RapidAML

Suspicious Activity Reporting (SAR) for DNFBPs and VASPs

info@rapidaml.com www.rapidaml.com

RapidAML

A Suspicious Activity Report (SAR) is a critical element of the regulatory framework against money laundering, financing terrorism, and proliferation financing.

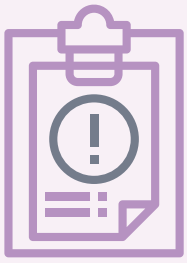
The UAE regulatory landscape mandates DNFBPs and VASPs to promptly report any suspicious behaviour that indicates involvement in illicit activities to the Financial Intelligence Unit (FIU) via the goAML portal.

info@rapidaml.com www.rapidaml.com

RapidAML

Table of Content

RapidAML



What is a Suspicious Activity Report (SAR)

What is a Suspicious Activity?

Any unusual, irregular or unnatural customer behaviour which can be interpreted as money laundering (ML), the financing of terrorist activity (FT), proliferation financing of weapons of mass destruction (PF), or any other criminal offence is termed as a **"Suspicious Activity".**

Suspicious Activity also refers to any unusual or abnormal pattern emerging from customer behaviour, conduct or activity that occurs during the course of a business relationship with a customer.

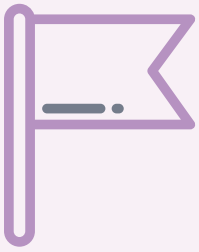
What is a Suspicious Activity Report (SAR)?

In the context of the UAE Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) regulations, the Designated Non-Financial Businesses and Professions (DNFBPs) and Virtual Asset Service Providers (VASPs) need to report promptly the events of any suspicious activity by their customers, suppliers or business partners to the Financial Intelligence Unit (FIU). A Suspicious Activity Report (SAR) can be filed by using the goAML portal.

DNFBPs and VASPs are exposed to the risk of money laundering (ML), financing of terrorism (FT), and proliferation financing (PF) of weapons of mass destruction due to the inherently risky nature of their goods, services, geographies, and delivery as well as transaction channels they are involved with.

Therefore, the customer-facing staff of the DNFBPs and VASPs need to be aware of indicators or signals of potentially suspicious behaviour that they may encounter while dealing with a large number of customers on a day-to-day basis. These indicators or signals are also known as red flags of ML/FT and PF. These signals should ideally form a part of the internal AML/CFT policy and procedure documentation and the AML/CFT training programs that are specifically designed for customer-facing personnel of DNFBPs and VASPs.

RapidAML



Red Flags Indicating ML/TF for DNFBPs and VASPs

Red flag indicators are warning signs that indicate the potential involvement of ML/FT or PF-related activities and crimes. The ML/FT and PF red-flag indicators help the customer-facing personnel of DNFBPs and VASPs identify potentially suspicious customers engaged in ML/FT and PF.

The red-flag indicators help the customer-facing staff of the DNFBPs and VASPs to become aware of the circumstances that would require the filing of an SAR.

RapidAML

Circumstances Warranting the Filing of a SAR

Various situations in the day-to-day business of DNFBPs and VASPs require the filing of a SAR, such as the following:

Customer's reluctance or refusal to provide KYC details

When a customer deliberately avoids or does not cooperate with the DNFBP or VASP to complete their KYC formalities, which include sharing key identifier information and verifying the same, then such a situation requires the customer-facing staff of the DNFBPs and VASPs to report such abnormal behaviour or pattern to the Compliance Officer, who upon further investigation, decides whether or not to file SAR on the goAML portal.

Various situations in the day-to-day business of DNFBPs and VASPs require the filing of a SAR, such as the following:

Proposed business on behalf of unknown person/entity

When a customer presents themselves as:

- a representative or acts on behalf of an individual or an entity who seidentity details cannot be traced or found or
- when the business is proposed to be conducted on behalf of a person or an entity whose identity details are unknown or untraceable,

then such a situation is required to be reported by DNFBPs and VASPs through the filing of a SAR on the goAML portal, as the inability to trace or identify the person behind the transaction or the ultimate beneficial owner (UBO) through the complex business structures by using shell companies poses a significant ML/FT and PF risk, which needs to be investigated and the attention of the authorities needs to brought to a situation where a customer is attempting to conduct business on behalf of a person or an entity whose identity cannot be found and verified.

Various situations in the day-to-day business of DNFBPs and VASPs require the filing of a SAR, such as the following:

Multiple intermediaries

Intermediaries are persons or entities that act as go-between or middlemen among parties to transactions. Intermediaries include financial institutions, banks, retailers, distributors, agents and brokers, among many others.

The involvement of multiple intermediaries to execute or carry out a transaction or channelling of funds for the purpose of transaction through multiple intermediaries is a cause for concern requiring the attention of authorities through the filing of SAR because such transactions could probably mean that there is an element of ML/FT or PF associated with such transactions and involvement of multiple intermediaries could denote that they are being used to layer illicit proceeds into the financial system by creating a trail of transactions.

Various situations in the day-to-day business of DNFBPs and VASPs require the filing of a SAR, such as the following:

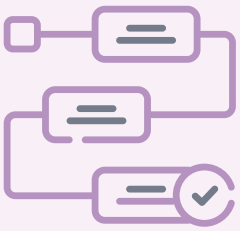
Association with sanctioned individual

Sanction lists are lists of individuals and entities published on the national and international levels containing names of individuals and entities with whom business should not be conducting because of their involvement with criminal or prohibited activities.

The Customer Due Diligence (CDD) process of any DNFBP and VASPs operating in the UAE requires that the prospective and existing customers are continuously screened against UAE local terrorist lists and UNSC consolidated lists to prohibit business with entities and individuals whose names appear in such lists.

When during such screening and monitoring process during CDD and ongoing monitoring, it is found that the existing or the prospective customer's name is appearing in sanctioned lists or that they are associated with persons or entities whose names are appearing in sanctioned lists, then such a finding requires for reporting to the authorities by filing of Fund Freeze Report {FFR} when the DNFBP or VASP have already received any payment or funds from the sanctioned individual or file a Partial Name Match Report {PNMR} if the DNFBP or VASP are not entirely sure that the name of their customer matches accurately or partially with those given in the sanction lists.

RapidAML



Step-By-Step Process to file SAR

The Step-by-Step process to file the SAR involves a blend of internal procedures to be followed within the organisation and steps for filing the SAR on the goAML portal.

The registration of DNFBPs and VASPs on the goAML portal is a mandatory obligation, enabling them to fulfil their regulatory reporting requirements, such as SAR, STR, and other such reports. Needless to say, the DNFBP or VASP have to maintain their status as "active" on the goAML portal.

As the Compliance Officer of a DNFBP or VASP gets notified of the potentially suspicious activity by receiving the internal SAR from the client-facing staff, then the Compliance Officer needs to investigate the internal SAR and decide if suspicious activity mentioned in such a report needs to be reported to the Financial Intelligence Unit (FIU) through the goAML portal by following the steps discussed.

Step-By-Step Process to file SAR

Internal SAR steps

Internal report by the first line of defence to the Compliance Officer

- Analyse details of internal SAR filed by client facing staff

Preparation of SAR in the required format by the Compliance Officer/MLRO

- Ensure all elements of SAR are contained in prescribed format

Steps on goAML portal

Logging in on the goAML portal

- Login with Company credentials

Select Report Type

1. Opting to file SAR from dropdown menu
2. Uploading XML version of SAR or entering SAR details in Web-Report format in real-time

Saving and Submitting

- Saving SAR details and submitting to the FIU on the goAML portal

1. Internal report by the first line of defence to the Compliance Officer

The customer-facing staff has to file an internal SAR to escalate the case of a potentially suspicious customer to the Compliance Officer. The Compliance Officer needs to investigate and analyse the internal SAR received concerning the potentially suspicious activity and decide whether to file a SAR on the goAML portal.

2. Preparation of SAR in the required format by the Compliance Officer/MLRO

Once the Compliance Officer is clear that the filing of the SAR would be required, they must start preparing the SAR in a manner and format prescribed, which is acceptable on the goAML portal, along with the necessary details for SAR submission, such as date, time, location of the alleged suspicious activity, parties involved, business purpose, and other relevant information.

3. Logging in on the goAML portal

As the details of SAR are ready, the Compliance Officer must log into their DNFBPs or VASPs goAML portal account using company credentials.

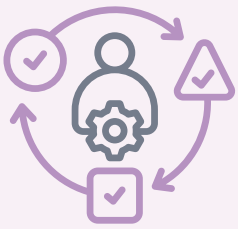
4. Select report type

The Compliance Officer or MLRO must select the type of report they intend to file (SAR in this case) from the list given in the dropdown menu on the goAML portal after selecting the SAR as the report type. The Compliance Officer or MLRO may either upload the SAR in XML format or fill in the details pertaining to suspicious activity in real-time by selecting the web-report option.

5. Saving and submitting

The last step while filing SAR on the goAML portal is to save the SAR details and submit the same.

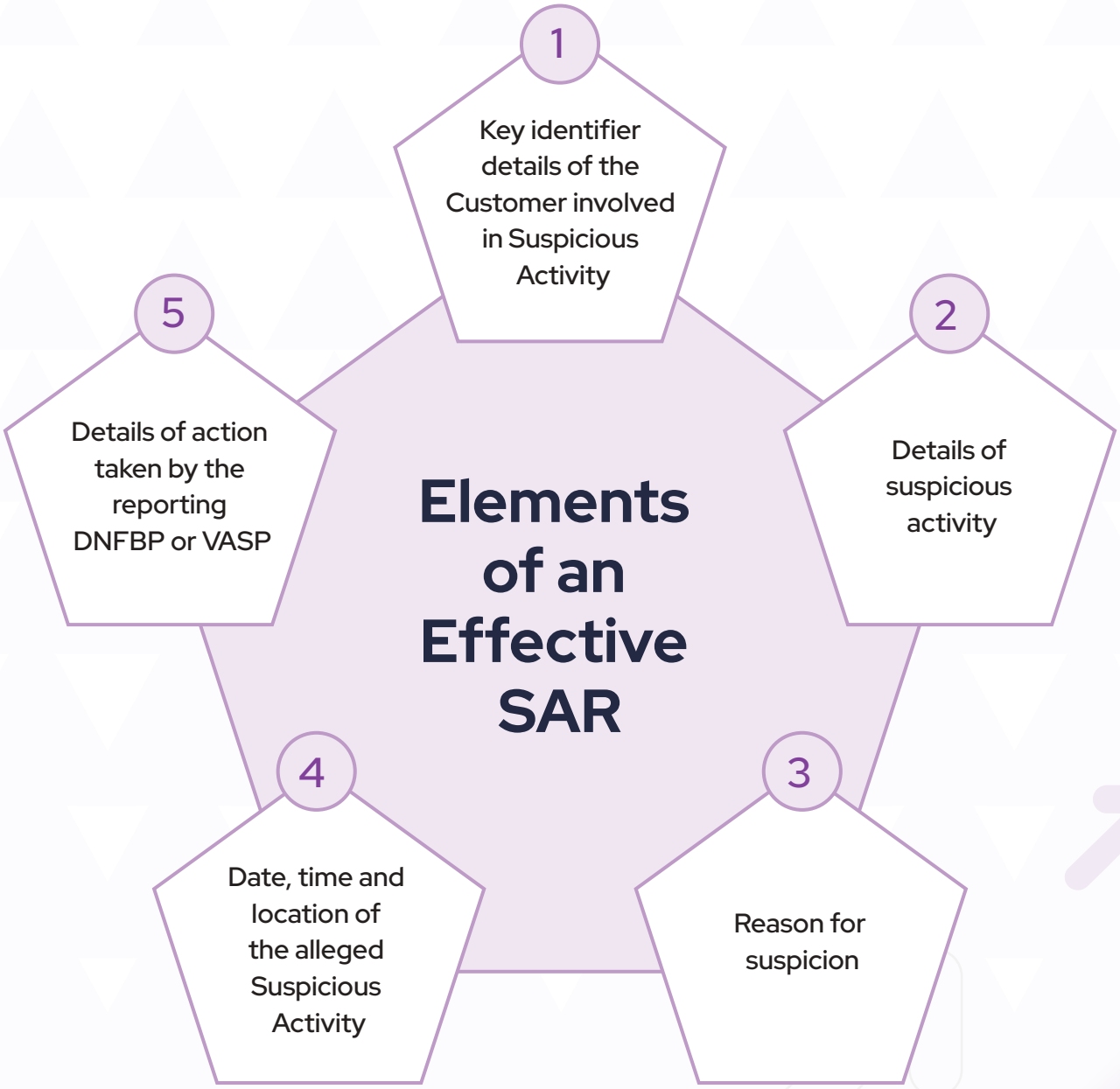
RapidAML



Elements of an Effective SAR

The responsibility of the Compliance Officer to file SAR on the goAML portal cannot be treated with a tickbox approach.

The Compliance Officer needs to ensure that the SAR contains necessary actionable details regarding the alleged suspicious activity so that the FIU can investigate the SAR thoroughly. The essential elements of an effective SAR would ideally contain the following details:



1. Key identifier details of the Customer involved

The SAR must clearly describe its subject of SAR, which is the details of individuals or entities that the DNFBPs or VASPs find suspicious, resulting in the need to file the SAR. The SAR must also include the identifying information of beneficiaries, accountholders, originators, or any other party involved in the allegedly suspicious activity. These details must also contain information about every individual's role and involvement in such alleged suspicious activity.

2. Details of suspicious activity

The SAR needs to contain details regarding the means and methods used for carrying out the alleged suspicious activity.

3. Reason for suspicion

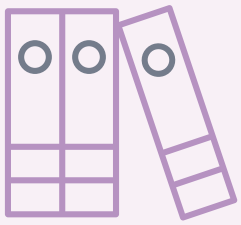
The SAR must also contain reasons behind why the customer-facing staff and compliance officer of the DFBPs or VASPs found the subject of the SAR to be suspicious, what red flag was observed, or what caused them to file the SAR. Such reason for SAR must be included in the SAR.

4. Date, time and location of the alleged suspicious activity

The SAR also needs to contain details of the date, time, and location of the alleged suspicious activity, and the DNFBPs and VASPs need to be mindful of mentioning this important element in the SAR.

5. Details of action taken by the reporting DNFBP or VASP

Lastly, the SAR needs to contain the details of mitigating measures taken by the DNFBP or VASP, such as suspending the business relationship and filing an internal SAR to escalate the suspicion to the Compliance Officer /MLRO.



What to do after Filing SAR

Once the SAR is filed, the customer-facing staff of the DNFBPs and VASPs need to navigate carefully through the business relationship with the prospective or existing customer,- whose name has been included in the SAR.

An abrupt or sudden break in communication or a distant approach while dealing with such a customer may cause the customer to sense that the DNFBP or VASP has become suspicious of them.

The DNFBPs and VASPs can rely on delaying tactics such as technical issues, internal approval processes, or operational issues as an excuse to wait for FIU's instructions while keeping the customer engaged.

The FIU may not respond or may give instructions as to what needs to be done with the subject matter of SAR. However, the DNBPs and VASPs need to follow FIU's instructions whenever they are sent. They should also classify such a customer as a high-risk customer and treat such a customer with Enhanced Due Diligence (EDD) and ongoing monitoring procedures as they would for any high-risk customer to mitigate and eliminate the possibility of ML/FT or PF.

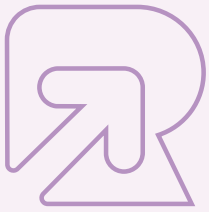
Conclusion

RapidAML

The DNFBPs and VASPs in UAE need to be alert about the regulatory requirement of filing SAR if they come across any suspicious or abnormal patterns which may point towards potential ML/FT or PF.

They should have appropriate methods and tools to identify suspicious activity by imparting adequate and suitable training regarding red flags and typologies of ML/FT and PF relevant to their business and the customer-facing staff.

They should also have a systematic workflow in place where the identification of suspicious activity is escalated through relevant staff to the compliance officer, enabling them to report the suspicious activity by filing SAR on the goAML portal.



About RapidAML

RapidAML

RapidAML is an AML software designed to support the compliance tasks of the DNFBPs and the VASPs, offering an advanced and secured technology platform

Who we are

Facctum, founded in 2021 by a group of enthusiasts who have experience in banking, financial crime risk management technology, data science, etc., specialises in building risk management solutions with new-age technology.

Our Mission

We understand the significance of AML compliance and recognise its complexity. Addressing this issue is our mission at RapidAML.

Our solution focuses on simplifying the intricate regime of AML compliance with advanced technology. We aim to help the regulated entities, specifically the DNFBPs and the VASPs, smoothen their AML efforts with RapidAML's end-to-end AML software..

Our Vision

Our vision is to empower DNFBPs and VASPs worldwide to combat financial crime, and protect the global financial system by providing innovative, affordable, and effective solutions.

While delivering the compliance solution to the customers, we do not undermine our adherence to the regulations and commitment to building a compliant economy.

Our working culture is in accordance with the applicable laws of the land, focusing on improving the lives of our people, elevating the compliance standard of our customers, and contributing to a society that is safe from money laundering and other financial crimes.

At RapidAML, we promote a sustainable value-creation approach, integrating human talent with advanced tech.

Our Core Values

We live by these guiding principles that guide our progress

Customer Focused

We are committed to offering quality AML support to exhibit a constructive effect on the customer's business.

Elevated Excellence

With a comprehensive, tech-driven financial crime compliance solution, we nurture customer's efforts and ignite brilliance to AML function.

Innovation Is The Key

We strive for healthy competition, bringing out the best version of the AML tools and technologies with continuous research and improvement.

Integrity

We value our customers, our team, and our society, and we build trust with our committed honesty and transparency.

Together We Win

With inclusiveness and a sense of collaboration, we assist our customers in accomplishing compliance and developing a sense of shared achievement.

RapidAML

info@rapidaml.com
www.rapidaml.com

Follow us on