Research Paper Series

Introduction on Money Laundering and Financial Terrorism Risks

Lorena Corna

June 2021

iason
ESSENTIAL SERVICES FOR
FINANCIAL INSTITUTIONS

iason
Research Paper Series
Year 2021 - Issue Number 36

Last published issues are available online:
http://www.iasonltd.com/research

Front Cover: **Carla Accardi**, *La ricerca del colore*, 1998.

Executive Summary

The author would provide an overview of Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) policies and procedures in place. In the first section, the author presents a general overview of International Standards with a focus on interpretative notes on the risk-based approach and FIU. To follow, the author gives a summary of the European legislation and the last contributions of Basel Committee and European Banking Authority.

About the Author

Lorena Corna:
Business Analyst
As Business analyst she currently works within the Risk IT dedicated team of a big pan European Bank. In particular, she follows the back-testing model for Counterparty Credit Risk.

Table of Content

Introduction on Money Laundering and Financial Terrorism Risks

Lorena Corna

Within the Risks whole that a Financial Institution should consider, the Basel Committee supports the Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) policies and procedures to avoid impact on reputational, operational, compliance and concentration Risks.

This is the goal of "*Financial Action Task Force Recommendations*" [12]: it represents the international foundation for all Countries and Financial Institutions. The mentioned recommendations have not a legal force but they should be adapted in the national context of each Country with the scope of hinder money laundering and terrorist financing.

In addition to international standards, we have the European regulations (the last one is Fifth European Directive 2018/843 [10], which integrate the Fourth European Directive 2015/849 [11]) and the national laws (in Italy it is represented by D. L. as of November 21st, 2007 , n. 231, updated with D. Lgs. as of October 4th, 2019, n. 125).

The last contribution is represented by the "*Sound Management of Risks related to Money Laundering and Financial Terrorism*" [3] of Basel Committee. In detail, the Committee:

- Accentuates the possible risks when a Bank use a third party (*e.g.* other banks, financial institutions or other entities) to conduct the Customer Due Diligence;
- Stresses on the risk-based approach application for correspondent banking relation.

Next to the above organisms, we can see other authorities named Financial Intelligence Units (*i.e.* FIUs): they are national units with administrative authorities that receive and analyze all the ML/FT information, supporting the disclosure of the results among the FIUs of other countries.

1. International Standards: the FATF's Recommendation

The FATF Standards represent a complete and robust framework to contrast money laundering and terrorism financing. The first issue was in 1990: over the years, we had several reviews of them until the last available version in June 2019 which comprises the Interpretive Notes.

The final version is composed of the following paragraphs:

- **AML/CFT Policies and Coordination**. In this section, the importance of identify, assess and understand via risk-based approach (*i.e.* RBA) the ML and FT risks is highlighted: to implement the risk-based approach is necessary a financial sector with a high degree of experiences on AML/CFT. By adoption of this approach, the financial institutions can activate the proper AML/CFT measures ensuring the efficient use of their resources, in terms of cost and human resources allocated. Due to the AML/CFT risks nature, the national principles should be reviewed periodically without: (i) compromise the cooperation among FIU, supervisors, law enforcement authorities, *etc.*; (ii) make a conflict between AML/CFT laws and Data Protection and Privacy rules.

- **Money Laundering and Confiscation**. Based on the Vienna Convention, the Palermo Convention and the Terrorist Financing Convention, also the International Standards dedicate a section on legislative measures like confiscation to hinder money laundering.

- **Terrorist Financing and Financing of Proliferation**. As already established in the Terrorist Financing Convention, in the FATF's Recommendation we have a section on terrorist financing and related measure to contrast them like the freezing of funds or other assets.

- **Preventive Measures**. As stated in [12], "*Financial Institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names*". In detail, a Financial Institution should be called to do a *customer due diligence measure* in some circumstance (*e.g.* in case of unreliable information obtained with customer identification process) using an independent source to validate the available information regarding customer's identity, the beneficial owner, the nature of the business relationship and transaction typologies: this analysis should be performed using a risk-based approach. In case of unsuccessful results from the procedure above, the Financial Institution "*should be required not to open the account, commence business relations or perform the transaction; or should be required to terminate the business relationship, and should consider making a suspicious transactions report in relation to the customer*" [12]. These information should be adequately stored by the Financial Institution and they should be enough to allow the rebuilt the transaction history in order to provide the evidence of a criminal activity. Furthermore, additional measures should be implemented for particular customers (*e.g.* Politically Exposed Person, PEP) and activities (*e.g.* development of new products and new business practices) to measure and mitigate their emerging risk.

- **Transparency and Beneficial Ownership of Legal Persons and Arrangements**. The fifth section of FAFT Recommendations is dedicated to transparency and beneficial ownership of legal persons and arrangements: each country should implement any measure to avoid the improper use of them from money laundering or terrorist financing.

- **Powers and Responsibilities of Competent Authorities and Other Institutional Measures**. As stated in sixth section [12], "*Countries should ensure that Financial Institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations*". In general, when Financial Institutions provide a service of money or value transfer, or money or currency changing, they should be subject to effective systems in compliance to national AML/CFT requirements. To permit the realization of FATF Recommendations, the Supervisor can force the production of compliant information. In case of failure, the supervisory should impose a disciplinary and financial sanctions, in line with Recommendation 35. As mentioned before, each country should have a Financial Intelligence Unit (FIU) that should receive and analyse the suspicious transactions' reports and any relevant money laundering information or related to terrorist financing. As remarked in [12], "*The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.*" Next to FIUs, each Country should have an investigative authorities with ML/FT responsabilities and they can made a parallel investigation with several techniquest like undercover operations, intercepting communications, accessing computer systems and ask to FIUs all the relevant information about ML/FT crimes.

- **International Cooperation**. The goal of last section is encourage the international cooperation. Countries should offer "*the widest possible range of mutual legal assistance in relation to money laundering, associated predicate offences and terrorist financing investigations, prosecutions, and related proceedings.*" [12] to enhance cooperation without jurisdiction conflicts among the countries. This mutual legal assistance is defined in terms of freezing, confiscation and extradition requests and all the other possible forms of international cooperation (via bilateral or multilateral agreements or arrangements).

	2015	2016	2017	2018	2019
Absolute values	84,627	103,995	94,018	98,117	106,318
Variation respect to previous year	11.6%	22.9%	-9.6%	4.4%	8.4%

TABLE 1: Suspicious transaction reports [2]

1.1 Interpretive Notes on Assessing Risks and Risk-Based Approach

The first interpretative notes in [12] is dedicated to risk-based approach used to hinder money laundering and terrorist financing. The relevance of the risk-based approach is established also with European Directive 2015/849: the latter recognizes that the ML/FT risk can change and it sets mentioned approach at the center of AML/CTF framework.

Using the risk-based approach (*i.e.* RBA), the Financial Institutions can use a AML/CFT measures proportionate with the risks identified. Then one of the advantage of RBA is that the level of human and financial resources allocated to obstruct the ML/FT crimes are commensurate with the level of AML/CFT risk: with higher risks, Countries should demand Financial Institutions "*to take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted*" [12]. The RBA implementation requires to Financial Institutions a dedicated processes in order to recognize, evaluate, supervise, handle and mitigate the money laundering and terrorist financing risks. In detail, the Committee discourages the size of operations or profits/losses of a bank as a ML/TF risk indicator, due to the fact that risks can come to light from small parts or activities of a Financial Institution [3].

The RBA can be adopted also by supervisory authorities and, in this case, the RBA demands that supervisors [3]:

- Improve a in-depth comprehension of risk level and related impact on the supervised entities;
- Based on national risk assessment, evaluate the adequacy of bank's risk evaluation;
- Understand the nature and size of supervised institution in terms of customer base, products and services offered by Bank (in terms of typologies and geographical locations);
- Judge the adequacy of measure and controls (including customer due diligence measures) of Financial Institution for ML/FT risks.

The risk-based supervision model (*i.e.* RBS) has four steps:

1. The risk factors identification;
2. The ML/FT risks evaluation;
3. The allocation of AML/CTF supervisory resources based on the previous step;
4. The monitoring and revision of the model.

In order to take advantage from RBS, the supervisors should have:

- A clear knowledge of ML/FT risk level in a country;
- On-site and off-site access to all relevant ML/FT information about risks linked to customers, products and services of the supervised institutions.

The risk profile assessment of a Financial Institution is performed periodically, based on the major changes and events in the management or operation of the Financial Institutions. The supervisors should be able to have operational independence and autonomy and each country should ensure a sufficient level of resource to gain it.

1.2 Interpretive Notes on Financial Intelligence Units

The FIU's definition and role are described in the FATF's Recommendation 29 and in the dedicated interpretative note. The FIU, which is an independent and autonomous unit, receives and analyses the suspicious transaction reports and all the relevant information about money laundering and Financial terrorism as well as related crime.

As first function, the FIU is a data collector that includes suspicious transaction reports and all other information as required by national legislation.

After that, the second function of FIU is represented by data analysis. The FIU is encouraged to adopt analytical software in order to increase efficiency of this function: in Table 1 we can see the amount of suspicious transaction reports analysed by Italian FIU collected through several platforms[1].

In order to enhance the value of information received and held by the FIU, the latter can perform two different analyses:

- *Operational Analysis* when the available information is used to identify the actors and the link among them;
- *Strategic Analysis* when, based on collected information, is possible to recognize the ML and TF patterns and trends.

The last FIU function regards the dissemination, which can be spontaneous or after competent authorities request, of those analyses.

Concerning the Italian case, the collection and management of data are supported by "*RADAR*" platform, in detail:

- The first assessment is done by Financial Institution that assigns a judgment (the latter is expressed by five values scale). It is represented by "Signaler's Rating" columns in Table 2.
- The second evaluation is performed with *RADAR*: using the above estimation, it assigned another automatic rating value that includes further information available in the FIU database. This rating value, expressed by five values scale, can be changed or confirmed by the FIU with the assignment of final rating that will be presented to investigative authorities. It is represented by "FIU's Rating" rows in Table 2.

From Table 2 we can see a convergence of rating provided by Financial Institution with the final Rating of FIU: the 43.9 % of warnings have the FIU's final rating equal to the signaler's one. When the automatic rating provided by RADAR does not correspond to the real risk level, the FIU updates it through a second level of analysis with the attribution of a final rating and a dedicated report writing for investigative authorities about the analysis. During this phase, FIU can demand further information to Financial Institution, refer to Revenue Agency's data and consult the foreign FIUs.
In case of money transfer warning, we have a third assessment level that examines a multiplicity of transactions jointly. In detail, the mentioned transactions have the following features:

- Reduced amount;
- Several interested parties;
- Geographic dispersion.

This further analysis level is performed in order to bring out significant connections that otherwise would not emerge.

Currently, the data analysis performed by FIUs is supported by SupTech tools, *i.e.* a set of data analytics tools that leverage on innovative technologies such as [4]:

- **Network analysis**, *i.e.* the investigating structures techniques via networks and graph theory;
- **Natural language processing**, *i.e.* a set of algorithms to analyse and comprehend human language;

[1] *e.g.* "*RADAR*" platform on "*Infostat-UIF*" portal, "*SAFE System*" with Italin investigative authorities, "*FIU.NET*". of European Union, "*Egmont Secure Web*" of Egmont Group, etc.

		Signaler's Rating			Total
		Low and Medium-Low	Medium	Medium-High and High	
FIU's Rating	Low and Medium-Low	16.8%	4.2%	1.3%	**22.3%**
	Medium	15.6%	8.8%	5.5%	**29.9%**
	Medium-High and High	12%	17.5%	18.3%	**47.8%**
Total		**44.4%**	**30.5%**	**25.1%**	**100%**

TABLE 2: Rating comparison between FIU and signaler [2]

- **Text mining**, *i.e.* a software that can recognise concepts, patterns, and further characteristics in a large amounts of unstructured text data;
- **Machine learning**, *i.e.* a methodology to solve a problem that updates itself via experience and without or limited human intervention.

These methodologies permit the processing of a large volume of data also coming from non-traditional sources (such as newspaper articles, social media) in order to strengthen the classic information and to decrease the number of false-positive alerts. It is important to highlight that the international nature of financial context involves the necessity of share the information among the FIUs of several countries. These data can be collected in different ways among the FIUs, therefore the FIU should be able to analyse a large volume of data, harmonizing them without compromise the data quality: it is one of the new challenges.

The issues that emerge with the increasing application of SupTech tools can be summarized in:

- **Computational capacity**, due to the large volume of data that represent the input of of SupTech tools;
- **Data privacy** and **confidentiality**, in particular it represents a limitation in the use of external resources;
- **Efficiency versus effectiveness**. Meanwhile, the efficiency of SupTech is easily quantified, we cannot affirm the same related to effectiveness, *i.e.* the output quality. Generally, the effectiveness is evaluated with regard to the reduction in the number of false-positives.

Despite the benefits of SupTech tools highlighted above, the human evaluation is still crucial to evaluate and verify the results of such engines.

2. Basel Committee Guidelines

As stated before, in July 2020 the Basel Committee put out an update of AML/CFT Guidelines published in January 2014 [3]: this new version regards the role of supervisors (*i.e.* paragraph 96 in Part IV) and the interaction and cooperation between prudential and AML/CFT supervisors (*i.e.* Annex 5). The document aims to promote the implementation of FATF Recommendation including the Basel expertise and considering the feature of these risks.

One key point of Basel Committee Guidelines is represented by *Customer Due Diligence*: to preserve the Financial Institution reputation, the latter should implement adequate policies and processes (in accord with its risk profile) in order to avoid the Financial Institutions' use for criminal activities. Additionally, the risk assessment for ML/FT Risks should be performed on different "degrees" (*i.e* country, sector, bank and business relationship levels) and a proper process should

inform the authorities about it. The international context and the size of Financial Institution can conduct a considerable amount of data that should be monitored with automatic process, in order to reduce and optimize the AML/CFT costs without compromise the data management structure.

Then the bank's profile is crucial in order to define the parameters that should be examined by IT monitoring system and the latter should be qualified to provide a detailed report to the Bank's board.

To properly manage ML/FT risks, the Basel Committee identifies three lines of defence:

1. The first line, *i.e.* **the business units**. The Financial Institution should provide to its employees the training programmes about AML/CTF procedures based on bank's risk profile and the ML/FT exposure of employees.

2. The second line, *i.e.* **the AML/CFT chief officer**. As stated in [3], the AML/CFT chief officer has "*the responsibility for ongoing monitoring of the fulfilment of all AML/CFT duties by the bank*". The AML/CFT chief officer is the contact point for authorities.

3. The third line, *i.e.* **the internal audit function**. The audit is performed on (i) the capacity of the bank's AML/CFT policies and procedures to manage these risks, (ii) the bank's staff capability to implement policies and procedures (and validate the IT system if it is present); (iii) the effectiveness of compliance; and (iv) the efficacy of the bank's training for relevant staff. In many countries we can have also the external auditors: in this case, the bank should ensure that they have the proper expertise and experience on bank's risk profile.

Moreover, due to the international context of the Financial System, we can have a Bank group with branches in several countries. This circumstance requires the implementation of group-wide AML/CFT processes and procedures. In this framework, the biggest challenge is to promote the information exchange among subsidiaries located in different countries, considering the issues and obligations related to local laws and regulations.

2.1 Customer Analysis

As stated in the fourth section of FATF Standards, Financial institutions should start a *Customer Due Diligence* (*i.e.* CDD) when:

- Establish business relations;
- Carry out occasional transactions[2];
- There is a suspicion of money laundering or terrorist financing;
- There are doubts about the veracity or adequacy of previously obtained.

With CDD, the Bank should identify the customer, the beneficial owner and verify their identity, understand the nature and reason of the business relationship. The Financial Institution can extent this analysis using a risk-based approach.

Concerning the risk factors that a Financial Institution should consider during the assessment, the European Banking Authority provided a Final Guidelines on CDD and risk factors that should be considered during the evaluation of ML/FT risk [8]. The CDD "degree" depends from the business-wide risk assessment, *i.e.*:

- In case of a low risk linked to a business relationship, the Financial Institution can apply a **Simplified Customer Due Diligence Measures** (*SCDD*). As stated in Final Guidelines [8], the Financial Institution can adapt the quantity, interval and kind of CDD measures to the low-risk level. For Retail Banks, the Final Guidelines [8] suggests the SSD measures that can be applied by Financial Institutions (paragraph 9.15 of Title II, [8]).

[2]The FATF Standards established that transactions should be *(i) above the applicable designated threshold (USD/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16.*

- If the risk associated with a business relationship is expected to grow, the Financial Institution must use the **Enhanced Customer Due Diligence Measures** (*ECDD*). As confirmed in Final Guidelines [8], the enhanced CDD measures do not replace the CDD measures, but they will be used additionally to the latter. The cases that should be treated as higher risk from the Financial Institutions are established in European Directive 2015/849 and they are collected also in Final Guidelines [8] (*e.g.*, the Financial Institution should use enhanced CDD measures when the customer is a PEP). For Retail Banks, the Final Guidelines [8] suggests the SSD measures that can be applied by Financial Institutions (paragraph 9.13 of Title II, [8]).

Usually, the evaluation of customer's risk profile is performed by Financial Institution via systematic procedure considering several relevant factors, *e.g.* "*customer's background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence (when different), products used, nature and purpose of accounts, linked accounts, business activities and other customer-oriented risk indicators*" [3]. Any material information gathered on customer activity should be used in renewing the client's risk assessment: these data should be retrieved by a reliable and independent source. In this assessment, the Financial Institution should also include the risk associated to complexity, transparency and size of products, services or transactions [8].

Based on the results of CDD, the bank should be able to decide if it is possible or not to open the new account and perform the transactions. This procedure whereby the Financial Institutions could reject to take part in or choose to terminate a business relationship with a customer due to a high level of ML/FT risk is named *de-risking*: with it, the customer could be blocked from financial services admission.

In order to mitigate ML/FT risks, the ongoing monitoring is a key aspects that should be performed concerning all business relationships and transactions to detect unusual transaction or patterns of activities. The management of CDD's information requires a focus on the following aspects:

- **Record-keeping**. All the information collected with CDD should be stored based on clear rules considering also the privacy laws, in other words "*they should include a definition of the types of information and documentation that should be included in the records as well as the retention period for such records, which should be at least five years from the termination of the banking relationship or the occasional transaction*"[3].

- **Updating of information**. With a regular upkeep activity of up-to-date information, the CDD results can be useful for the banks in order to monitor the suspicious activities properly and for the FIUs (or competent authorities) to comply with their own tasks.

- **Supplying information to the Supervisors**. The banks can be able to prove the suitability of its CDD procedure and of all policies and measures to evaluate and manage the ML/FT risks.

The Basel Committee puts the attention two features of terrorism financing: (i) it can derive from legal sources and (ii) it can be performed via small amounts. The Bank should be able, with CDD, to recognize potential financial terrorism transactions: the Financial Institution should examine the customer with the terrorist's list provided by authorities. For this reason, a bank should be capable to recognise mentioned transactions and to put in place funds freezing arrangements.

3. European Banking Authority Guidelines

Starting from January 2020, the EBA has the powers to lead, coordinate and monitor the AML/CFT efforts of all European stakeholders.

With the **leading role** on AML/CFT, EBA promotes the implementation of a risk-based approach for AML/CFT by competent authorities and Financial Institutions in the European Union. In order to achieve this goal, the EBA:

- Enhance the EU-wide AML/CFT policy and set regulatory expectations via standards, guidelines, and opinions;

- Support the competent authorities to have a harmonized AML/CFT approach in the EU and promote a consistent enactment of AML/CFT policy;
- With continuous consultation with all the stakeholders, the EBA promotes a common procedure to relieve ML/FT risks;
- Include the ML/CFT risk in the SREP process.

With the **coordination function**, EBA encourages collaboration and information exchange among the competent authorities. This aim is obtained with the following EBA's actions:

- Build a permanent internal AML/CFT standing organization (named AMLSC) where "*its main task will be to provide subject matter expertise to inform the EBA's work, and to prepare decisions for the EBA's Board of Supervisors*" [5];
- Create a new AML/CFT database with qualitative and quantitative data to support competent authorities' activities and promote investigations;
- Promote the cooperation among EU competent authorities and between competent and prudential organizations;
- Collaborate with FIUs and supporting the cooperation with third-country institutions.

The **monitoring role** of EBA consists to supervise the implementation of European AML/CFT Standards, supporting the competent authorities to mitigate their vulnerabilities in the application of the AML/CFT framework. This purpose is attained by EBA with the following activities:

- Leading thematic peer reviews on AML/CFT requirements;
- From EBA's database, encourage competent authorities to take corrective action in case of a law breach.

In March 2021, the EBA published its final revision of Guidelines on ML/FT risk factors with the aim of more effective AML/CFT risk-based approach implementation. In this revision, the EBA provides new guidance about risk factors of the CDD measures that should be considered in the assessment of ML/FT risks (as anticipated in the dedicated subsection 2.1) providing the details about the degree of CDD measures that should be applied in line with ML/FT risk level. Other major impacts regard the insertion of new sectoral recommendations for:

- **Crowdfunding platforms** (Guideline 17 of [8]). In this case, the risk can grow from the location of the crowdfunding service provider that can be in a high-risk jurisdiction. The provider should know their customers to block the misuse of crowdfunding platforms. The Guideline provides the risk factors that can rise the risk level, *e.g.* when (i) the provider allows early redemption of investments; (ii) no restriction on size, volume, or value of the transactions by the crowdfunding platform is established; (iii) the provider permits payments in virtual currency. In the same way, the Guideline lists the risk factors that can reduce the risk level, *e.g.* when (i) low-value limits on size and number of payment are present; (ii) the creation of multiple accounts on the crowdfunding platform is forbidden; (iii) limits on funds amount stored in an account are present.
- **Corporate finance** (Guideline 20 of [8]). When corporate finance services are supplied by firms, the latter should consider the associated ML/FT risks. In the Guideline are listed the risk factor that can increase the ML/FT risk level, *e.g.* when there is a lack of transparency in the transaction that is illogical considering the business purpose. Likewise, we have the risk factors that can decrease the ML/FT risk, *e.g.* when the customer is a Financial Institution with AML/CFT framework.
- **Account information service providers (AISPs) and payment initiation services providers (PISPs)** (Guideline 18 of [8]). These services are defined by Article 4 of Directive (EU) 2015/2366, *i.e.*:

  - *"an account information service provider (AISP) is a payment service provider offering account information services which in accordance with the definition in point 16 of Article 4 of Directive (EU) 2015/2366 means online services to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider);"*
  - *"a payment initiation service provider (PISP) is a payment service provider pursuing payment initiation services which in accordance with the definition in point 15 of Article 4 of Directive (EU) 2015/2366 means services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider)."*[8]

  They should be taken into account for ML/FT risk because in the first case, the AISPs are not included in the payment chain and do not have ownership of payment service user's funds; instead, in the second case, the PISPs, despite they are included in the payment chain, do not carry out themselves the transaction and do not keep payment service user's funds. Both of them should consider the risk factors related to the customer, distribution channel and country or geographical area highlighted in Guideline 18.

- **Firms providing activities of currency exchange offices** (Guideline 19 of [8]). Guideline 19 provides some circumstances for which the MR/FT risk level can grow with this activity: *e.g.* when (i) the transaction amount is oddly large for the customer profile or in absolute terms; (ii) the fund's origin information is not provided by the customer.

For all the above cases, the Guidelines [8] have provided dedicated recommendations about the CDD, in particular when SCDD and ECDD should be applied.

Thanks to the EBA role explained above, the EBA has reviewed the Guideline with a dedicated Consultation Paper [6] where they add further guidance on critical aspects showed by ESA and FATF reports. In order to have an effective implementation of the risk-based approach, the key points in the draft recommendation are:

- Point out the relevance of a sectoral and sub-sectoral risk evaluation from competent authorities. The "sectors" and related risk factors are defined in a Paragraph 25. This clarification impacts the risk profile determination and the latter should be defined considering the inherent risk besides the residual risks.

- Highlight the several supervisory tools and furnish the instructions for the better use of them by competent authorities. The supervisory actions used by competent authorities should be proportionate to ML/FT risks and not on the size and nature of the subject of assessment. This implicates that the RBA should be executed at cluster level where the latter is composed of comparable Institutions on the features side and ML/FT risk level.

- Stress the relevance of a follow-up process and how it should be done by competent authorities to define the better follow up actions;

- Furnish the guideline on the supervisory strategy and plan fulfillment. In lack of them, the competent authorities cannot put an effective RBS model into effect, and the supervisory actions cannot have an incisive effect.

- Emphasize the relevance of cooperation among the competent authorities and between the latter and the other stakeholders (*e.g.* tax authorities). In the mentioned draft guideline, there is a mention of the informal channels and private relations and relative riskiness for a correct assessment by competent authorities, therefore this informal tools should not substitute the formal channels.

4. European Legislation

In the light of AML/CTF rules, we can find the European commitment in the Fourth Directive (EU) 2015/849 and Fifth Directive (EU) 2018/843.

The freedom of capital movements and supply financial services, the constant evolution of technology and the means at the disposal of criminals required the adoption of European rules against the money laundering and the terrorist financing: this is the aim of Fourth Directive (EU) 2015/849. Due to international context of these crimes, the European Union recognises the importance of a compatible measures with the international context and, for this reason, it takes into account the FATF's Recommendation described before. The European Union acknowledges the importance of accurate and updated information of obliged entities (the latter, defined in Article 2) to track AML/CFT crimes, in detail [10]:

- *Member States should therefore ensure that entities incorporated within their territory in accordance with national law obtain and hold adequate, accurate and current information on their beneficial ownership, in addition to basic information such as the company name and address and proof of incorporation and legal ownership;*
- *Member States can, for that purpose, use a central database which collects beneficial ownership information, or the business register, or another central register. Member States may decide that obliged entities are responsible for filling in the register;*
- *Member States should make sure that in all cases that information is made available to competent authorities and FIUs and is provided to obliged entities when the latter take customer due diligence measures;*
- *Member States should also ensure that other persons who are able to demonstrate a legitimate interest with respect to money laundering, terrorist financing, and the associated predicate offences, such as corruption, tax crimes and fraud, are granted access to beneficial ownership information, in accordance with data protection rules. The persons who are able to demonstrate a legitimate interest should have access to information on the nature and extent of the beneficial interest held consisting of its approximate weight.*

The Fourth Directive (EU) 2015/849 does not consider only the "traditional" payment (*i.e.* large cash payment) but also electronic money products and all other activities performed online. Besides, the European Union, with this Directive, stresses the attention on the following topics:

- The importance of risk-based approach to identify, understand and mitigate the ML/TF risks;
- The assessment of risks relating to cross-border activities should be performed by such as the Expert Group on Money Laundering and Terrorist Financing and the representatives from the FIUs, therefore "*Member States should make available the results of their risk assessments to each other, to the Commission and to European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA) and European Securities and Markets Authority (ESMA)*" [10];
- The independence and autonomy of FIUs. The intent of FIUs is "*establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing*" [10]. The coordination and cooperation among FIUs are a significant features to obstruct ML/FT crimes: for this reason, the EU Financial Intelligence Units' Platform is defined as "*an informal group composed of representatives from FIUs and active since 2006, is used to facilitate cooperation among FIUs and exchange views on cooperation-related issues such as effective cooperation among FIUs and between FIUs and third-country financial intelligence units, joint analysis of cross-border cases and trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level*" [10].

The Fifth Directive (EU) 2018/843 represents an update of the previous one: terrorist attacks, the proliferation of alternative financial systems and the "*Action Plan for strengthening the fight against terrorist financing*" have required a new version of legal framework. The role of FIUs is remarked in Fifth Directive *i.e.* "*to identify the financial operations of terrorist networks, especially cross-border, and in detecting their financial backers*" [11]: to pursue this goal, FIUs should access to all necessary information without undue delays and promoting the FIUs cooperation to exchange financial, administrative and law enforcement information.

One of relevant update is to extend the scope of Fourth Directive including the *virtual currency networks* that should be monitored with a "*balanced and proportional approach*" [11]. This interest in **virtual currency networks** is due to their anonymity feature: in particular, the European Union established that "*FIUs should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed*" [11]. The Italian FIU received 732 warnings about the virtual assets in 2019, where 84.4% of them was provided by Banks and Postal services. However, from a qualitative point, the warnings about virtual assets are inadequate to understand the actors and amount of flows involved [2]. Next to the virtual assets, we have the stablecoins: the transfer of these instruments is based on blockchain and, at international level, some studies are ongoing to provide guidelines against the ML/FT crimes. Finally, also the anonymous prepaid cards can be used with ML/FT purposes, for this reason, the regulation establishes that the customer should be identified when the transaction amount exceed 50 € (in case of remote payment transaction).

The Fifth Directive (EU) 2018/843 has been recognized in Italian law with the D. Lgs. as of October 4^{th}, 2019, n. 125 entered into force on November 10^{th}, 2019.

5. Covid-19 Pandemic Impacts on AML/CFT Risk

As asserted in EBA's Opinion document [9], the Covid-19 pandemic impacts also the ML/TF risks. In particular, events like:

- The decrease of firms' revenues;
- The increase of remote on-boarding of customers.

Exposed the financial sector to new ML/FT risks. Furthermore, the pandemic has brought out new crimes, *i.e.*:

- **Misuse of government and emergency funds**. In this case, we need to pay attention to the destination of mentioned financial flows and enhance the control procedure of them when they are addressed to Countries with high ML/FT risks.
- **Frauds on the medical products sale**. As remarked by the Italian FIU, it is necessary to evaluate all the available data, in particular, possible incompatibility or contradictory elements between the financial operation and profile of the actors involved in the transaction. Moreover, the PEP's involvements should require an in-depth analysis (*e.g.* the assessment of emergency funds received with regard to customer activities).
- **Improper use of electronic payments and online services**. Regarding the first case, the UIF asked to monitor accurately the online transactions that can be related to the commerce of non-existent or counterfeit products. Concerning the second case, the increase of online services can augment the risk exposure of IT crimes (*e.g.* phishing fraud).

As stated in [1], the suspicious transaction should be signaled to FIU with promptness, highlighting the Covid-19 emergency connection. Finally, also the competent authorities have been impacted: in particular, they recognized (i) a quality decrease of CDD measures applied by Financial Institutions; (ii) a reduction of AML/CFT resources allocated.

Furthermore, also the supervisory activities of competent authorities have been impacted by the health emergency and they required a rearrangement of supervisory priority and plans. Therefore the inspections can be done remotely with virtual meetings and the EBA role, *i.e.* the support in terms of management, coordination and monitoring of competent authorities approach to the AML/CFT supervision, is remarked in EBA statement [7].

References

[1] **Banca d'Italia and UIF.** *Prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza da COVID-19*. Banca d'Italia and UIF, April 2020.

[2] **Banca d'Italia and UIF.** *Rapporto Annuale 2019*. Banca d'Italia and UIF, July 2020.

[3] **Basel Committee on Banking Supervision.** *Sound Management of Risks related to Money Laundering and Financing of Terrorism*. Basel Committee on Banking Supervision, May 2020.

[4] **Coelho, R. De Simoni, M. and Prenio, J.** *Suptech applications for anti-money laundering*. Banca d'Italia, October 2019.

[5] **European Baking Authority.** *Anti-Money Laundering and Countering the Financing of Terrorism*. EBA, February 2020.

[6] **European Baking Authority.** *Consultation Paper on Draft Guidelines on the riskbased approach supervision under Article 48(10) of Directive (EU) 2015/849*. EBA, March 2021.

[7] **European Baking Authority.** *EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic*. EBA, March 2021.

[8] **European Baking Authority.** *Final Report on Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions*. EBA, March 2021.

[9] **European Baking Authority.** *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector*. EBA, March 2021.

[10] **European Parliament and The Council of European Union.** *Directive (EU) 2015/849 of European Parliament and The Council of 20 May 2015*. Official Journal of the European Union, May 2015.

[11] **European Parliament and The Council of European Union.** *Directive (EU) 2018/843 of European Parliament and The Council of 30 May 2018*. Official Journal of the European Union, May 2018.

[12] **Financial Action Task Force.** *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Financial Action Task Force, October 2020.

Iason is an international firm that consults Financial Institutions on Risk Management. Iason is a leader in quantitative analysis and advanced risk methodology, offering a unique mix of know-how and expertise on the pricing of complex financial products and the management of financial, credit and liquidity risks. In addition Iason provides a suite of essential solutions to meet the fundamental needs of Financial Institutions.

ESSENTIAL SERVICES FOR
FINANCIAL INSTITUTIONS