the FIU's analysis function.

Activity-based reports consists of the parties only and do not include the option to fill out transaction details. Note that it is not allowed to report suspicious activity as “activity” if there is a transaction involved. Failure to report a transaction correctly is a rejection reason for a submitted report.

## 3.3 Report Nodes

All report elements have nodes that are obligatory while others are optional. Obligatory fields are separately marked in the web application with an asterisk (*). The reporting entity should always aim to fill in all available information instead of the required minimum.

Some nodes are obligatory if they are active on the report. For instance, if the PEP node is activated by the reporting entity, it has to either be filled out or deleted completely in order for the report to be valid for submission. In the reporting application, the fields are required upon activation. Similarly in XML, a node requires filling out once it is included in the file.

Some of the nodes, however, are obligatory to fill out even though they are not technically required by the reporting application or the XML schema. Continuing with the PEP node as an example, if the reported person is in fact a PEP, the information has to be reported to the FIU. Failing to report this information is a rejection reason for a submitted report. This Regulation, the web application and user manuals help you to fill all obligatory fields.

# 4 Report Types

Reporting starts by choosing the correct report type. Please pay attention in this phase, since it defines the entire reporting process. There are three basic reporting categories available for reporting to FIU Finland. The categories are risk-based, threshold and background reporting. The categories consist of six different report types: four for risk-based reporting and one for threshold reporting and background reporting, respectively.

## 4.1 Suspicion-based (Suspicious Activity and/or Transaction) reporting

Risk-based reports concentrate on reporting only the essential transactions and parties (STR or TFRT) or parties (SAR or TFRA) related to a suspicious incident. All clients of the reporting entity must be listed as my-clients. There are no exceptions to this rule.

In this category, report structure can be based on either transaction or activity. These reports can be submitted both manually and as an XML file submission.

**Transaction-based reporting**

**STR:** Suspicious Transaction Report. This report type is for reporting suspicious activity which includes at least one suspicious transaction or a transaction attempt (when details of the attempted transaction is known to the reporting entity). STR is the most common type of risk-based report.

**TFRT:** Terrorism Financing Report, includes transactions. Identical to STR in technical details, TFRT is only for reporting transactions related to terrorism financing. TFRT must include at least one suspicious transaction.

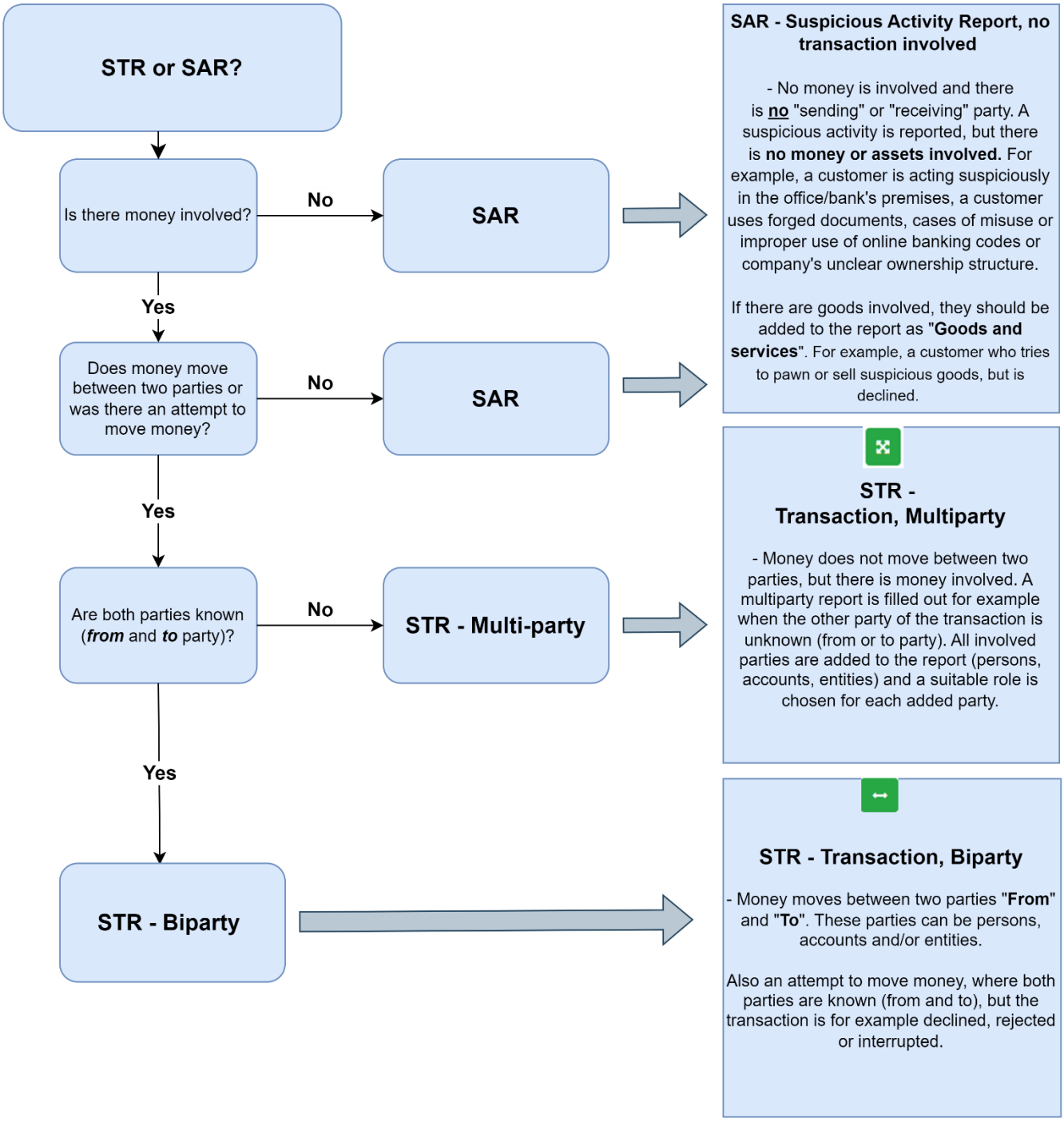
**Activity-based reporting**

**SAR: Suspicious Activity Report.** This report type is for reporting suspicious activity that does not include any monetary transactions. E.g. a SAR can be associated with suspicious behaviour of the customer in office space, usage of forged documents or unclear business or ownership structure of a company. If the activity includes even one attempted or conducted transaction, the correct report type would be STR.

**TFRA: Terrorism Financing Report, no transactions.** Identical to SAR in technical details, TFRA is only for reporting activity related to terrorism financing. Choose this report type if you are reporting suspected terrorism financing activities that do not include any monetary transactions.

Incorrect report type is a rejection reason for a submitted report. Incorrect choices typically occur within the risk-based category as transaction and activity-based reports get mixed up. STR and THR might also get mixed up.

The following flowchart instructs in choosing the correct report and transaction type for a suspicion-based report. For choosing a correct transaction type, please check chapter 7.


STR or SAR?
Is there money involved?
No
SAR
Yes
Does money move between two parties or was there an attempt to move money?
No
SAR
Yes
Are both parties known (*from* and *to* party)?
No
STR - Multi-party
Yes
STR - Biparty
SAR - Suspicious Activity Report, no transaction involved
- No money is involved and there is no "sending" or "receiving" party. A suspicious activity is reported, but there is no money or assets involved. For example, a customer is acting suspiciously in the office/bank's premises, a customer uses forged documents, cases of misuse or improper use of online banking codes or company's unclear ownership structure.
If there are goods involved, they should be added to the report as "Goods and services". For example, a customer who tries to pawn or sell suspicious goods, but is declined.
STR - Transaction, Multiparty
- Money does not move between two parties, but there is money involved. A multiparty report is filled out for example when the other party of the transaction is unknown (from or to party). All involved parties are added to the report (persons, accounts, entities) and a suitable role is chosen for each added party.
STR - Transaction, Biparty
- Money moves between two parties "From" and "To". These parties can be persons, accounts and/or entities.
Also an attempt to move money, where both parties are known (from and to), but the transaction is for example declined, rejected or interrupted.

## 4.2 THR: Threshold Reporting

Threshold report (THR) is for reporting single or combined transactions of a single person or a single account which exceed the threshold limit regulated in the Act on Preventing Money Laundering and Terrorist Financing. THR does not include suspicious activity. All threshold reports are transaction-based.

THR reports can be submitted both manually and as an XML file submission. However, typically THR reporters report in large quantities, and it is therefore advisable to implement XML reporting.

## 4.3 Background reporting: ATL – Account Transaction List

ATL is a report type that provides background information. It is a list of transactions either connected to a risk-based report or as a response to a FIU request for information. The background information is always related to a single account. Typically used in the banking sector, this report type closely resembles a bank statement. Transactions should not be double submitted as both STR and ATL. Since it requires agreement and implementation with FIU Finland, ATL reporting is for XML reporters only.

# 5 Specific Guidelines for Filling in Report Details

A report consists of several nodes which must be filled out correctly for the report to be successfully submitted. If the report is not filled out correctly, it will face rejection upon integration to the FIU register.

A report includes the basic and complementary information of the reported incident, as well as activity and/or transaction nodes. This chapter specifies the requirements for the basic information sections of the report: report headers, attachments, indicators and nodes related to goods and services. The following chapters then specify the actual substance of the report, from activity and transaction, fining down to report parties.

## 5.1 Report Headers

The report headers section includes the basic details of the report. The obligatory nodes for this section are:

**Reporting entity ID:** The entity ID for the reporting application. For manual reporters, the ID is integrated in the report.

**Submission code:** The value is always “IMP” (import) in XML. For manual reporters, the code is integrated in the report.

**Reporting entity reference number:** The reporting entity reference is a code which the reporting entity assigns for each separate report it has sent to the FIU. The reference number is obligatory in every report. It should be a running number or otherwise designed so that there are no two identical reference numbers within the same reporting entity.

**Report date:** The reporting date (when report finally submitted to the FIU).

**Local currency**: EUR. For manual reporters, the currency is integrated in the report. EUR value of the reporting date. If the transaction has been made in another currency, specify this in the currency node.

**Reason:** Reason is an obligatory field for all risk-based (suspicious activity) reports. The report cannot be submitted with the reason node empty. Insufficient information in the reason field is also a rejection reason, even if there is something filled in.

The node is used to describe why the suspicious activity is reported. It needs to form a clear idea of what is being reported and what the suspicious aspect is. There should also be an overview of the reported suspicious transactions, as well as a list of all the parties involved. All parties listed should be included in the report transactions or activity.

## 5.2 Attachments

Although not obligatory, it is recommended to share relevant customer information of the reported party, e.g. KYC information, bank statements, possible asset origin statements and other correspondence regarding the suspicious activity in question. If not apparent, please specify the relevance of the attachment to the reported case in the “reason” field of the report.

There is a maximum size limit in place for attachments. If the attachments exceed the size limit even after compressing the files, the reporting application message board may be used to send the missing attachments.

## 5.3 Indicators

It is obligatory to include certain indicators to all suspicious activity reports. THR and ATL reports do not require indicators. Insufficient indicators are a reason for report rejection. The following indicators are obligatory for each report type:

**STR/TFRT:**

- One indicator from the indicator class “amount” (S): the amount should refer to the activity in its entirety instead of a single transaction. Only one amount indicator is allowed.
- Minimum one other indicator: the indicators should be selected so that they accurately describe the reported suspicious activity. There is no maximum limit to the allowed indicators.

**SAR/TFRA:**

- Minimum one indicator other than “amount” (S): the indicators should be selected so that they accurately describe the reported suspicious activity. There is no maximum limit to the allowed indicators.
- If goods and services are reported, one amount indicator indicating their value.

The list of indicators with descriptions is available on the reporting application site for reference.

## 5.4 Goods and Services

The goods and services node is used for additional information related to the reported suspicious activity. It is used for specifying valuable items or equivalent goods and services involved.

The goods and services node can be a part of either a transaction or activity nodes, depending on the reported suspicious activity.

If activated, the minimum required information is:

**Item type:** Choose the correct item type from the lookup values.
**Item description:** Describe, what the item actually is. E.g. brand of the car, name of the piece of art.

**Estimated value:** Provided or estimated time value (in EUR) by the reporting entity.

It is advisable to add all available information of the reported goods and services on the report.

# 6 Activity Node - Adding Parties Involved

The activity node is available in all report types for suspicious activity. It is used for adding parties involved in the reported suspicious activity. Parties are reported as my client if the party factually is a client. Depending on the report type, the activity node has different methods of use:

**In action-based reports SAR/TFRA:** The activity node is used to add all involved parties to the report. This is the main source of information in these report types. At least one party must be added for the report to be valid for submission. However, all parties mentioned in the reason node should be added as parties under activity.

**In transaction-based reports STR/TFRT:** The activity node is used for complementing the report substance. All parties that are not part of the reported transactions, yet are relevant to the reported suspicious activity, should be added as parties under activity.

Failing to report parties as described above is a reason for rejection.

If the report includes goods and services which are not a part of a transaction, they should be reported using the activity node.

# 7 Transaction Types

Transactions are reported in the transaction node. All legally required information for transactions is listed in this chapter. Failing to choose a transaction-based report type (STR, TFRT) when there are transactions involved is a rejection reason for a submitted report.

Typically, at least one of the parties should be filled in as my-client. Failure to report a client as my-client is a rejection reason.

Although certain nodes are not obligatory in the reporting application schema, failing to provide information required in this document is a rejection reason. Insufficiently submitted report will be reverted for completion.

## 7.1 Choosing the Correct Transaction Type

There are two types of transactions, bi-party and multi-party.

**Bi-party transactions** is used when money or value moves between two parties or if the party is changing currency to another currency. Bi-party transactions always have two parties: source (from) and destination (to). The party can be a person, entity or account. As the standard transaction type, bi-party should always be chosen whenever applicable.

**Examples of bi-party transactions**

**Person → Person:** a cash transfer or currency exchange.

**Person → Account:** a cash deposit to an account.

**Person → Entity:** a money or value transfer, e.g. a company receives funds from a person in cash or whose account number is not known

**Account → Person:** a cash withdrawal from an account.

**Account → Account:** a monetary transaction.

**Entity → Account:** a money or value transfer, but the account information of the payer company is insufficient.

**Entity → Entity:** a money or value transfer, e.g. an insurance company receives funds from a company whose account number is not known.

**Entity → Person:** a salary is paid in cash by the company to the employee.

**Multi-party transactions** are mostly used when either of the parties is completely unknown (no name or account number).

With the implementation of activity-based reporting, multi-party should be selected as a transaction type fairly rarely. Before implementing the SAR/TFRA as report types, zero value transactions were used for reporting parties that were not a part of the actual transaction, but were

essential to the suspicious activity report as a whole. This practice has been replaced by SAR. Therefore, multi-party should always have an amount different than zero.

Essentially, multi-party should mostly be used as an exception. If both the source and destination of a transaction are known, choosing multi-party is a reason for rejection in most situations. If a reporting entity has technical difficulties in reporting a bi-party transaction, contact FIU for guidance.

## 7.2 Required Transaction Information

Regardless of the type, the following information is required for all transactions:

**Transaction Number:** A unique identifier for the transaction. In the banking sector, SEPA or archive number ideally. Other sectors may create a transaction number using the tool on the reporting application, or use another applicable unique identifier. For instance, in the virtual currency sector, the identifier would be the transaction ID ideally.

**Transaction date:** The actual date that the transaction was conducted, not the value date.

**Transaction type code:** Selected from lookup values.

**Transmode code:** Where or how the transaction has taken place. Selected from lookup values.

**Amount:** The amount is always reported in euros. If the transaction was conducted in another currency, the details are specified in *foreign currency* in the report party node. Note that as using activity node is current protocol, transaction amount can never be zero in either transaction type.

**Transaction status:** Whether the transaction is rejected, pending or completed. Selected from lookup values.

Bi-party transactions require **source (from)** and **destination (to)** parties to be valid for submission. The parties are selected according to the transaction details.

From

**From funds code:** Selected from lookup values. UNKNOWN is not allowed for my-client.

**From party:** Account, entity or person.

**From country:** The country of the transaction source. Finland is the default value in the reporting application.

To

**To funds code:** Selected from lookup values. UNKNOWN is not allowed for my-client.

**To party:** Account, entity or person.

**To country:** The country of the transaction destination. Finland is the default value in the reporting application.

Multi-party transaction requires at least one party to be valid for submissions. All relevant parties should be reported.

**Party role:** Selected from lookup values.

**Party:** The node for either person, person (my client), account, account (my client), entity or entity (my client) is selected accordingly. The required party information is filled in.

**Party country:** The country where the party is conducting the transaction or select UNKNOWN. In bi-party transaction, choose the country of the source and/or the destination of the transaction. In multi-party transaction, choose the correct country from *Involved parties - Country*. Finland is the default value in the reporting application.

**Party is suspected:** If the reporting entity considers a transaction party suspicious, e.g. a fraud destination account.

## 7.3 Special cases in submitting a transaction

There are some special requirements to consider when reporting certain types of transactions.

### 7.3.1 Card (non-debit card) payments:

Always a bi-party transaction, unless one of the parties is completely unknown. For example, a card payment in a specific store is illustrated as follows:

*From:* Card number

*To:* Entity or Person. Add the name of the web shop / shop / other party as the recipient of the transactions. Please, add the incorporation number to the entity information if the incorporation number is available. If the name of the recipient is not available, add the account number as the recipient of the funds.

### 7.3.2 Debit card payments

Always a bi-party transaction, unless one of the parties is completely unknown. For example, a card payment in a specific store is illustrated as follows:

*From:* Account number that is connected to the debit card. Report the debit card number in related accounts section.

*To:* Entity or Person. Add the name of the web shop / shop / other party as the recipient of the transactions. Please, add the incorporation number to the entity information if the incorporation number is available. If the name of the recipient is not available, add the account number as the recipient of the funds.

### 7.3.3 Collection accounts as a transaction party

A collection account (also known as a pooled account) refers to a single account managed by a reporting entity (e.g. a payment service provider) that holds funds for several different clients. Several different parties can make payments to the collection account, from which they are allocated to the correct client using an internal accounting system.

Always a bi-party transaction, unless one of the parties is completely unknown. For example, a wire transfer from bank account to a payment service provider's collection account.

*From*: Account number

*To*: If the reporting entity can identify that the payment is made to a specific person or business via a collection account, add the Person or the Business as the recipient of the funds. The account number of the payment service is then added to Activity node and the account type is selected as Collection Account.

If the reporting entity cannot identify a specific person or business from the transaction, add the account number of the payment service as the recipient of the funds and select the account type to Collection Account.

Please note that there are less requirements for submitting KYC information if the collection account owner is not a suspicious counterparty. This exception is explained in chapter 8.1.3.

# 8 Report Parties

There are six different choices available for report parties:

**Account** or **Account my client**
**Entity** or **Entity my client**
**Person** or **Person my client**

The party nodes are identical in technical form but my-client party always requires more information than non-client. Choosing non-client to simplify reporting when the party should be reported as my client is a rejection reason.

The reported party should be chosen depending on the reported subject. It is important to link all related parties together whenever possible, as this significantly improves the FIU analysis.

It is recommended to report the parties in the following hierarchy:

1. Account
2. Entity
3. Person

In transactions, account is always the primary report party. As accounts typically have related entities and persons, these related parties are filled in as a part of the account information.

There are strict requirements for the reporting entities to provide all necessary information about the account. However, if the reporting entity is not the account provider but the account holder is my-client, it is recommended to choose account non-client and fill in all available information instead of choosing person/entity my-client. This is the best practice for providing sufficient information, yet avoiding fictious values, which are a rejection reason.

If there is no account available, entity should be the main transaction party and its related persons linked in as a part of the entity.

## 8.1 Required party information

In this chapter, the requirements for Account, Entity and Person are specified. Some information is required only for my client. These requirements are marked with a star ★ in the following subchapters. However, it is recommended to fill in all available information regardless of the minimum requirements.

Some nodes have specific format restrictions defined by the FIU in the reporting application and the XML instructions. Incorrect format is a rejection reason for report submission.

If an information is underlined, it means that the information is always mandatory for my-clients and non-clients. If there is a ★ after the information, it means that the information is always

mandatory only for my-clients. If the information is not underlined or there is not a ★, it means that the information is mandatory only when the information is available.

### 8.1.1 Account

The following requirements apply to account information:

**Institution code or SWIFT:** For accounts of banking institutions, SWIFT is selected and the correct BIC/SWIFT code for the institution is filled in. BIC must correspond to IBAN. The BIC country code must correspond to the account country. For other types of accounts that do not have BIC/SWITF code, institution code is reported. This should be used together with "**non-bank institution**". For example: institution code for card numbers should be "CARD_BIN-number". Card BIN-number is the first six or eight numbers of the card number.

**Collection account:** If an account is a collection account of a financial institution, this information is filled in. Please see more specific instructions in chapter 7.3.3.

**Account category ★:** IBAN Account, a bank account, block chain account etc. Always in IBAN format, if technically possible. Another format of bank account number may refer to accounts outside of European Union or formats of some older, technical accounts. An account category is selected from lookup values.

**Account type ★:** Current Account, Savings Account, Collection Account etc. An account type is selected from lookup values.

**Account:** Account number is filled in with no spaces between characters. If the account is an IBAN account, no other format of the account number is accepted. The IBAN country code has to correspond to the account country.
Card numbers are filled in unmasked with no spaces between characters.
Virtual currency addresses are filled in with no spaces between characters.

**Entity:** Account-entity relation is submitted, if an entity is the account owner / holder. If the entity is my-client, all requirements for entity my-client apply.

**Account related person ★:** Person, role. All account owners and users are filled in with their roles. If the person is my-client, all requirements for person my-client apply. If the account owner is a non-client, it is still recommended to add them in as "unconfirmed".

**Related accounts:** Account relationship, account. The bank account related to a reported card is obligatory. Generally, if my-client account is related to another account relevant for the reported suspicious activity.

**Sanctions:** Provider, sanction list name. If a person or entity related to my-client account is on a sanction list which is binding *in Finland* (national, EU and UN sanctions) at the time of the report submission or reported events. Non-binding sanction list hit may be reported based on the risk assessment of the reporting entity.

**Note!** If the reporting entity can identify an account as a collection account, it is utmost important to report the account as collection account and choose the account type as “Collection Account”. In this case please do not report a person as the owner of the collection account. An entity can be reported as the owner if the reporting entity is absolutely sure that the entity is the owner of the collection account.

### 8.1.2 Person

The following obligatory requirements apply to Person:

**First name:** Current official first name or names (if several first names). If relevant, previous names can be added in the person previous names node.

**Last name:** Current official last name. If relevant, previous names can be added in the person previous names node.

**Date of birth ★:** Date must correspond to possible social security number ("SSN").

**SSN:** The Finnish SSN of a Finnish citizen is obligatory, when reporting entity has it. IF a non-Finnish citizens’ Finnish SSN is available, it is recommended to fill in. If my-client has no Finnish SSN, their nationality cannot be Finland. SSN must correspond to date of birth. No other country’s SSN or equivalent is allowed.

**Nationality 1 ★:** If my-client has no Finnish SSN, their nationality cannot be Finland.

**Phone:** When phone number is available**.** Phone type (home, mobile, work), communication type (mobile phone, fax, satellite phone etc), number. The accepted format: country code, area code without the first character (0) and the phone number all in one field with no spaces in between characters, e.g. +358401231231.

**Address ★:** Address type, address, city and country code. The Finnish postal service Posti (UPU) standard for addresses is recommended: street name, house number, apartment number, postal code, city, country.

**Identifications ★:** Type, number and issue country of the identification document or, in the case of non-face-to-face identification, data on the procedure or sources used in verification are obligatory for all my-clients. It is required to submit all of the identifications used in the reported suspicious activity. Recommended to fill in for other parties (non-my-client) as well.

**Politically exposed person (PEP):** Country (where the person is active at the moment), function name, function description. Obligatory for all my-client persons with a PEP status.

**Sanctions:** Provider, sanction list name. If a person related to my-client is on a sanction list which is binding in Finland (national, EU and UN sanctions) at the time

of the report submission or reported events. Non-binding sanction list hit may be reported based on the assessment of the reporting entity

**Related persons:** If the reported person e.g. has a trustee relationship, the trustee's information is obligatory. The rule of a trustee relationship also applies to adults as legal guardians of children under 15 years old.

### 8.1.3 Entity

The following requirements apply to entity:

**Name:** The complete official name of the legal entity.

**Incorporation legal form:** Selected from lookup values.

**Incorporation number:** Please insert only Finnish business ID numbers in this field. Please use the correct format, e.g. 1234567-8.
If my-client entity incorporation country is Finland, Finnish business ID is required.
If my-client entity is non-Finnish, the equivalent ID number is filled in *entity identification*.
Available tax numbers are filled in at *Tax number*.

**Entity status:** Current status from the business register.

**Address ★:** Address type, address, city and country code. The place of registered office address and the primary commercial address, if they differ.
The Finnish postal service Posti (UPU) standard for addresses is recommended: street name, house number, apartment number, postal code, city, country.

**Incorporation country ★:** Please fill in the incorporation country of the Entity. Obligatory for all my-clients.

**Related persons ★:** Person, role.

Every member of the entity board or equivalent management body with their name, date of birth and citizenships.

For beneficial owners, name, date of birth, Finnish SSN and citizenship (when SSN missing) are obligatory. When relevant, add the grounds for beneficial ownership role (e.g. share of ownership or voting rights or other grounds for exercising control).

**Entity identification:** Foreign business ID or equivalent. Type, number and issue country are obligatory for non-Finnish my-clients.

**Sanctions:** Provider, sanction list name. If an entity related to my-client is on a sanction list which is binding in Finland (national, EU and UN sanctions) at the time of the report submission or reported events. Non-binding sanction list hit may be reported based on the assessment of the reporting entity.

**Exception on reporting a non-suspicious counterparty as a non-client:**

Sometimes a reporting entity needs to report an entity (my-client) in a suspicious activity / transaction report even if the entity is not a suspicious counterparty. These entities are usually well-known customer companies or governmental agencies which are associated with a large amount of transaction flow. In this case reporting entities are allowed to report the entity as non-client and provide the following minimum information only:

- Incorporation number;

- Official name of the entity.