LA JUSTICE
Grand-Duché de Luxembourg

Cellule de renseignement financier (CRF)

goAML Indicators

New collaborative approach serving the national AML/CFT Framework

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 were implemented in goAML. In the second phase, a total of 12 out of the 13 categories will be available: the original five categories remain in place, and seven new categories have now been added. The final category, "Business Activity Related to the Filed Report," will be made available as soon as possible.

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 clear articulation of suspicion; for the FIU, it increases operational capacity to detect, prioritize, and process high-risk cases in a timely manner.

The first section of this handbook presents the 12 categories together with their corresponding indicators. Each category and indicator are accompanied by a brief description explaining its intended use and the circumstances in which it should be applied.

The second section contains 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.

[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.

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.

All terms, not otherwise specifically defined herein, should be understood as defined in the Luxembourg Criminal Code, or failing that, as these terms are defined or understood under the FATF recommendations, the law of 12 November 2004 on the fight against money laundering and terrorist financing or any other guidelines or legal provisions that may be applicable.

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

Reporting

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.

Categories and related indicators

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/transaction may be connected to money laundering or terrorist financing. When completing the report, please select the indicator(s) that most accurately corresponds 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 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/pharming 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.

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.

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.

Transaction monitoring

Select when the suspicion has been identified as a result of transaction monitoring activities.

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.

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.

[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 virtual assets

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

ML/TF Typology

The *"ML/TF Typology"* category refers to the scheme, method, or modus operandi commonly used by a suspect in the context of money laundering or terrorist financing. Please select the applicable typology from the list below.

Beneficial ownership concealment

Select if the suspected typology concerns beneficial ownership concealment, namely the deliberate act of obscuring or hiding the identity of the true beneficial owner of an entity.

Circular transactions

Select if you suspect that the typology concerns circular transactions, defined herein as a pattern of fund movements in which money is transferred through one or more accounts, whether held by individuals or corporate entities, and ultimately returns to the originating account or to another account controlled by the same beneficial owner or related persons. Such transactions involve funds circulating within a closed loop without a legitimate economic purpose.

Complex ML scheme

Select if the suspected typology concerns a complex money laundering (ML) scheme, understood herein as a sophisticated arrangement with multilayered series of transactions, entities, or financial movements designed to obscure the origin, ownership, and destination of illicit funds by creating a confusing or opaque trail.

Cyber-enabled fraud

Select if the suspected typology concerns a cyber-enabled fraud (CEF), being a fraud that leverages digital platforms, online systems, or cyber technologies to deceive victims and commit financial crimes.

Mispricing

Select if the suspected typology concerns mispricing, defined herein as the intentional overvaluation or undervaluation of goods, services, or assets in commercial or financial transactions.

Misuse of artificial intelligence (AI)

Select if the suspected typology concerns the misuse of artificial intelligence (AI), namely the exploitation of AI tools to facilitate financial crimes, including, but not limited to, document falsification, identity manipulation, or automated fraud schemes.

Misuse of crowdfunding/fundraising

Select if the suspected typology concerns the misuse of crowdfunding or fundraising, defined herein as the exploitation of online platforms or public campaigns to collect funds from multiple individuals or entities for illicit purposes.

Misuse of legal entities (LE) or legal arrangements (LA)

Select if the suspected typology concerns the misuse of legal entities or legal arrangements, due to the improper use of companies, trusts, foundations, or other legal structures to conceal ownership, control, or the movement of illicit funds.

Other typology

Select if the filed report pertains to other typologies that do not fit into the mentioned category. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other Typology: [description]*).

Suspicious loans

Select if the suspected typology concerns suspicious loans, which consist, for example of a loan application or credit activity that shows unusual, inconsistent, or high-risk characteristics (e.g. lending arrangements that lack legitimate economic purpose, involve questionable counterparties, omit standard terms such as interest rates, or present unrealistic repayment conditions) that cannot be reasonably explained by the customer's profile or documentation and may indicate potential fraud or illicit activity.

Trade-based money laundering

Select if the suspected typology concerns trade-based money laundering (TBML), defined herein as the process of disguising the proceeds of crime and transferring value through trade transactions, often by misrepresenting the price, quantity, or quality of goods and services.

Use of money mules

Select if the suspected typology concerns the use of money mules, understood as individuals who transfer or move money on behalf of criminals, knowingly or unknowingly, thereby facilitating fraud or laundering schemes.

ML/TF affected Sector

The " *ML/TF affected Sector*" category refers to the sector of activity in which the suspicious transaction/activity or money laundering case has been identified. It should not be confused with the sector in which the reporting entity operates, as that information is captured under the *category "Business Activity Related to the Filed Report".* Please select the relevant sector(s).

Example: Real estate transactions

A bank submits a report concerning suspicious transactions involving questionable entities seeking to purchase real estate. In this scenario, the *"ML/TF affected sector"* is the *"Real Estate and Construction sector",* rather than the *"Banking sector"*. *"The Banking sector"* is instead the business activity related to the filed report*,* as it reflects the activity of the reporting entity. In contrast, the *"Real Estate and Construction sector"* is identified as the sector in which the money laundering activity itself is taking place.

However, if the questionable entities transfer for example, funds through multiple bank accounts prior to purchasing the real estate, the *"ML/TF affected sector"* would include both the *"Real Estate and Construction sector"* and the *"Banking sector",* as money laundering concerns would arise in both sectors.

Banking sector

Select if the suspected ML/TF affected sector concerns the banking sector, which covers traditional financial institutions and deposit-taking services.

Crypto-assets sector

Select if the suspected ML/FT affected sector concerns the crypto-assets sector, which includes virtual currencies and blockchain-based financial instruments.

Defense sector

Select if the suspected ML/TF affected sector concerns the defense sector, defined as the entirety of industrial, technological, and strategic activities directly related to the protection of national interests and the maintenance of international security.

E-commerce platform and online marketplace sector

Select if the suspected ML/TF affected sector concerns the e-commerce and online marketplace sector, which involves digital platforms for buying and selling goods or services.

E-money and payment institutions sector

Select if the suspected ML/TF affected sector concerns the e-money and payment institutions sector, which provides electronic money issuance and payment processing services.

Energy sector

Select if the suspected ML/TF affected sector concerns the energy sector, including the production, distribution, or trading of energy resources.

Gambling sector

Select if the suspected ML/TF affected sector concerns the gambling sector, which includes casinos, betting shops, and online gaming platforms.

High-value sector

Select if the suspected ML/TF affected sector concerns the high-value goods sector, including, but not limited to, luxury items, artwork, jewelry, vehicles, or valuable other collectibles that may be used to store or transfer value.

HORESCA sector

Select if the suspected ML/TF affected sector concerns the HORESCA sector, which covers hotels, restaurants, and cafés.

Insurance sector

Select if the suspected ML/TF affected sector concerns the insurance sector, which provides coverage and risk management through policies and premiums.

Investment fund sector

Select if the suspected ML/TF affected sector concerns the investment fund sector and/or any other types of collective investment vehicles.

Non-profit organization (NPO) sector

Select if the suspected ML/TF affected sector concerns the non-profit organization sector, which consists of entities operating for charitable, social, or community purposes.

Other sector

Select if the suspected ML/TF affected sector concerns any additional areas not specifically listed. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other Sector: [description]*).

Professionals of the financial sector (PFS)-Non-TCSP sector

Select if the suspected ML/TF affected sector concerns services or products provided by professionals of the financial sector, excluding trust and company service providers.

Public sector

Select if the suspected ML/TF affected sector concerns the public sector.

Real estate and construction sector

Select if the suspected ML/TF affected sector concerns the real estate and construction sector, which involves property development, sales, and building activities.

Trust and company service provider (TCSP) sector

Select if the suspected ML/TF affected sector concerns the trust and company service provider (TCSP) sector, which offers services related to company formation, management, domiciliation and fiduciary arrangements.

Product used for ML/TF

The *"Product used for ML/TF"* category refers to the specific financial products, instruments, or services that are employed to facilitate a suspicious transaction or activity linked to money laundering or terrorist financing activities. This classification highlights the means through which illicit funds are moved, concealed, or integrated into the financial system. Please select the relevant product(s).

Automobiles

Select if the product used for ML/TF are automobiles, which include vehicles purchased, sold, or transferred as part of financial activity.

Bank account

Select if the product used for ML/TF involves bank accounts, such as current accounts, savings accounts, or other deposit-holding accounts.

Cards

Select if the product used for ML/TF involves cards, including debit, credit, prepaid, or stored-value cards.

Cash

Select if the product used for ML/TF is cash, referring to physical currency used in deposits, withdrawals, or exchanges or cash-intensive transactions.

Consumer goods

Select if the product used for ML/TF involves consumer goods, including everyday retail items such as alcohol, tobacco, food products, clothing, household items, or other goods.

Crowdfunding/Fundraising

Select if the product used for ML/TF involves crowdfunding or fundraising mechanisms, including online platforms used to collect, pool, or distribute funds.

Crypto-assets

Select if the product used for ML/TF involves crypto-assets, including virtual currencies and digital tokens that are transferred or stored using blockchain or similar distributed-ledger technologies.

Electronics

Select if the product used for ML/TF involves electronics, such as mobile phones, computers, or other electronic devices purchased, traded, or resold.

E-money account

Select if the product used for ML/TF involves e-money accounts, including digital wallets or electronic payment accounts used to store or transfer value.

Energy and commodities

Select if the product used for ML/TF involves energy products or commodities, such as fuel, metals, agricultural goods, or raw materials.

High-value goods

Select if the product used for ML/TF Select if the product used for ML/TF involves high-value goods, such as luxury items including, but not limited to, artwork, jewelry, vehicles, or collectibles used to store or transfer value.

Insurance products

Select if the product used for ML/TF are insurance products, such as life, health, or investment-linked policies.

Investment funds

Select if the product used for ML/TF are investment funds and/or any other collective investment vehicles.

Legal entities/Legal arrangements

Select if the product used for ML/TF are legal entities or legal arrangements, such as companies, trusts, partnerships or similar structures.

Loans

Select if the product used for ML/TF are loans, including personal loans, commercial loans, inter-entity loans, or mortgage lending facilities.

Other product

Select if the product used for ML/TF is another product not specifically listed. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., *Other Product: [description]*).

Payment account

Select if the product used for ML/TF involves payment accounts, including accounts used to send, receive, or process payments.

Precious metals and gems

Select if the product used for ML/TF involves precious metals or gems, such as gold, silver, diamonds, or other high-value minerals.

Real estate

Select if the product used for ML/TF is real estate, including property purchases, sales, or development projects.

Virtual IBAN

Select if the product used for ML/TF is a virtual IBAN, which is a digital account identifier used to route payments electronically.

Weapons/ Military and defense goods

Select if the product used for ML/TF involves weapons, military equipment, or defense-related goods used in procurement, trade, or financing activities.

Suspected person/entity

The *"Suspected person/entity"* category refers to the person or entity identified as the subject of suspicion within the report. This category refers to the individual, legal entity or organization believed to be directly involved in, or otherwise connected to, the suspicious activity/transaction. Please select the relevant target(s).

Account holder

Select if the suspected person or entity is the account holder, meaning the individual, legal entity or organization in whose name the account is formally registered.

Account proxy

Select if the suspected individual or legal entity is an account proxy, referring to a person authorized to act on behalf of the account holder in managing or conducting transactions.

Investor

Select if the suspected individual or legal entity is an investor, defined herein as an individual or legal entity that allocates capital to financial products, ventures, or markets with the expectation of returns.

Other suspected person/entity

Select if the suspected individual or legal entity falls under another category not specifically listed in this category. It is strongly recommended to provide an explanation in the "Reason for suspicion" field in goAML (e.g., Other suspected person/entity: [description]).

Shareholder

Select if the suspected individual or legal entity is a shareholder, meaning an individual or entity that holds equity or shares in a company and thereby possesses ownership rights.

Third party entity

Select if the suspected legal entity is a third party entity, such as a company or organization directly or indirectly involved in the transaction or activity under suspicion.

Third party individual

Select if the suspected individual is a third party directly or indirectly linked to the transaction or activity under suspicion.

Transaction counterparty

Select if the suspected individual or legal entity is the direct counterparty to the reported suspicious financial transaction.

Ultimate beneficial owner (UBO)

Select if the suspected individual or legal entity is the ultimate beneficial owner (UBO), defined herein as the natural person who ultimately owns or controls an entity, arrangement, or set of assets.

Underlying client

Select if the suspected individual or legal entity is the underlying client of the actual customer or beneficial party on whose behalf a transaction or relationship is conducted, even if represented by an intermediary.

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.

Extortion

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 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.

Fraud legal entities (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 entities of money, property, or other assets.

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.

Organized crime

Select if you suspect that the facts described in the report may be related to an organized crime, defined herein as a structured, permanent, and collaborative group of individuals acting in concert to commit offences for financial or material gain, potentially operating across national or regional boundaries, and employing coordinated methods that may facilitate activities such as money laundering or the financing of terrorism.

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.

In situations where a transfer was attempted but not completed, the suspicious amount corresponds to the intended value of the transaction, even if no funds were ultimately transferred.

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.

Relationship Status

The *"Relationship Status"* category refers to the status of the business relationship between the reporting entity and its client at the time of the report. Please select the corresponding status.

Onboarding Accepted

This indicator pertains to new business relationships. Select if you validated the onboarding and accepted the business relationship.

Onboarding Ongoing

This indicator pertains to new business relationships. Select if the onboarding is still ongoing.

Onboarding Refused

This indicator pertains to new business relationships. Select if you refused the onboarding.

Relationship Offboarded

This indicator pertains to existing business relationships subject to a Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) procedure. Select if you concluded to offboard the relationship.

Relationship Ongoing

This indicator pertains to existing business relationships subject to a Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) procedure. Select if you concluded to keep the relationship ongoing.

Relationship Ongoing – Account blocked

This indicator pertains to existing business relationships subject to a Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) procedure. Select if you concluded to keep the business relationship ongoing, but the client's account has been blocked.

Crypto

The *"Crypto"* category encompasses facts and circumstances described in the report that may involve the use of crypto-assets or blockchain-based technologies in a manner that raises concerns regarding money laundering, terrorist financing, or other illicit activities. These indicators are primarily applicable to entities operating as Crypto-Asset Service Providers (CASPs) or Virtual Asset Service Providers (VASPs).

Darknet market

Select if direct or indirect transactions, interactions, links or involvements between an individual, legal entity or wallet and online illicit marketplaces operating on the darknet have been identified.

Direct transaction to an obfuscation platform (Mixers, DEFI Privacy Mixers, CoinJoin)

Select if direct transactions are identified involving the use of obfuscation services, such as crypto mixers, DeFi privacy mixers, CoinJoin protocols, or any other services designed to hide the origin, destination or ownership of the crypto-assets.

Instant withdrawal of funds (from crypto deposit)

Select if newly deposited cryptocurrencies, including, without limitation, EMTs and ARTs, are withdrawn immediately following the deposit.

Link to fraudulent address/smart contract

Select if transactions are detected that involve fraudulent wallet addresses or malicious smart contracts.

Suspicious transactions from gaming, gambling and/or NFT platforms

Select if suspicious transactions are detected that originate from or are directed to gaming platforms, online gambling services, or NFT (Non-Fungible Token) marketplaces.

E-commerce

The category *"E-commerce"* refers to facts described in the report that may be related to the use of online platforms for buying or selling goods and services in a manner that raises concerns about money laundering, terrorist financing, or other illicit activities. These indicators are mainly applicable to entities which are enabling transactions on e-commerce platforms.

Buyer complaints

Select if a significant proportion of buyer complaints are linked to a particular seller (e.g., 10% of all sales).

Dissolved entity

Select if you suspect that a dissolved or inactive legal entity has been used in the transaction chain.

Gift cards

Select if you suspect that gift cards have been misused for money laundering or terrorist financing purposes, as they can function as anonymous value-transfer instruments.

Non-Delivery

Select if you suspect that goods or services were not delivered despite payment being made.

Rights owner complaint

Select if rights holders have submitted complaints, which may indicate, but is not limited to, counterfeit goods, trademark infringement, or other intellectual property violations.

Unauthorized access

Select if an account has been breached or compromised and subsequently used for ML/TF-related activities, as unauthorized access often indicates account takeover fraud or other cyber-enabled crime.

Case Studies[3]

Case Study 1: Suspicious Transaction Report (STR) submitted by Retail Bank XYZ:

On December 15, 2025, retail bank XYZ identified a series of suspicious transactions involving John Doe and his company, John Doe SA. The suspicion was triggered by open-source information, including adverse media reports, which revealed potential links between John Doe and corrupt activities. The suspicious transactions totaled 5.500.000 EUR and were carried out over a period of three months. John Doe SA purchased several real estate properties at prices significantly above market value, raising suspicions of money laundering. These real estate acquisitions did not align with John Doe SA's legitimate financial profile.

The funds used for these purchases originated from bank accounts located in jurisdictions known for their lack of financial transparency. The transactions were structured in a complex manner, involving multiple entities and bank accounts, in order to conceal the ultimate beneficial owner. Funds were moved between various bank accounts before being used for the real estate purchases.

In summary, the suspicious transactions involving John Doe and John Doe SA exhibit several indicators of money laundering and corruption, justifying the selection of the following indicators:

- **Trigger of suspicion – Beneficial ownership issues:** The multiple transactions and entities suspect beneficial ownership issues.
- **Trigger of suspicion – Fraudulent transaction:** The transactions were identified as fraudulent due to the concealment of the beneficiary and the use of sophisticated methods to obscure the origin of the funds.
- **Trigger of suspicion –Inconsistencies regarding the economic origin of funds:** The funds originated from accounts in jurisdictions lacking financial transparency, inconsistent with John Doe SA's declared business activity.
- **Trigger of suspicion –Inconsistencies regarding the source of wealth:** The purchase of real estate at prices far above market value did not align with the company's legitimate financial profile.
- **Trigger of suspicion –Offshore based companies:** The transactions involved funds routed through offshore jurisdictions known for weak AML controls.
- **Trigger of suspicion – Open-source information including adverse media:** The suspicion was triggered by open-source information, including adverse media, revealing potential links between John Doe and corrupt activities.
- **ML/TF Typology – Beneficial ownership concealment:** The scheme aimed to hide John Doe's identity as the ultimate beneficial owner through layered transactions.

[3] The case studies included in this paper are purely fictional and are not derived from, nor intended to represent, any actual cases, persons, or organizations. All the names used herein are purely indicative and are placeholder names.

- **ML/TF Typology – Complex ML scheme:** The transactions were structured in a complex way, involving multiple entities and bank accounts, to conceal the origin of the funds.
- **ML/TF affected Sector – Banking sector:** The suspicious transactions were detected within the banking sector during retail operations.
- **ML/TF affected Sector - Real estate and construction sector:** The activities of John Doe SA in the real estate sector were particularly suspicious, involving the purchase, sale, and management of properties at abnormally high prices.
- **Product used for ML/TF – Real estate:** The suspicious transactions involved real estate, including property purchases, sales, and management.
- **Suspected person/entity – Ultimate beneficial owner:** John Doe was identified as the concealed ultimate beneficial owner behind the transactions.
- **Suspected Predicate Offence – Corruption and bribery:** Media reports indicated John Doe used his influence for personal gain, linking the funds to corruption and bribery.
- **Suspicious Amount – I. 5.000.001+ EUR:** The total amount of suspicious transactions exceeds 5.000.001 EUR.

Case Study 2: Suspicious Transaction Report (STR) submitted by Super Manco XYZ:

In December 2025, an alternative investment fund manager, Super Manco XYZ, based in Luxembourg, reported a series of suspicious activities linked to an investor named John Doe. He invested a total amount of 6.000.000 EUR in a sub-fund dedicated to infrastructure projects in Eastern Europe. This sub-fund is managed by a third-party company, ZYX Partners, acting as the external manager.

From the outset, John Doe's behavior raised concerns. He insisted that his investment be made through an offshore company, Doe Holdings Ltd, without providing any clear economic justification. He also requested that all communications be limited to a generic email address, refusing any direct contact with the fund managers.

Investment instructions were transmitted exclusively through a law firm based in another offshore jurisdiction, acting on behalf of Doe Holdings Ltd. This law firm failed to provide satisfactory documentation on the relationship between John Doe and the offshore entity, or on the origin of the funds.

A few weeks after the subscription, the fund granted a loan of 3.000.000 EUR to a construction company based in another jurisdiction, Build SA, officially engaged in a public infrastructure renovation project. Further analysis revealed that Build SA shares several directors with Doe Holdings Ltd and that John Doe is indirectly linked to both entities. The loan was granted under non-commercial terms: very low interest rate, no collateral, and a vague repayment schedule.

Open-source research revealed that John Doe is suspected of having close ties to corrupt public officials. He is mentioned in several media reports as being involved in opaque financial arrangements related to public procurement contracts.

All these elements, structuring via an offshore entity, involvement of non-transparent third parties, suspicious loans to related companies, and a background of corruption, led the fund manager to file a Suspicious Transaction Report.

In summary, the suspicious transactions, as well as the behavior of John Doe and the entities involved, present several indicators of money laundering and corruption, justifying the selection of the following indicators:

- **Trigger of suspicion –Inconsistencies regarding the economic origin of funds:** The origin of the funds used for the 6.000.000 EUR investment is unclear.
- **Trigger of suspicion –Inconsistencies regarding the source of wealth:** The investor provided no credible explanation for the source of wealth supporting such a large investment.
- **Trigger of suspicion – Offshore based companies:** The investment was made through Doe Holdings Ltd, an offshore company with no clear economic rationale.
- **Trigger of suspicion – Open-source information including adverse media:** Media reports linked John Doe to opaque financial arrangements and corruption in public procurement projects.
- **Trigger of suspicion – Politically exposed persons:** Open-source research indicated John Doe has close ties to corrupt public officials, suggesting possible PEP involvement.
- **Trigger of suspicion – Third party involvement:** All investment instructions were transmitted by a law firm based in another offshore jurisdiction acting on behalf of Doe Holdings Ltd.
- **Trigger of suspicion – Unusual behavior of the customer:** John Doe refused direct contact, insisted on using an offshore entity without justification, and communicated only via a generic email address.
- **ML/TF Typology – Misuse of legal entities (LE) or legal arrangements (LA):** Doe Holdings Ltd appears to be used to conceal the identity of the beneficial owner and the origin of the funds.
- **ML/TF Typology – Suspicious loans:** The fund granted a 3.000.000 EUR loan to Build SA, a company linked to John Doe, under non-commercial terms such as low interest and no collateral.
- **ML/TF affected Sector – Investment fund sector:** The suspicious activity occurred within the alternative investment fund sector.
- **Product used for ML/TF – Investment fund:** The product used is a compartment of an alternative investment fund.
- **Product used for ML/TF – Loans:** A loan was granted under suspicious conditions to a company connected to the investor.

- **Suspected Person/entity – Investor:** John Doe is the main investor in the relevant sub-fund.
- **Suspected Predicate Offense – Corruption and bribery:** Links to corrupt officials and questionable public projects were identified through open sources.
- **Suspicious Amount – 5.000.001+ EUR:** The total amount invested by John Doe in the fund is 6.000.000 EUR.

Case Study 3: Suspicious Transaction Report (STR) submitted by the electronic money institution XYZ-PAY:

On January 3, 2026, an electronic money institution operating in Luxembourg, XYZ-PAY, detected suspicious activity on a recently opened account in the name of John Doe. The account had been activated via a mobile application, with identity verification that was compliant but minimal, and was linked to a virtual debit card.

Within 48 hours of activation, the account received several incoming transfers totaling 22.500 EUR from six different individuals located in three EU countries. The payment references were vague, often limited to terms like “loan,” “help,” or “reimbursement.” None of the transfers appeared to correspond to any identifiable commercial activity.

Immediately after receiving the funds, John Doe carried out a series of rapid cash withdrawals from ATMs in various border towns, along with several purchases of electronic gift cards and high-value electronic goods. The entire balance was drained from the account in under 36 hours.

Behavioral analysis revealed that John Doe’s account exhibited all the characteristics of a transit account: rapid receipt of funds followed by immediate withdrawal or transfer, without any consistent economic activity. Furthermore, the incoming transfers originated from individuals believed to be victims of online fraud, having been convinced to send money to John Doe under false pretenses related to investment opportunities or administrative assistance.

The institution also identified inconsistencies with the declared business activity: at account opening, John Doe claimed to be an independent consultant, but none of the transactions reflected any professional activity. No supporting documentation for such activity could be provided, despite multiple follow-up requests.

Finally, the collected evidence suggests that John Doe may be acting as a money mule, serving as an intermediary to transfer proceeds from fraud schemes. His profile, the movement of funds, the use of cards, and the speed of the transactions are all typical indicators of such activity.

In summary, the suspicious transactions and John Doe’s behavior present several indicators of money laundering, justifying the selection of the following indicators:

- **Trigger of suspicion – Amount of transfer:** The account received EUR 22,500 in several transfers within 48 hours of activation.

- **Trigger of suspicion – Fraudulent transaction:** The funds received originated from individuals believed to be victims of online scams.
- **Trigger of suspicion – Frequent transactions and in small amounts (smurfing):** Several separate transfers from different individuals in small amounts were received in a short time frame.
- **Trigger of suspicion – Inconsistencies regarding the business activity:** John Doe declared himself as an independent consultant, but no transactions reflected professional activity.
- **Trigger of suspicion – Inconsistencies regarding the economic origin of funds:** The origin of funds was unclear and linked to individuals suspected of being victims of online fraud.
- **Trigger of suspicion – Phishing/pharming:** The incoming transfers originated from individuals believed to be victims of online fraud.
- **Trigger of suspicion – Transit account:** The account received funds from multiple sources and immediately withdrew or spent them, without any identifiable economic activity.
- **ML/TF Typology – Money mules:** The client's behavior is typical of a money mule, facilitating the transfer of fraudulent funds.
- **ML/TF affected Sector – E-money and payment institutions sector:** The suspicious activity occurred within the electronic money institution sector.
- **Product Used for ML/TF – Cards:** The funds were used via debit cards and to purchase electronic gift cards.
- **Suspected person/entity – Account holder:** John Doe is the account holder used for the suspicious transactions.
- **Suspected Predicate Offense – Fraud individuals (Scam (including attempts)):** The funds originated from victims of online scams, constituting fraud against individuals.
- **Suspicious Amount – E. 15.001 – 25.000 EUR:** The total amount of suspicious transactions is 22.500 EUR.
- **Time Elapsed– B. 24h–48h:** All funds were received and withdrawn within less than 48 hours.
- **E-commerce – Gift cards:** Part of the funds was used to purchase electronic gift cards.

Case Study 4: Suspicious Activity Report (SAR) submitted by the trust and company service provider XYZ-TCSP:

In November 2025, a trust and company service provider based in Luxembourg reported a series of suspicious activities related to a complex legal structure set up on behalf of John Doe, identified as the ultimate beneficial owner. The structure included a Luxembourg holding company, JD Management Sàrl, and two subsidiaries, Subsidiary 1 and Subsidiary 2, located in two different jurisdictions.

JD Management Sàrl obtained a commercial loan of 2.000.000 EUR from a local financial institution, justifying the funding with a planned commercial real estate acquisition in Country A. However, an analysis of the financial flows revealed that the funds were quickly transferred to Subsidiary 1, and subsequently redirected to a foreign real estate company, C Real Estate SL, for the purchase of a luxury residential property in the name of a third party.

At the same time, JD Management Sàrl declared a business activity of strategic consulting, but no corresponding income was recorded on its accounts. The only incoming funds came from intercompany loans and internal transfers, with no clear economic rationale. In addition, the documents provided to justify the origin of the funds contained inconsistencies: some loan agreements were backdated, and the counterparties identified were entities with no real business activity.

A compliance check revealed that one of the directors of Subsidiary 2 was listed on an international financial sanctions list, further reinforcing suspicions regarding the true purpose of the operations.

The entire structure appears to have been designed to conceal the identity of the beneficial owner, obscure the origin of the funds, and facilitate foreign real estate transactions without proper tax disclosure. The service provider therefore submitted a Suspicious Activity Report, considering that the case may involve a serious tax offense.

In summary, the suspicious activities involving John Doe present several indicators of money laundering, justifying the selection of the following indicators:

- **Trigger of suspicion – Beneficial ownership issues:** The entire structure appears to have been designed to conceal the identity of the beneficial owner.
- **Trigger of suspicion – Inconsistencies regarding the business activity:** The declared consulting activity generated no revenue, indicating a mismatch between stated and actual operations.
- **Trigger of suspicion – Inconsistencies regarding the economic origin of funds:** The funds originated from intercompany loans with no clear economic justification and contradictory documentation.
- **Trigger of suspicion – Inconsistencies regarding the KYC/KYT documentation:** The provided documentation contained irregularities that undermined the credibility of the client's profile and transactions.
- **Trigger of suspicion – Inconsistencies regarding the source of wealth:** The origin of funds was obscured through backdated loan agreements and counterparties without genuine business activity, raising suspicion about the legitimacy of the declared source of wealth.
- **Trigger of suspicion – Sanctions lists:** A director of Subsidiary 2 appeared on a sanctions list.
- **ML/TF Typology – Beneficial ownership concealment:** The multi-jurisdictional structure was designed to conceal John Doe's identity as the beneficial owner.
- **ML/TF Typology – Complex ML scheme:** The rapid fund transfers across jurisdictions and entities illustrate a sophisticated layering process typical of money laundering.

- **ML/TF Typology – Misuse of legal Entities (LE) or legal arrangements (LA):** Shell companies and subsidiaries were exploited to disguise transactions and obscure accountability.
- **ML/TF Typology – Suspicious loans:** The commercial loan was misused as a mechanism to channel funds into unrelated real estate purchases.
- **ML/TF affected Sector - Real estate and construction sector:** The suspicious funds were ultimately invested in luxury real estate abroad.
- **ML/TF affected Sector - Trust and company service provider sector (TCSP):** The suspicious legal structure used the services of a TCSP to establish and domicile the structure.
- **Product used for ML/TF – Loans:** A commercial loan was used as a vehicle for transferring funds.
- **Product used for ML/TF – Real estate:** The funds were used to purchase a residential property abroad.
- **Suspected Person – Beneficial owner:** John Doe is the beneficial owner of the structure involved.
- **Suspected Predicate Offense – Tax offenses:** The overall operations appear intended to circumvent tax obligations.
- **Suspicious Amount – H. 1.000.001–5.000.000 EUR:** The total amount of suspicious transactions is 3.200.000 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 the 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 regarding the business activity*"? 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, patterns, 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."*

ML/TF Typology

Q: Could you define the term "complex" for the indicator *"Complex ML Scheme"*?

A: In a Complex Money Laundering Scheme, the term complex refers to the deliberate use of sophisticated, multi-layered structures that obscure the origin and movement of illicit funds. These schemes often involve, for example, a web of legal entities such as shell companies, trusts, and foundations, frequently spread across multiple jurisdictions with weak transparency laws. By employing nominee directors and shareholders, true ownership is hidden, making it difficult for investigators to trace the beneficial owner. Transactions are layered across various accounts and institutions. The complexity is not just in the number of entities or steps involved, but in how strategically they are orchestrated to evade scrutiny and hinder financial oversight.

Q: Could you provide further clarification or examples of cases that should be reported under the indicator *"Cyber enabled fraud"*?

A: *"Cyber-enabled fraud"* refers to fraudulent activity carried out through digital platforms or technological tools. This includes schemes conducted via email, social media, fraudulent websites, malware, or other online channels. Use this indicator when the fraudulent behavior is facilitated or executed through cyber or internet-based means. It applies to situations such as phishing, account takeovers, online investment scams, and similar cases.

Q: Do the indicator *"Suspicious loans"* also apply to zero-interest loans (or loans granted outside market conditions), as well as loans to a UBO not authorized under the statutes?

A: The indicator *"Suspicious loans"* encompasses any type of loan whose terms or conditions appear questionable, unusual, inconsistent, or otherwise indicative of heightened risk. This includes, but is not limited to, zero-interest loans, loans granted under non-market conditions, and loans extended to a UBO not authorized under the company's bylaws.

Suspected person/entity

Q: Should the "*Investor*" indicator be used any time the customer who is the subject of a report uses our investment services, or only when the suspicion specifically originates from/is linked to their investment activity?

A: The *"Investor"* indicator should only be selected when the individual identified as *the "Suspected person/entity"* in the report is acting in their capacity as an investor. It should not be applied solely because the customer uses investment services.

Q: In cases of Account Takeover (ATO), would it be appropriate to use the *"Third-party individual"* indicator?

A: Yes. In cases of account takeover, the *"Third-party individual"* indicator may be selected.

Q: Could you please clarify what is meant by the *"Underlying client"* indicator and in which scenarios it should be used?

A: The *"Underlying client"* refers to the actual customer or beneficial party on whose behalf a transaction or relationship is ultimately conducted, even when an intermediary is involved. Example: Entity A provides a service to Entity B (acting as an intermediary), and Entity B uses that service to serve Customer C. If the suspicion relates to Customer C and Entity A files the report, then Customer C is the *"Underlying client"* and should be identified as the *"Suspected person/entity."*

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"* from the category "*Crypto"* must also be selected.

Q: For negative balance cases resulting from SEPA Direct Debit (SDD) fraud, would the indicator *"Fraud – Individuals (Scam, including attempts)"* be the most appropriate?

A: Yes. 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.

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.

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".*

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 SEPA Direct Debit (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.

Crypto

Q: Does the indicator *"Darknet Market"* link with potential purchases of drugs or sales of drugs or trafficking?

A: This indicator should be selected when the darknet market is involved, regardless of the product or service used.

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 activity/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:

2026