LA JUSTICE
Grand-Duché de Luxembourg

Cellule de renseignement financier (CRF)

goAML Indicators

New collaborative approach serving the national AML/CFT Framework – Part 1

Introduction

The fight against money laundering and terrorist financing depends on close and effective cooperation between reporting entities and the Financial Intelligence Unit (FIU). To reinforce this collaboration and address the increasing complexity of financial crime, this handbook introduces a new set of structured indicators designed to support reporting entities in the preparation of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs).

These indicators provide a comprehensive framework that organizes key elements of suspicion into categories[1] such as transaction patterns, triggers, typologies, sectors, products, and contextual factors. Depending on the specific circumstances of a case, multiple indicators may be selected, including several from the same category. In the initial phase, five categories will be available to reporting entities, the remaining categories will be introduced in a subsequent phase.

By selecting the relevant indicators, reporting entities enhance the clarity, precision, and consistency of their suspicion reports. This enables the FIU to analyze submissions more effectively, identify emerging typologies and trends, and share insights with the relevant sectors to reinforce awareness and preventive measures. Indicators should be chosen based on the factual elements and context described in the suspicion report. While their use is not mandatory, reporting entities are strongly encouraged to include them whenever they contribute meaningful context to the suspicion being reported.

For the FIU, the implementation of these indicators represents a noteworthy improvement to the processing of SARs and STRs. Indeed, improved readability and faster identification of red flags will strengthen the FIU's ability to prioritize cases based on risk, streamline report handling, and initiate in-depth analyses or investigations more efficiently where warranted.

This approach enhances the effectiveness of both parties: for reporting entities, it reduces uncertainty in the reporting process and promotes a more targeted, consistent, and defensible articulation of suspicion; for the FIU, it increases operational capacity to detect, prioritize, and process high-risk cases in a timely manner.

The handbook presents a series of illustrative case studies that demonstrate the practical application of the indicators. These examples are designed to assist reporting entities in effectively utilizing the new framework and to encourage the adoption of consistent, high-quality reporting standards across all sectors.

In conclusion, the handbook includes a Frequently Asked Questions (FAQ) section, which highlights common queries raised by reporting entities. The feedback received from these entities has been integrated into both the implementation of the indicators and the refinement of their descriptions.

Should you have any questions regarding the indicators, please feel free to contact us at crf_dd@justice.etat.lu.

[1] Categories have been set up in goAML to provide a systematic framework for classifying and select indicators under a unified pillar. This approach ensures clarity, consistency, and ease of reference. For example, indicators may be grouped within a *Predicate Offence* category or a *Trigger* category, thereby allowing reporting entities to navigate and apply the indicators in a coherent and organized manner under each category.

Indicators

Reporting Mode

The *"Reporting Mode "* category pertains to specialized reporting methodologies that fall outside the scope of conventional practices. These methodologies utilize predefined templates and require only the necessary documents as defined by the underlying reporting mode. Please ensure that the appropriate reporting mode is selected in alignment with the relevant underlying indicators.

Reporting light

Select if you are submitting your report under the Reporting Light mode. The Reporting Light mode may be used only in specific, predefined scenarios.

Trigger of suspicion

The *"Trigger of Suspicion"* category designates the specific element(s) or circumstance(s) that prompted the identification of potential concerns regarding an activity or transaction. These triggers serve as the initial basis for suspecting that the activity may be connected to money laundering or terrorist financing. When completing the report, please select the indicator(s) that most accurately correspond to the observed trigger(s).

Amount of transfer

Select if the suspicion concerns the amount of the transfer, where the sum is unusual, disproportionate, or inconsistent with the transaction's context.

Beneficial ownership issues

Select if the suspicion concerns situations where for example the true identity of the person(s) ultimately controlling or benefiting from a company, trust, or account is unclear, concealed, or deliberately misrepresented.

Cash transactions

Select if the report pertains to cash transactions, namely operations conducted using physical fiat currency.

Fraudulent transaction

Select if the suspicion concerns fraudulent transactions, including but without limitation, deceptive financial activities designed to secure unlawful gains.

Frequent transactions and in large amounts

Select if the suspicion concerns situations in which numerous high-value transactions are carried out within a defined period, including the frequency or scale of the transactions which appear unusual,

inconsistent with the customer's established profile, or disproportionate to its legitimate financial activities.

Frequent transactions and in small amounts (smurfing)

Select if the suspicion concerns situations in which numerous low-value transactions are carried out within a defined period. Although each transaction may appear insignificant on its own, the cumulative pattern can raise suspicion of smurfing.

Geolocation anomaly

Select if the suspicion concerns geolocation anomalies, such as the use of multiple VPN addresses originating from different locations or jurisdictions, or payments and transactions conducted in jurisdictions that appear inconsistent, suspicious, or unusual when compared to the registered address or the known profile of the customer or entity.

Impersonation Fraud

Select if the suspicion concerns identity theft fraud, like fraudulent activities in which a person impersonates someone else in order to deceive others for personal gain.

Inconsistencies regarding the business activity

Select if the suspicion concerns inconsistencies related to business activity. Such inconsistencies may reveal differences between an entity's declared business activities and the operations actually observed, including financial flows, business partners, or transactions that do not correspond to its sector, stated activity, or economic profile.

Inconsistencies regarding the economic origin of funds

Select if the suspicion concerns inconsistencies regarding the economic origin of funds, meaning discrepancies in the declared source of funds. This applies even in cases where information about the source of funds is incomplete or insufficient, yet inconsistencies are nevertheless identified.

Inconsistencies regarding the source of wealth

Select if the suspicion concerns inconsistencies regarding the source of wealth. This indicator refers to situations in which the information provided by a customer regarding the source of their wealth is for example ambiguous, contradictory, or insufficiently substantiated by appropriate documentation or evidence.

Inconsistencies regarding the KYC/KYT documentation

Select if the suspicion concerns inconsistencies in KYC/KYT documentation, for example discrepancies identified in identification documents, customer due diligence information, or transaction records provided, which may undermine the reliability of the customer's profile or raise concerns about the authenticity of the information submitted.

Involvement of minors

Select if the suspicion concerns the involvement of minors. This indicator concerns transactions or activities involving individuals who have not yet reached the legal age of majority.

No client response

Select if the client fails to respond or does not provide the requested information or feedback. This may include, but is not limited to, unanswered requests for documentation, lack of response to communication attempts, or failure to provide clarifications during ongoing procedures.

Non-respect of AML/CFT obligations by another professional involved in the business relationship

Select if the suspicion concerns non-compliance with AML/CFT obligations as applicable by another professional involved in the business relationship.

Non-transactional link with high-risk countries

Select if the suspicion relates to a non-transactional link involving countries identified as high risk for money laundering or terrorist financing.

Offshore based companies

Select if the suspicion concerns transactions or activities involving companies registered in offshore jurisdictions at any level. Offshore-based companies are businesses registered in a foreign jurisdiction, which might have been chosen for tax, regulatory, or confidentiality advantages.

Open-source information including adverse media

Select if the suspicion concerns indicators or information derived from open sources, meaning publicly accessible data that may point to a potentially suspicious activity.

Other Trigger

Select if the report concerns other triggers that do not correspond to one of the categories mentioned herein. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other Trigger: [description]*).

Phishing/pharming

Select if the suspicion concerns cases where a phishing attack has actually taken place or where there has been a clear attempt.

Politically Exposed Persons

Select if the suspicion concerns politically exposed persons (PEPs) as provided for in the provisions of the law of 12 November 2004 on the fight against money laundering and terrorist financing, the FATF recommendations and other applicable provisions.

Reluctance to provide KYC/KYT documentation

Select if the suspicion relates to a client's reluctance or refusal to provide KYC/KYT documentation, including mandatory identification documents, customer due diligence information, or required transaction records.

Sanctions lists

Select if the suspicion relates to sanction lists, namely transactions or activities involving natural or legal persons included on such national and international official lists.

Social media content

Select if the suspicion relates to social media content, namely information from those platforms that may reveal suspicious activities linked to ML/CFT.

Suspicious transaction pattern

Select if the suspicion concerns a recurring or structured set of financial behaviors or activities that deviate from normal, expected, or lawful transaction practices and may indicate potential money laundering, terrorist financing, or other illicit activity. Such patterns are identified for example through anomalies in transaction frequency, volume, counterparties, geographic routing, or structuring techniques, and are assessed in relation to the customer's profile, business activities, and the broader economic context.

Third party involvement

Select if the suspicion concerns activity in which a person other than the account holder or their authorized representative exercises control over the account or conducts transactions. This may include a family member, a business associate, a close contact, or any other individual.

Transactions to/from high-risk countries

Select if the suspicion concerns transactions involving countries identified as high-risk for money laundering or terrorist financing.

Transit account

Select if the suspicion concerns a transit account, that is, an account[2]used temporarily to transfer funds in order to conceal their illicit origin, often prior to transferring them to a final account or a legitimate investment.

Unusual behavior of the customer

Select if the suspicion concerns unusual client behavior, in relation, amongst others, to its transactions and/or actions which deviate from the client's normal profile and may raise suspicions of money laundering, fraud, or other illicit activities.

Use of forged documents

Select if the suspicion concerns the use of falsified documents, regardless of their nature or the context in which they appear.

Use of front persons/companies

Select if the suspicion concerns the use of front persons or companies, which refers to situations where individuals or entities act as intermediaries to conceal the true identity of the parties involved or the actual purpose of financial transactions or activities.

[2] For the purposes of this document, the term refers to any arrangements or tools that enable the holding, transfer, or control of monetary value or digital assets (e.g. bank accounts, e-money accounts, payment accounts, crypto wallets).

Use of informal networks to remit funds (hawala type)

Select if the suspicion concerns the use of informal fund transfer networks (such as hawala), namely parallel systems that are frequently unregulated and employed to move money outside official financial channels.

Public authorities request

Select if the suspicion arises from, or has previously been prompted by, a request issued by a public authority, such as law enforcement, judicial authorities (including an investigating judge, court, or public prosecutor), a regulatory body, or a supervisory authority.

Use of virtual assets

Select if the suspicion concerns the suspicious use of virtual assets, namely transactions involving digital instruments such as cryptocurrencies.

Suspected Predicate Offence

The *"Suspected Predicate Offence"* category identifies the underlying criminal offence(s) that are reasonably believed to be connected to the facts and circumstances described in the report. Reporting entities are requested, to the extent possible, to select the relevant predicate offence(s) from the provided list, based on the nature of the suspicion and the information available.

Corruption and bribery

Select if you suspect that the facts described in the report may be related to acts of corruption or bribery.

Counterfeiting and piracy of products

Select if you suspect that the facts described in the report may be related to counterfeiting or product piracy. These offenses involve for example the unauthorized reproduction, imitation, or distribution of goods, often in violation of intellectual property rights.

Counterfeiting currency

Select if you suspect that the facts described in the report may be related to currency counterfeiting.

Drug trafficking

Select if you suspect that the facts described in the report may be related to the illegal trafficking of narcotic drugs or psychotropic substances. This includes, but without limitation, for example the production, transport, distribution, sale, or purchase of controlled substances in violation of applicable laws.

Embezzlement of public funds

Select if you suspect that the facts described in the report may be related to the embezzlement of public funds.

Environmental crimes

Select if you suspect that the facts described in the report may be related to environmental offences.

Extorsion

Select if you suspect that the facts described in the report may be related to extortion, which involves for example obtaining money, property, or services through coercion, threats, intimidation, or abuse of authority.

Forgery

Select if you suspect that the facts described in the report may be related to forgery. This includes, without limitation, the falsification of documents, signatures, or other records, or the alteration of genuine documents with the intent to deceive or commit fraud.

Fraud individuals (Breach of trust)

Select if you suspect that the facts described in the report may be related to fraud involving a breach of trust. This occurs whenever for example someone in a position of confidence unlawfully exploits that trust to obtain a benefit for themselves or others.

Fraud individuals (Exploitation of vulnerability)

Select if you suspect that the facts described in the report may be related to fraud involving the exploitation of an individual's vulnerability.

Fraud individuals (Scam (including attempts))

Select if you suspect that the facts described in the report may be related to fraud in the form of a scam, including attempted scams. This includes, for example, deceptive schemes designed to defraud individuals or entities of money, property, or other assets.

Fraud involving subsidies, compensation, or benefits

Select if you suspect that the facts described in the report may be related to fraud involving for example the unlawful acquisition of public financial aid, such as subsidies, compensation, or social benefits. This includes attempts to obtain such aid through false declarations, forged documents, or misrepresentation.

Fraud legal entities (Fraudulent bankruptcy)

Select if you suspect that the facts described in the report may be related to fraudulent bankruptcy.

Fraud legal entities (Misuse of company assets)

Select if you suspect that the facts described in the report may be related to the misuse of company assets. This refers, but without limitation, to the unauthorized or dishonest use of corporate resources for personal gain or for purposes unrelated to the company's legitimate business.

Insider trading and market manipulation

Select if you suspect that the facts described in the report may be related to insider trading or market manipulation. These offenses involve for example the misuse of confidential, non-public information for securities trading or the artificial distortion of market prices to mislead investors.

Money laundering

Select if you suspect that the facts described in the report may be related to money laundering.

Other suspected predicate offence

Select if you suspect that the facts described in the report may be related to another criminal offence not explicitly listed in this category. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other suspected predicate offence: [description]*).

Proliferation financing

Select if you suspect that the facts described in the report may be related to proliferation financing. This offence refers, but without limitation, to the act of providing funds or financial services that directly or indirectly support the development, acquisition, or spread of weapons of mass destruction, including nuclear, chemical, and biological weapons, as well as their means of delivery.

Sanctions evasion

Select if you suspect that the facts described in the report may be related to the evasion of international, regional, or national sanctions, including the use of intermediaries or deceptive practices to circumvent restrictions.

Sexual exploitation of adults

Select if you suspect that the facts described in the report may be related to the sexual exploitation of adults. This includes, but without limitation, for example coercing or forcing individuals into sexual acts for financial gain, commercial advantage, or other benefits.

Sexual exploitation of children

Select if you suspect that the facts described in the report may be related to the sexual exploitation of children. This includes, but without limitation, any act involving the coercion, manipulation, or abuse of minors for sexual purposes, often for profit or gratification.

Smuggling

Select if you suspect that the facts described in the report may be related to smuggling. Smuggling involves for example the clandestine transportation of goods or substances across borders, in violation of applicable customs, tax, or trade laws.

Tax crime

Select if you suspect that the facts described in the report may be related to tax crimes, including aggravated tax fraud or tax evasion.

Terrorism and terrorist financing

Select if you suspect that the facts described in the report may be related to acts of terrorism or the financing of terrorism.

Theft and/or illegal trafficking of stolen goods

Select if you suspect that the facts described in the report may be related to theft or the trafficking of stolen goods.

Trafficking in human beings and migrant smuggling

Select if you suspect that the facts described in the report may be related to human trafficking or migrant smuggling. These offenses involve, but without limitation, the exploitation of individuals through coercion, deception, or abuse, and the illegal transportation of persons across borders.

Weapon trafficking

Select if you suspect that the facts described in the report may be related to the illegal trafficking of weapons. This includes for example the unauthorized manufacture, sale, transfer, or distribution of firearms, ammunition, or other arms.

Suspicious Amount

The *"Suspicious Amount"* category designates the aggregate monetary value of funds considered suspicious within the scope of the report. This amount must exclusively reflect transactions or activities that give rise to suspicion and should not encompass the total volume of financial operations conducted by the individual or entity concerned.

When calculating the suspicious amount, it is essential to avoid double counting. Specifically, incoming and outgoing flows associated with the same transaction or activity should be treated as a single instance, not as separate entries. This principle ensures the accuracy and consistency of the reported figures, as demonstrated in the illustrative examples provided below. Please select the range corresponding to the amount concerned.

Example 1: Money mule transaction

A money mule receives 10.000 EUR on their account and transfers this amount to another person. The suspicious amount to be reported in this case is 10.000 EUR.

Example 2: Real estate transaction

A person receives 5.000.000 EUR from a suspicious real estate deal. With these funds, the person purchases apartments, cars, and jewelry. The suspicious amount to be reported in this case is 5.000.000 EUR, as this represents the initial receipt of funds from the suspicious activity, even if subsequent transactions are carried out to obscure their origin.

A. 0 EUR

Select if no suspicious amount has been identified.

B. 1 - 5000 EUR

Select if the identified suspicious amount (after conversion) ranges from 1 EUR to 5.000 EUR.

C. 5.001-10.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 5.001 EUR to 10.000 EUR.

D. 10.001-15.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 10.001 EUR to 15.000 EUR.

E. 15.001-25.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 15.001 EUR to 25.000 EUR.

F. 25.001-100.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 25.001 EUR to 100.000 EUR.

G. 100.001-1.000.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 100.001 EUR to 1.000.000 EUR.

H. 1.000.001-5.000.000 EUR

Select if the identified suspicious amount (after conversion) ranges from 1.000.001 EUR to 5.000.000 EUR.

I. 5.000.001+ EUR

Select if the identified suspicious amount (after conversion) exceeds 5.000.001 EUR.

Time Elapsed

The *"Time Elapsed"* category denotes the duration that has passed since the most recently identified suspicious transaction. Kindly select the time range that accurately reflects this interval.

A. Less than 24h

Select if the last suspicious transaction occurred within the past 24 hours.

B. 24h - 48h

Select if the last suspicious transaction occurred between 24 and 48 hours ago.

C. 48h - 72h

Select if the last suspicious transaction occurred between 48 and 72 hours ago.

D. 72h – 2 weeks

Select if the last suspicious transaction occurred between 72 hours and 2 weeks ago.

E. Over 2 weeks

Select if the last suspicious transaction occurred more than 2 weeks ago.

Case Studies

Case Study 1:

John Doe SA, a company registered in Luxembourg, has been a client of our institution since 2019. It is purportedly engaged in asset management consulting. During the last quarter, our compliance department identified a series of unusual transactions on the company's business account, which triggered several internal alerts.

First, a suspicious transaction pattern was observed: multiple incoming transfers, each close to 24.000 EUR, were received from accounts located in low-tax jurisdictions. These funds were quickly transferred to third-party accounts outside the EU, without any apparent commercial justification. The beneficiaries are not recognized as known business partners of John Doe SA, and the outgoing transfers are often labeled with vague descriptions such as "service fees" or "consulting."

An analysis of the company's profile revealed that John Doe SA has no active website, its registered address corresponds to a coworking space, and its listed directors are also involved in several other companies with no real business activity. These elements suggest the use of a shell structure.

Additionally, an open-source search revealed that John Doe was mentioned in a local news article regarding an ongoing tax investigation for income concealment and false invoicing. Although the investigation is not yet concluded, this information reinforces the suspicion.

The total amount of suspicious transactions identified over a two-month period amounts to 87.500 EUR.

Finally, the observed transaction flows do not align with the declared business activity of asset management consulting. No contracts or supporting documentation were provided for either incoming or outgoing payments, and the movement of funds appears more consistent with transit operations than with the provision of legitimate services.

Selected indicators and justification:

- **Suspicion Trigger – Inconsistencies regarding the business activity:** The observed financial flows do not correspond to the declared asset management consulting activity and lack supporting documentation.
- **Suspicion Trigger – Inconsistencies regarding the economic origin of funds:** The origin of incoming funds from low-tax jurisdictions is unclear and unsupported by any legitimate commercial rationale.
- **Suspicion Trigger – Offshore based companies:** Several transactions involve entities located in offshore or low-tax jurisdictions.
- **Suspicion Trigger – Open-Source Information including adverse media**: Press articles mention John Doe in connection with a tax investigation, which contributes to the suspicion.

- **Suspicion Trigger – Suspicious Transaction Pattern**: The incoming and outgoing transfers follow a repetitive pattern, with similar amounts and unidentified beneficiaries, lacking economic justification.
- **Suspicion Trigger – Use of front Persons/Companies**: John Doe SA exhibits typical characteristics of a shell company: fictitious address, no real activity, and directors involved in multiple similar entities.
- **Suspected Predicate Offence – Tax Crime**: The financial flows and absence of supporting documentation suggest possible income concealment or false invoicing.
- **Suspicious Amount – 25.001-100.000 EUR**: The total amount of identified suspicious transactions is 87.500 EUR.

Case Study 2:

John Doe, a retail banking client since 2022, recently became the subject of suspicion following a series of unusual activities on his personal account. The case was submitted under the *Reporting Light* mode, as it falls within predefined scenarios where simplified reporting is permitted.

The first alert was triggered by a phishing attempt. John Doe reported receiving an email that appeared to come from our institution, requesting him to re-enter his login credentials. Shortly afterward, his account showed unauthorized access from foreign IP addresses. These logins were followed by multiple transfers to a newly opened account under his name.

This new account was quickly identified as a transit account. Several incoming transfers from unrelated third parties were received, each in amounts ranging between 20.000 EUR and 50.000 EUR. Within hours, the funds were moved onward to accounts in other jurisdictions. The account itself showed no legitimate business activity, reinforcing the suspicion that it was being used solely to obscure the origin of funds.

Further investigation revealed clear signs of third-party involvement. The transactions were executed at unusual hours, often late at night, and from devices not previously associated with John Doe. Supporting documents submitted during Know Your Transaction (KYT) procedures were inconsistent and appeared to have been prepared by someone other than the client.

Additionally, a copy of an identification document used to validate the transit account contained discrepancies compared to the original records on file. This strongly suggests that another individual impersonated John Doe to gain control of his accounts.

The total value of suspicious transactions identified during this period amounts to approximately 275.000 EUR. The last suspicious transaction was executed 29 hours ago.

Selected indicators and justification:

- **Reporting Mode - Reporting Light:** The report was submitted under the Reporting Light mode, as it falls within predefined scenarios.

- **Suspicion Trigger – Fraudulent transaction**: Multiple unauthorized transfers were carried out, constituting fraudulent financial activity.
- **Suspicion Trigger – Impersonation Fraud**: Falsified identity documents and inconsistencies in client data indicate impersonation.
- **Suspicion Trigger – Phishing/Pharming**: The client was targeted by a fraudulent email designed to capture his banking credentials.
- **Suspicion Trigger – Transit Account**: A newly opened account was used exclusively to channel funds before immediate onward transfers.
- **Suspicion Trigger – Third-Party Involvement**: Transactions were executed by unauthorized individuals, at unusual times, from unrecognized devices.
- **Suspicion Trigger – Use of forged documents**: The identification document used to validate the new account contained inconsistencies, suggesting the use of forged or altered documentation.
- **Suspected Predicate Offence – Fraud individuals (Scam (including attempts)):** The report involves fraud in the form of a scam, including phishing and impersonation attempts.
- **Suspicious Amount – 100.001–1.000.000 EUR**: The total value of suspicious transactions identified was 275.000 EUR.
- **Elapsed Time – 24h–48h**: The last suspicious transaction was executed 29 hours ago.

Case Study 3:

John Doe SA, a company registered in Luxembourg, has been a corporate client of our institution since 2018. The company declares its business activity as “international consulting services.” Over the past six months, our compliance monitoring team has identified a series of transactions and behaviors that raise significant suspicion.

The first red flag concerns the amounts of the transfers. Several large transactions exceeding 5 million EUR were initiated from John Doe SA’s account to entities located in jurisdictions subject to international sanctions. These amounts are disproportionate to the company’s declared business activity and far exceed its historical transaction profile.

Further investigation revealed that one of the ultimate beneficiaries of these transfers is a politically exposed person (PEP), currently serving as a senior official in a foreign government. The involvement of a PEP increases the risk of corruption and misuse of funds, particularly given the lack of transparency surrounding the transactions.

The structure of the transactions also suggests the use of front companies. Funds were routed through multiple intermediary entities, some of which are newly incorporated and have no identifiable commercial activity. These companies appear to serve only as conduits to disguise the true origin and destination of the funds.

In addition, there are clear beneficial ownership issues. Documentation provided by John Doe SA lists nominee directors and shareholders, making it impossible to determine the actual controlling party. The opacity of ownership raises concerns that the company may be concealing the involvement of sanctioned individuals or politically exposed persons.

We also identified inconsistencies in the declared economic origin of the funds. John Doe SA claims that the transfers are related to consulting contracts with foreign clients. However, no contracts, invoices, or supporting documentation have been provided. The amounts transferred are inconsistent with the company's declared turnover, and the counterparties do not appear to be legitimate consulting clients.

Moreover, screening against international databases confirmed that some of the counterparties involved in these transactions are listed on official sanctions lists. This direct connection to sanctioned entities significantly heightens the risk and strongly supports the suspicion of sanctions evasion.

Selected indicators and justification:

- **Suspicion Trigger – Amount of transfer**: The suspicious activity relates to unusually large transfers exceeding 5 million EUR.
- **Suspicion Trigger – Beneficial ownership issues:** The company's opaque ownership structure, relying on nominee directors and shareholders, prevents identification of the true controlling party.
- **Suspicion Trigger – Inconsistencies regarding the business activity:** The observed financial flows do not correspond to the declared activity and lack supporting documentation.
- **Suspicion Trigger – Inconsistencies regarding the economic origin of funds:** The claimed consulting contracts do not justify the amounts transferred, and no evidence of legitimate economic origin was provided.
- **Suspicion Trigger – Politically exposed persons (PEPs)**: One of the ultimate beneficiaries is a senior government official, classified as a PEP.
- **Suspicion Trigger – Sanctions lists**: Some counterparties are listed on official sanctions lists, directly linking the transactions to sanctioned entities.
- **Suspicion Trigger – Use of front persons/companies:** The funds were routed through intermediary shell companies with no real commercial activity, indicating the use of front structures.
- **Suspected Predicate Offence – Sanctions evasion**: The transaction pattern suggests deliberate attempts to circumvent international sanctions through layered transfers.
- **Suspicious Amount – 5,000,001+ EUR**: The total value of suspicious transactions identified exceeds 5 million EUR.

FAQ

In this section, we present the questions (Q) raised by the reporting entities together with the corresponding answers (A). The recommendations submitted by the reporting entities are not mentioned in this handbook; however, they have been duly acknowledged and incorporated as appropriate.

Trigger of Suspicion

Q: Does the indicator *"Amount of transfer"* apply to all suspicious transactions? Both debit and credit, as well as transfers and cash?

A: The indicator *"Amount of transfer"* should be selected when the suspicion specifically relates to the value of the transaction. This applies irrespective of whether the transaction is a debit, credit, transfer, or cash movement. The amount is considered suspicious if, in the context of the transaction, it appears unusual, disproportionate, or otherwise inconsistent with expected activity. Nevertheless, a double counting of debit and credit transactions should be avoided as explained further below in the category *"Suspicious Amount"*.

Q: We currently report negative balance cases resulting from failed SEPA Direct Debits under the *"Fraudulent transaction"* indicator. Is this sufficient, or should a more specific indicator be used? At present, the suggested list does not include any other indicator that could complement our report.

A: You may continue to use the *"Fraudulent transaction"* indicator for negative balance cases, while also applying the relevant indicator from the *"Suspicious amount"* category.

Q: It would be useful to define the terms "frequent," "numerous," and "large transactions."

A: The terms "frequent" and "numerous" refer to operations repeated within a short period and in high volume relative to the client's profile. Such activity may raise suspicions in the AML context.

Q: What is meant by *"Inconsistency/divergence in commercial activities*"? For example, flows unrelated to the activity, unauthorized transactions under the articles of association, or misuse of company assets?

A: This indicator highlights discrepancies between a company's declared business activities and the operations actually observed. Examples include financial flows, partners, or transactions that do not align with the company's sector, stated business activity, or economic profile.

Q: Lack of information regarding the economic origin of funds: In most cases, the subject/suspect is not our direct client (but rather the client of our client). We therefore lack immediate visibility on the

suspect's stated source of funds. In such cases, would it be more precise to use *"Lack of information regarding the economic origin of funds"* rather than *"Inconsistencies"*?

A: This indicator may also be used to report a lack of information regarding the source of funds. The definition has been updated accordingly: *"Select if the suspicion concerns inconsistencies regarding the economic origin of funds, meaning discrepancies in the declared source of funds. This applies even in cases where information is incomplete or insufficient, yet inconsistencies are nevertheless identified."*

Q: *"Involving minors"* does this apply at the level of originators/beneficiaries, or at the level of transaction wording/documentation, or otherwise?

A: The indicator should be selected when a minor is involved in a suspicious activity or transaction, regardless of the level of involvement.

Q: Additional clarity on certain terms used in the indicators would be helpful, such as *"Offshore-based companies."* Does this apply at the account holder level or to third parties?

A: The indicator *"Offshore-based companies"* should be selected when transactions involve entities registered in offshore jurisdictions, regardless of whether they appear at the account holder level or as third parties. Offshore-based companies are typically incorporated in foreign jurisdictions that are often chosen for tax benefits, regulatory arbitrage, or confidentiality purposes.

Q: Is *"Other Trigger"* a catch-all category if the situation does not fit within the available definitions? Must a free-text field be completed to provide details and prevent it from becoming a catch-all?

A: The *"Other"* trigger should be selected when the observed trigger is not listed. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other Trigger: [description]*).

Q: Should the indicator *"Phishing/pharming"* only be used for attempts? If actual fraud occurs based on phishing/pharming, should this be considered solely a fraudulent transaction?

A: The indicator *"Phishing/pharming"* should be selected if the suspicion concerns either an actual phishing/pharming attack or a clear attempt to carry out such an attack.

Q: What is the difference between the indicators *"Unusual behavior of the client"* and *"Suspicious transaction pattern"*?

A: The indicator "*Unusual behavior of the client"* refers to actions deviating from a customer's typical conduct (e.g., evasiveness, frequent changes of personal details) that may not directly involve illicit activity. The indicator "*Suspicious transaction patterns"* refers to financial movements such as structuring

deposits, transfers to high-risk jurisdictions, use of shell companies, or sudden spikes in transaction volume inconsistent with the client's profile.

Q: Would the "*Third party involvement*" indicator adequately reflect the cases of Account Takeover (ATO -when a customer's account has been compromised and a third party has taken over the control of the account)?

A: The indicator *"Third-party involvement"* refers to situations where a person other than the account holder or their authorized representative exercises control over the account or conducts transactions. This may include, for example, a family member, business associate, close contact, or any other individual. In the case of an account takeover (ATO), where a customer's account has been compromised and controlled by an unauthorized party, both the indicators *"Third-party involvement"* and *"Impersonation fraud"* should be selected.

Q: Indicator for connections to high-risk countries: Current indicators include *"Transactions to/from high-risk countries."* However, in practice we are increasingly observing cases involving connections to high-risk countries rather than direct transactions to or from such countries.

A: To address non-transactional connections with high-risk countries, a new indicator entitled *"Non-transactional links with high-risk countries"* has been created.

Q: Concerns related to documentation authenticity/legitimacy: We do not always know if a document is fully forged or only partially altered (e.g., signature altered).

A: The indicator *"Use of forged documents"* should be selected whenever there is a suspicion that a document has been falsified, whether in its entirety or only partially (e.g., an altered signature). This applies regardless of the type or nature of the document.

Q: Should we consider only the trigger element, or all suspicious elements found after investigation? Regarding requests received from authorities, should these be classified as *"Other"*?

A: All indicators that contributed to the decision to file the report should be selected, not only the initial trigger element. For requests received from public authorities, a dedicated indicator has been created. In such cases, please select the indicator *"Public authorities request."*

Suspected Predicate Offence

Q: Does *"Drug Trafficking"* include drug purchases and sales? Could this involve Darknet Markets?

A: The indicator "*Drug Trafficking"* encompasses all activities related to drug trafficking, including both the purchase and sale of drugs, as well as involvement with darknet markets. If darknet markets are implicated, the indicator "*Darknet Market Exposure"* from the category "*Crypto"* must also be selected. This category will be introduced in a subsequent stage.

Q: For negative balance cases resulting from SDD fraud, would the indicator *"Fraud – Individuals (Exploitation of Vulnerability, Breach of Trust, Scam, including attempts)"* be the most appropriate?

A: For negative balance cases, please select the predicate offence "*Fraud – Individuals (Scam, including attempts)".*

Q: Regarding the predicate offence *"Fraud":* does it concern fraud committed with our product, or fraud committed by our customer but not directly involving our product (e.g., adverse media or requests from authorities)?

A: It is strongly recommended to always select one or more suspected predicate offences when submitting a report. The suspected predicate offence must be directly related to the suspicion described in your report. It is not relevant whether the offence was committed using your product or another product.

Q: Recommendation to create a predicate offence called *"Identity Theft, Use of Stolen IDs and/or Card Payments."*

A: For this scenario, you may select the suspected predicate offence "*Theft and/or illegal trafficking of stolen goods"* and "*Impersonation Fraud"* from the category "*Trigger of suspicion".*

Q: Recommendation to classify the use of virtual assets under suspected predicate offences and select the relevant offence *"Money Laundering – Crypto Related" (*e.g., use of crypto assets, darknet markets, CSAM, money laundering).

A: For this scenario, you may select the related predicate offence and, from the category "*Product used for ML",* apply the indicator "*Crypto".* Additionally, from the category "*ML affected sector",* select the indicator "*Crypto-Assets Sector",* along with the relevant crypto-specific indicators. The categories *"Crypto",* "*Product used for ML"* and "*ML affected sector"* will be introduced in a subsequent stage.

Q: Recommendation to classify the use of virtual assets under suspected predicate offences and select the relevant offence "*Movement of stolen crypto funds*" (e.g., use of crypto assets, darknet markets, CSAM, money laundering).

A: For this scenario, you may select the predicate offence "*Theft and/or illegal trafficking of stolen goods".* In addition, from the category "*Product used for ML",* apply the indicator "*Crypto",* and from the category "*ML affected sector",* select the indicator "*Crypto-Assets Sector",* along with the relevant crypto-specific indicators. The categories *"Crypto",* "*Product used for ML"* and "*ML affected sector"* will be introduced in a subsequent stage.

Q: Recommendation to classify the use of virtual assets under suspected predicate offences and select the relevant offence *"Use of virtual assets – Rapid dispersal of funds (Crypto In > Out)"* (e.g., use of crypto assets, darknet markets, CSAM, money laundering).

A: For this scenario, you may select the related predicate offence and, from the category "*Product used for ML",* apply the indicator "*Crypto".* Additionally, from the category "*ML affected sector",* select the indicator "*Crypto-Assets Sector",* along with the crypto-specific indicator "*Instant withdrawal of funds (from crypto deposit")* from the category "*Crypto".* The categories *"Crypto",* "*Product used for ML"* and "*ML affected sector"* will be introduced in a subsequent stage.

Suspicious Amount

Q: Can we confirm that this refers to the amount reported in the STR/SAR, rather than the alerted numbers, which are only indicative and may include institutional accounts?

A: The *"Suspicious Amount"* category designates the aggregate monetary value of funds considered suspicious within the scope of the report. This amount must exclusively reflect transactions or activities that give rise to suspicion and should not encompass the total volume of financial operations conducted by the individual or entity concerned.

Q: In STRs related to SDD fraud, the primary financial impact is a negative balance on the account. Should the number reported under *"Suspicious Amount"* be the total value of this negative balance?

A: For negative balance cases, please select the indicator that reflects the total negative balance.

Q: A new indicator appears to be very beneficial on the sending/receiving side. Currently, a '0' suspicious amount determines whether a SAR or STR is filed. Is this changing?

A: No, this remains unchanged; both the Suspicious Activity Report (SAR) and the Suspicious Transaction Report (STR) continue to follow the same criteria.

Q: We would appreciate clarification on how suspicious amounts should be calculated. Different FIUs seem to apply varying approaches; for example, FIU A sums all suspicious transactions (incoming and

outgoing), whereas FIU B specifies that fund flows cannot be double counted. Will further guidance be provided on your preferred calculation method?

A: The *"Suspicious Amount"* category designates the aggregate monetary value of funds considered suspicious within the scope of the report. This amount must exclusively reflect transactions or activities that give rise to suspicion and should not encompass the total volume of financial operations conducted by the individual or entity concerned.

When calculating the suspicious amount, it is essential to avoid double counting. Specifically, incoming and outgoing flows associated with the same transaction or activity should be treated as a single instance, not as separate entries. This principle ensures the accuracy and consistency of the reported figures.

Please refer to the description of the *"Suspicious Amount"* category, where several illustrative examples are provided.

Time Elapsed

Q: Should this category be selected every time? Most of our cases will likely exceed 72 hours.

A: This category should only be selected in cases involving fraudulent operations.

Q: How should the timeframe for *"Time Elapsed"* be calculated? Should the calculation begin from the date of the earliest suspicious transaction or from the most recent one? Can we confirm what is meant by *"Time Elapsed"*?

A: The "*Time Elapsed"* category refers to the duration that has passed since the most recently identified suspicious transaction. Please select the time range that most accurately reflects this interval.

Disclaimer

Pursuant to Article 5 (I) a) of the amended Law of 12 November 2004 on anti-money laundering and counter-terrorist financing (hereinafter referred to as the 'Amended Law of 2004'), the obligation to report suspicious transactions applies without the reporting parties having to qualify the underlying offence.

Without prejudice to obligations towards supervisory authorities or self-regulatory bodies, professionals, their managers and employees must inform the FIU without delay when they know, suspect or have reasonable grounds to suspect that money laundering, an associated predicate offence or terrorist financing is being committed, has been committed or has been attempted, in particular because of the person concerned, their behavior, the origin of the assets, the nature, purpose or terms of the transaction. The report must be accompanied by all relevant information and documents.

All suspicious transactions, including attempts, must be reported, regardless of their amount.

This handbook is intended to guide professionals subject to the Amended Law of 2004 in the submission of suspicious transaction reports. They are encouraged to use the indicators in this handbook on a best effort basis in order to help improve the quality and relevance of reports.

This document is for information purposes only and does not replace the legal or regulatory obligations in force.

LA JUSTICE
Grand-Duché de Luxembourg

Cellule de renseignement financier (CRF)

Questions on this document may be sent to:
crf_dd@justice.etat.lu.

Contact

Cellule de Renseignement Financier (CRF)
Email address: crf@justice.etat.lu
Website: www.crf.lu

Follow us:

January 2026