Dipartimento del Tesoro

Italy's national money laundering and terrorist financing risks assessment drawn up by the Financial Security Committe

Up to date as of 2018

SUMMARY

www.dt.mef.gov.it

The Financial Security Committee
Department of Treasury
Directorate V - Prevention of Use of the Financial System for Illegal Purposes
Office V - The Financial Security Committee Secretariat

Address
Via XX Settembre, 97
00187 Rome Italy

Website
http://www.mef.gov.it
http://www.dt.mef.gov.it

The national analysis of the risks of money laundering and terrorist financing was drafted by the Financial Security Committee within the bounds of the powers provided by article 5, paragraph 6, of Legislative Decree no. 231 of 21st November 2007. The data and information used relates to the period 2014-2018.

This translation of the " National money laundering and terrorist risks assessment " in English is for information purposes only. The original Italian text is the official version, authorized by the Financial Security Commitee, of the "Analisi Nazionale dei rischi di riciclaggio e finanziamento del terrorismo" and prevails over the English version.

CONTENTS

INTRODUCTION

In the framework of the powers laid down in Article 5, paragraph 6 of Legislative Decree no. 231/2007, amended by Legislative Decree n. 90 of 25th May 2017, the Financial Security Committee (FSC) processes the national assessment of money laundering and terrorist financing risks (*National Risk Assessment* - NRA).

The analysis was conducted by a working group composed of the authorities taking part in the FSC, as well as other authorities with specific expertise on relevant topics issues and representatives from Italy's Presidency of the Council of Ministers, in accordance with the provision set out in Article 14 of the mentioned Decree. The analysis has also benefited from the collaboration of academic scholars and representatives, to professional regulatory bodies (SRBs) and private associations representing interested categories.

The conclusions reflect the shared assessment of phenomena, of threats and vulnerabilities, achieved by starting with information, data and analysis from a variety of multiple sources. The conclusions are the basis for strategic coordination of the policies of the relevant authorities.

The relevant authorities referred to in Article 21, paragraph 2, letter a) of Decree no. 231/2007 use analysis for the purposes of establishing the prioritisation and distribution of resources in order to improve the system of preventing and combatting money-laundering and terrorist financing. In addition to this, this analysis also allows them to optimise the practice of their own skills, depending on the level of risk encountered, and report to the FSC about the measures and criteria adopted in order to mitigate the risks identified in the analysis.

In accordance with Article 5, paragraph 7 of Decree no. 231/2007, on the basis of the information received, the Financial Security Committee (CSF) presents to the Minister of Economy and Finance the annual report containing the analysis of the activities for the prevention of money laundering and terrorist financing put in place by the relevant national authorities who contribute to the assessment, as well as direct proposals to make the said activities more effective.

I. UPDATE OF THE METHODOLOGY

The analysis was developed on the basis of the methodology already adopted in 2014 and subsequently summarised:

- assessment of the inherent risk of money laundering and terrorist financing through the detection of threats and criticalities of the socio-economic system;
- assessment of the effectiveness of the of the *Anti-money laundering/Countering financing of terrorism* (AML/CFT) in its preventative, investigative and repressive stages.

This model carries out a sectoral analysis for each category of recipients of anti-money laundering legislation: financial intermediaries, professionals and non-financial operators. In this section, vulnerability is appreciated in relation to the functioning of each category analysed (i.e., relative vulnerability). Despite starting with the available data and information, the assessment was fundamentally the result of a qualitative analysis, i.e., the merging of participating authorities' judgements towards a shared opinion. This opinion is based on data and information relating to the period 2014-2018 and is developed on scale of four values.

Finally, it should be noted that with respect to the risk assessment carried out in 2014, the supervision model of the Supervisory Authorities has changed in line with the recommended actions made by the *Financial Action Task Force/Groupe d'action financière* (FATF/GAFI), by the Basel Committee and by other international organisations, and the risk-based approach was strengthened. Therefore, the supervisory activities now take into consideration the relevant risk profile, also in relation to the nature, scope and type of activity carried out by the supervised entities. Therefore, with respect to the previous assessment, the supervised intermediaries are no longer classified based on the scope of their activities, but in relation to their specific risks to which supervised entities are exposed to determined on the basis of a specific system of statistical indicators.

II. MAIN OUTCOMES OF THE NATIONAL ANALYSIS OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS - SUMMARY

II.1 ANALYSIS OF THE THREATS AND WEAKNESSES OF THE SOCIO-ECONOMIC SYSTEM

The analysis is conducted by differentiating the assessment on money-laundering from the assessment on terrorist financing; in both cases the assessment is carried out at the national level.

The analysis also takes into account the vulnerabilities of the socio-economic system and especially the importance of the informal economy as well as the use of cash. Concerning the national situation, these contextual factors are hugely relevant for their influence on the inherent risk level in the country. With regard to corruption, the assessment does not intend to ignore its systemic nature and confirm the same methodological choice as the one adopted in the 2014 analysis, to assess the effects of corruption in the context of threats and not within contextual factors.

The characteristics of the economic and social system could broaden or contribute to contain the threat that the proceeds of criminal activities can be rechannelled into the formal, regulated economy. There are two elements to be taken into account by the analysis: the use of cash and the unobserved economy. Both factors continue to represent critical elements with a very significant influence on the Country's level of risk.

II.1.1 The use of cash in Italy

In Europe there is not in force an uniform ban on the use of cash above a given thresholds and the legislation in many Member States is absent, whereas in others it varies.

The European *Supra National Risk Assessment* (SNRA) therefore has highlighted that in countries where a legal threshold exists, vulnerabilities related to transactions involving a significant use of cash has been greatly mitigated by the ban of using cash above a certain threshold; in these countries, targeted checks and the preparation and circulation of anomaly indicators allow obliged entities to send more clear and detailed suspicious transactions reports to the Financial Intelligence Units (FIU). Because of this, preventative measures are considered by the Commission more effective in mitigating the high risk linked to cash.

In 2016, 129 billion cash transactions were made in the Eurozone. The countries which have the most significant share of these cash transactions are mainly the countries in Southern Europe but also Germany, Austria and Slovenia. With regard to the estimated value of these transactions, the countries with the highest percentage are Cyprus, Malta and Greece, followed by Italy together with Spain

and Austria. The Eurosystem's declared objectives include opposing the illegal use of cash for money laundering purposes. This is in line with the recent decision to suspend the issuing of the 500 euro denomination starting from 27th January 2019[a].

The results of the survey from the European Central Bank (ECB) on the use of cash. In 2016, the ECB conducted an extensive study at shops within the Eurozone[b], in order to estimate the value and the amount of payments made by cash, compared to other forms of payment.

The results of the study show, with regard to the sample of Italian residents,

that in 2016 cash was the most frequently used form of payment in shops: 86% of the transactions were paid for with cash, compared to just 79% registered as cash payments in the Eurozone.

With reference to the national distribution of transactions, the processing of data directly carried out by the Bank of Italy has highlighted how cash is the most frequently used form of payment for transactions made in shops across all Italian regions, albeit with significant differences. Cash has proven to be used less in the North but is more common in the Centre and South: the lowest percentages of cash transactions were recorded in Lombardy (81%), Sardinia (82%) and Tuscany (82%), while the highest ones were in Calabria (94%), Abruzzo, Molise and Campania (91%).

With regard to the use of cash as a store of value, 28% of those interviewed claimed that they keep cash on them even as a 'precaution' measure, mainly a figure between 100 and 500 euros. This percentage is higher in the South (32%) and lower in the North-west (24%), while the European average stands at only 24%.

Based on the available data, we can assume that in Italy, the use of cash is still widespread and represents a contextual factor of risk for money laundering and tax evasion[c], even though a growth in the use of other forms of payment has recently been noticed.

The introduction of further, effective threshold for cash payments after 2010 and more stringent controls with regards to combatting money laundering have discouraged the possession and use of the 500 euro denomination, by favouring

inflow at the Bank of Italy of both accumulated stock by residents in the previous years and new flows from abroad.

Provincial mapping of cash across Italy. The use of cash in Italy is not uniform. In order to respectively guide the private sector in adjusting its operation, when sensitive to the use of cash, based on the assumption that cash is a measure - albeit partial - of the risk of money laundering, we are introducing a risk indicator developed at the provincial level by the Financial Intelligence Unit (UIF).

Excessive use of cash: a risk indicator to the private sector. This indicator is based on a 'relative' measure of anomalies: for every euro deposited in the bank using payment methods other than cash, the amount is considered of cash

[a] To read about the possibility of use of high denomination banknotes for illegal purposes, see also the study published by the UIF: A. Cassetta, A. Di Filippo e V. Roversi (2016), "L'utilizzo delle banconote di taglio elevato come potenziale strumento di riciclaggio: lo studio del 2011 con nota di aggiornamento", Quaderni dell'antiriciclaggio – Collana analisi e studi, n.6, UIF.

[b] Henk Esselink, Lola Hernández, Study on the use of cash by households, Occasional Paper Series, N. 201, November 2017.

[c] On a micro level, the survey *Indagine sui bilanci delle famiglie* carried out by the Bank of Italy on family budgets allows one to establish a connection between the preference for cash and the socio-economic characteristics amongst households.

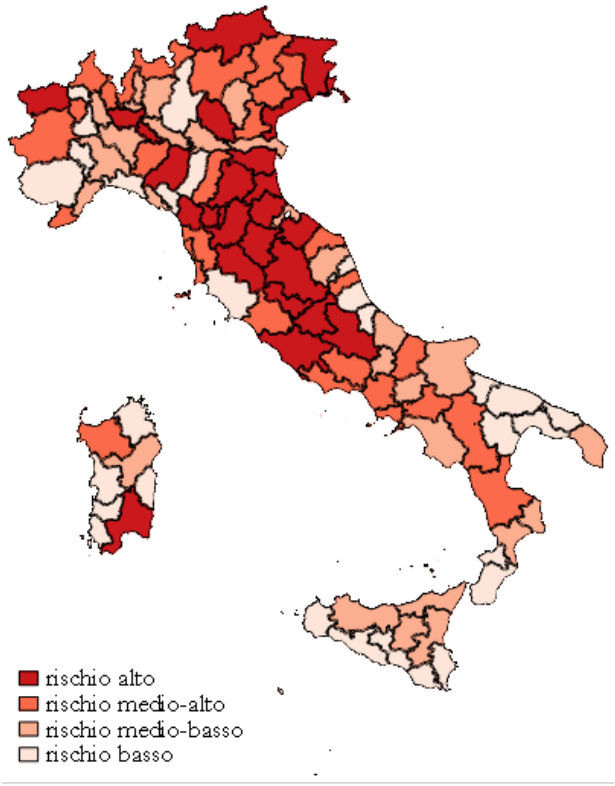
payments that are not justified by local, 'structural' socio-economic and financial factors.

In this respect, this indicator appears to be a useful measure that can be used to measure exposure of privates to money laundering risk.

For each province, the ratio was calculated between the number of anomalies detected at the bank-municipality level and the total number of bank-municipality combinations observed in the same province.

The mapping of this measure of risk across each province of Italy is presented in Figure 1, which distinguishes between four different levels of risk: high, medium-high, medium and low. The complete lists of corresponding provinces are contained in Table 1. The provinces standing out as having a 'relatively' high level of risk are mainly in central and northern Italy; the category below it, that of 'middle-high risk', includes some central and southern provinces as well some northern ones (mainly located in the north-east and on the border), the three groups being almost equal in number.

FIG. 1 – THE DISTRIBUTION OF RISK ACROSS ITALIAN PROVINCES: THE PROPORTION OF BANK-MUNICIPALITY ANOMALIES PER PROVINCE



Source: UIF

TABLE 1 – PROVINCIAL CLASSES OF RISKS . EXCESSIVE USE OF CASH: RISK INDICATOR FOR THE PRIVATE SECTOR

Risk classes	Provinces
High risk (27)	Aosta, Milan, Lodi, Bolzano, Udine, Trieste, Gorizia, Venezia, Verona, Parma, Bologna, Ferrara, Ravenna, Forlì-Cesena, Florence, Prato, Pistoia, Lucca, Siena, Arezzo, Pesaro-Urbino, Perugia, Terni, Rieti, Rome, L'Aquila, Cagliari.
Medium-high risk (28)	Imperia, Turin, Biella, Verbano-Cusio-Ossola, Varese, Como, Sondrio, Trento, Belluno, Pordenone, Treviso, Padova, Piacenza, Modena, Livorno, Pisa, Ancona, Ascoli Piceno, Viterbo, Latina, Frosinone, Campobasso, Caserta, Naples, Avellino, Potenza, Cosenza, Sassari.
Medium risk (27)	Savona, Alessandria, Novara, Pavia, Monza-Brianza, Lecco, Bergamo, Cremona, Mantova, Rovigo, Vicenza, La Spezia, Rimini, Macerata, Chieti, Isernia, Benevento, Salerno, Foggia, Lecce, Crotone, Catanzaro, Palermo, Messina, Enna, Catania, Nuoro.
Low risk (28)	Cuneo, Asti, Vercelli, Genoa, Brescia, Reggio Emilia, Massa-Carrara, Grosseto, Fermo, Teramo, Pescara, Barletta-Andria-Trani, Bari, Brindisi, Taranto, Matera, Vibo Valentia, Reggio Calabria, Trapani, Agrigento, Caltanissetta, Ragusa, Siracusa, Carbonia-Iglesias, Medio Campidano, Oristano, Ogliastra, Olbia-Tempio.

Source: UIF

II.1.2 The unobserved economy

In 2016, the unobserved economy[d] (the underground economy and illegal activities[e]) was worth approximately 210 billion euros, equal to 12,4 % of the GDP. The added value generated by the underground economy amounts to a little less than 192 billion euros, whereas the value connected to illegal activities (including turnover) is worth approximately 18 billion[f].

According to the data in the *Report* released by ISTAT in October 2018, the

[d] On the basis of the *ISTAT Report* of October 2018, in the years 2013-2016, the unobserved economy (NOE non-observed economy) includes those economic activities which, for various reasons, succeed in avoiding direct, statistical observation. The main components of the unobserved economy are represented by the underground economy and illegal economies; the statistical underground economy and the informal economy complete the spectrum.

[e] Illegal activities: they represent the productive activities involving illegal goods and services, or those, despite concerning legal goods and services, are carried out without adequate permission or entitlement. There are three types of activity that stand out: the illicit production and trafficking of drugs and psychotropic substances, sexual exploitation (prostitution cases) and tobacco smuggling.

[f] *Source Report* ISTAT, October 2018. See note d.

effect of the unobserved component of the economy on GDP, which had recorded an increasing trend in the period 2012-2014 (from 12.7% to 13.1%), in 2015 recorded an abrupt decrease, decreasing by 0.5% compared with the previous year. In addition, its composition changed significantly.

In 2016, the component relating to under-reporting of income counted for 45.5% of the added value (about a 0.6% decrease compared to 2015). The remaining part can be attributed for 37.2% to irregular work (37.3% in 2015), 8.8% to other components (irregular renting, gratuities and supply and demand integration) and 8.6% to illegal activities (respectively 9.6% and 8.2% in the previous year).

The sectors where the impact of the underground economy is higher lie with services activities (33.3% in 2016), trade, transport, accommodation, catering (23.7% in 2016), and also the construction industry (22.7% in 2016)[g].

Illegal activities considered in the compilation of national accounts (the illicit production and trafficking of drugs and psychotropic substances, sexual exploitation - prostitution cases - and tobacco smuggling) have produced a little less than 18 billion euros of added value (including auxiliary activities), with an increase of 0.8 billion euros, mainly due to the prices dynamic relating to drug trafficking.

Therefore, it is necessary to reiterate the “very significant” influence of the unobserved economy on the country’s level of risk.

[g] Source *Report* ISTAT, October 2018. See note d.

III. THE ASSESMENT OF THE SYSTEM'S INHERENT RISK OF MONEY LAUNDERING

III.1 CRIMINAL ACTIVITIES CARRIED OUT WITHIN THE NATIONAL TERRITORY

The influence of illegal activities on the Italian economy is relevant and finding in 2014 stated is confirmed.

Although there is not a unique and official economic estimate of the value of criminal activities, the various estimates (that range from 1,7% to 12% of GDP, according to the underlying definition and methods used[a]) contribute to supporting an absolute significance assessment of the threat that illegal proceeds are produced across the nation and are circulated back into the economical and financial loop of Italy and other foreign countries[b].

The financial crisis has offered further opportunities for criminality to enter into the economic framework. For example, financial difficulties, especially as to liquidity, can lead to the growth of usury, making businesses and individuals more vulnerable when criminals attempt to extend their control over the formal and legal economy.

The money laundering threat affecting our economy is therefore assessed as **very significant**.

On the other hand, the risk that Italy is the place where money from abroad is laundered is considered quite low by the majority of financial intermediares, because of the safeguards put in place against money laundering, the economic situation and the tax burden discourage such wealth from entering our country. The risk that capital from abroad is laundered in Italy is perceived by most financial intermediaries as low, since anti-money-laundering safeguards, as well as the economic situation and tax burdens discourage the entry of such capital in Italy.

[a] The criminal economy may be estimated according to both direct and indirect methods. The first ones are based on household surveys and on indicators related to crimes and crime, while the second ones assume the scope of criminal economy by comparing macroeconomic indicators. Estimates made by SOS Impresa belong to the first group, which in its 13th report of 2012 and also referred to in 2010, estimates the turnover of mafias to be 138 billion euros, corresponding to 8.7% of the GDP. Using the same method, *Transcrime*, within the National Operational Programme Safety 2007-2013, produces very different results: the turnover of illegal activities is reported to have amounted to 1.7 % of the GDP in 2010, equivalent to a turnover of between 17.7 and 33.7 billion euros. A study conducted by the Bank of Italy, in collaboration with researchers from some universities (cf Ardizzi et alii), uses a variation of the currency demand approach for separately estimating the component of the unground economy linked to activities classified as legal but carried out in a non regular way (due to tax evasion tax and contribution payments), from the illegal component in the strict sense (excluding violent crimes, theft, blackmail, extortion, robberies, usury; therefore, it especially concerns prostitution and selling illegal drugs). In the four years of 2005-2008, the amount of undeclared tax was estimated to be equal to 16.5% of the GDP, with the amount of inherently illegal activity being equal to 10.9%. Another academic study (Argentiero et al., 2008) has proposed a macroeconomic estimate of money laundering in Italy in the period between 1981 and 2001. The adopted model suggests that, during the period in question, the amount of money laundering taking place was equal to almost 12% of the GDP. The study also shows that the money laundering has a anti-cyclical nature, increasing in times of crisis (cf Signorini's speech, BDI 2012).

The safeguards and monitoring activities in place in Italy, especially with reference to the last decade, are qualitatively perceived as greater than in many other countries where money laundering is "easier". The analysis of external threats, i.e. the proceeds of predicate offence perpetrated abroad and intended to be channelled into Italian economy, will be further deepened as a result of the current analysis update.

III.2 ANALYSIS OF THE ACTIONS THAT GENERATE PROCEEDS TO LAUNDER

Based on the analysis of predicate offences carried out as per relevant indicators – *proxy* of economic impact, geographical distribution, and attributed social disvalue – a judgement on the significance of threats posed by predicate offences was given.

This judgement reflects the perception of the severity of the crimes considered, based both on the operational experience of the authorities in charge of preventing and combatting money laundering, and on that of the private sector.

The major criminal behaviours, not only for their financial impact but also for their wider consequences, are corruption, extortion, tax evasion and tax offences, usury, drug trafficking, bankruptcy and corporate offences, the latter having been particularly affected by a long period of financial crisis. Gambling, smuggling and counterfeiting, sexual exploitation and illegal waste trafficking are offences that, despite having a lesser degree of severity, present a significant importance within our system.

Corruption continues to pose a threat of the extreme relevance. It has been confirmed the view that the proceeds of this type of crime cannot be appropriately estimated, because in the first instance proceeds of such offence – even when it is appraisable - may also be other than financial in nature; in addition to that, the number of individuals reported or arrested for such offences has further increased.

In relation to drug trafficking, while it is believed that the estimate of its proceeds in the previous year (15.2 billion euros) has not decreased (as a matter of fact, the expense for purchasing drugs is estimated at 14.2 billion euros) there has been a definite increase of the number of people involved in this illegal market.

In relation to tax evasion, although the extent of this phenomenon now appears to be decreasing (estimate of the previous analysis was equal to 140 billion euros) and amounts to an average of 86.4 billion euros[b], the number of individuals reported/arrested for such crimes has increased.

The gaming industry, both illegal and legal, turns out to be of great interest for organised crime, for which gaming has historically been an important form of financing, as well as the management of the illegal trafficking of waste.

Sexual exploitation generates criminal proceeds that are mainly reinvested outside of the Italian economy. As a matter of fact, this crime is essentially perpe-

[b] The estimate refers to the average for the period 2011-2016, equal to a total amount of 86.4 billion euros. Not the entire above amount is estimated to be the proceeds generated from offences: 13.2 billion euros of this is due to non-payment of taxes and errors in completing tax returns (Relazione sull'economia non osservata e sull'evasione fiscale e contributiva, anno 2018).

trated by foreign criminal organisations, mainly from Romania or other eastern Europe countries, that generally reinvest the illegal proceeds back into their own country.

Except in specific cases, local criminal organisations have not shown a great interest in this illegal phenomenon. Human trafficking usually proves to be managed almost exclusively by foreign criminal organisations: to be more precise, it concerns individual organisations, each of which have their own organised structures, linked by and dependent upon a leader who tends to remain abroad. These criminal associations, noted by the term 'the new mafias', manage the market with a *modus operandi* typical of foreign mafia organisations. This means that in Italy and Europe, only the weakest organisations can be successfully targeted[c].

Organised crime remains the dominant and most worrying perpetrators of criminal behaviours, which however, does not exclude the significant role of foreign criminal organisations operating in the country. With the exclusion of tax evasion, almost the entirety of crimes carried out are for the most part and, in some cases, exclusively attributable to organised - including mafia-style - crime (e.g., drug trafficking, extortion, gambling, illegal waste trafficking, smuggling and counterfeiting), with particularly dangerous effects due to the integration process and overlapping between organised crime and economic crime.

III.3 CONCLUSIONS

Overall, taking into account the prevailing profiles linked to the proceeds generated by criminal activities in Italy and that a substantial part of these proceeds - although not specifically measured - is circulated back into the domestic financial and economic sectors, the threat of money laundering is considered to be **very significant**. By also considering the vulnerabilities of the socio-economic sector as very significant, in the final assessment the inherent risk takes on the maximum value attributable within the model (the so-called "very **significant** inherent risk").

[c] Source NRA 2014.

TABLE 3 1 SUMMARY ASSESSMENT OF THE MONEY LAUNDERING SYSTEM INHERENT RISK

Threat	Very significant				Money-Laundering inherent risk
	Rather significant				
	Lowly significant				
	Non-significant				
		Non-significant	Lowly significant	Rather significant	Very significant
		Vulnerabilities of the system: Use of cash and unobserved economy			

Key:

- Non-significant inherent risk
- Lowly significant inherent risk
- Rather significant inherent risk
- Very significant inherent risk

IV. THE ASSESSMENT OF THE INHERENT RISK OF TERRORIST FINANCING

As has emerged from the investigative evidences, terrorist activities require the availability of funds and resources, such as money, logistical facilities, weapons, counterfeit documents, masks and places of refuge.

Some international terrorist groups have taken on the image of real 'mafia-organisation' because, together with the ideological radicalism and terrorist violence, they have also expressed criminal business attitude, territorial control and international perspective: the essential features typical of mafia-style associations.

These criminal organisations were able to accumulate large financial resources on the basis of large-scale criminal activities: drug trafficking, oil smuggling and smuggling of cultural artefacts, weapons trafficking, tobacco smuggling, human trafficking and migrant smuggling, extortion and kidnapping, corruption and money-laundering. We are dealing with criminal activities that, in order to be carried out, need a vast complicity network even outside of terrorist groups. Funds may also have a lawful origin and may be transferred through traditional regulated systems (e.g. terrorist financing through MVTSs).

The international community, at different cooperation fora, underline how, in order to prevent terrorist financing, it is crucial to detect and cut off the financial flows aimed at financing such conducts in whatever way the flows are channelled.

The appropriation of considerable resources in countries occupied at the time by ISIS did not detract from the importance of both preventative and repressive actions aimed at intercepting the financial flows, revealing the accumulation points, the channels used to transfer funds and especially to identify, regarding the financing side, the international terrorism branching.

Terrorist financing, with respect to money laundering, presents rather peculiar characteristics: financial resources requested to meet operational and organisational needs are not generally very high. The funds typically have a lawful origin and their use for illegal purposes may be dissimulated through entrepreneurial or charitable activities, acting as a façade. The transfer of funds and resources takes place through both formal and informal systems. These characteristics make the possibility of identifying targets more and more difficult.

Such a camouflaging risks concealing the real extent of the threat and make the legal system seem exempt from illegal exploitation. We need instead to refine the preventative techniques, by basing them on a careful evaluation of the different elements concerning the financial anomalies of operations, subjective profiles of the authors, places of origin and the destination of the funds. It is therefore essential to widen our knowledge of the phenomenon by integrating all the available information both in the public and private sector, starting with the knowledge of the terrorist threat and the context in which it develops, in order to strengthen our ability to analyse and exploit such information.

IV.1 ANALYSIS OF THE TERRORIST THREAT

Domestic terrorism. The most concrete and relevant threat continues to be represented by the anarcho-insurrectionalist movement, in particular by the component which recognise themselves in the cartel 'Informal Anarchist Federation - IAF" (*Federazione Anarchica Informale-FAI*). It supports the far-reaching planning aimed at the globalisation of the insurrectional fight pursued by dozens of organisations around the world that have agreed to the proposal, launched at the end of 2010 by the Greek group 'Conspiracy of The Fire Cells', to recognise themselves in the brand 'International Revolutionary Front - IRF'(*Fronte Rivoluzionario Internazionale-FRI*).

In a context traceable to IAF/IRF, the publication of the document aimed at declaring the subversive strategies proposed by the team should not be underestimated, especially on websites in the area. The topicality of the threat and the relevant risk profiles connected are witnessed by the attack carried out in December 2017 against the Carabinieri barracks in the district of San Giovanni in Rome, where a device placed at the entrance exploded, as claimed by the IAF. This event is part of a much larger factual context that shows how, in recent years, the insurrectional, revolutionary project represented primarily by the IAF, also due to its international connections with similar organisations, has increased its offensive potential that, currently, is fuelled by unpredictable and spontaneous actions. The threat is therefore considered as **rather significant**.

With regard to the groups with Marxist-Leninist roots present across the country, we can state that they have favoured participating in campaigns about social issues, alongside also anarchistic and antagonistic subjectivities, with the viewpoint of "sharing the struggle' on sporadic themes, highlighting forms of sharing between anarchic-insurrectionist elements and others traceable to subversive Marxist-Leninist environments. This area, due to the scope of attacks and the projects pursued in the past, seems still worthy of significant in-depth analysis, even though no specific activism has been encountered in the last few years. The threat is considered to be of lowly significance.

The extreme right-wing eversive group in Italy is nowadays characterised by its multi-faceted nature and is still very fragmented, devoid of a unique and shared strategy, oriented towards the protection of social demands, and considered the only viable way to reach a consensus, especially amongst those most exposed to the effects of the current financial crisis. Right-wing terrorism, despite having regressed over the years, might find in the changed social balances, mainly due to migration, a suitable basis to fuel renovated processes of extreme identity seeks. However, at present no specific terrorist risk is identified.

International, religiously motivated terrorism. Even throughout 2018, the main threat perceived nationally continues to be that posed by Jihadist terrorism. Despite not holding any more a dominant position, it should be noted how Al-Qaida still represents a threat for European countries and their interests abroad. In this sense, and with a much more dynamic mindset, the danger of attacks from the cited terrorist organisation seems to be continuing against the Western targets, in the attempt to underline its true existence and dominance, taking advantage of the losses of influence suffered by ISIS/Daesh. The series of attacks in recent years, most of which were claimed by ISIS, confirms the exacerbation of the offensive of Jihadi terrorism, not least proving the effectiveness of the strategy based on the propaganda towards a community of web users, even through 'of-

ficial' social networks, a propaganda that has evolved content and delivers 'an accurate product', with even operating instructions to hit 'crusader countries' with an indiscriminate violence aimed at killing as many people as possible. In the last few years, in fact, a growth has been highlighted in the frequency of terrorist attacks, often consisting of individual actions, even with a decrease in the level of sophistication in the preparation and execution, which makes attacks unpredictable and highly lethal.

This context reveals how strategies of the widespread distribution of ISIS/Daesh propaganda, addressed especially to the general public through the web and social networks, are capable of having a significant impact on individuals more receptive to radical, Islamic ideologies (e.g. persons not well integrated into the socio-economic fabric). It has been noted (at least from 2015) that the Italian language has been used to broadcast instructions aimed at carrying out terrorist acts in Western countries.

In particular, ISIS/Daesh, despite the loss of the occupied territories, continue to represent a significant risk factor for Western countries and those within the European Union, including Italy, because:

- their ranks are characterised by a huge, international presence foreign militants, many of whom come from Western countries;
- they use a method distinguished by inflexible, blind and indiscriminate violence, which has even forced other Jihadi groups to distance themselves;
- they continue to obtain the financial resources necessary for survival, just from their activities;
- they stand out because of the huge amount of media coverage given to their actions, which acquire strong and effective propaganda content, aimed at generating effects in terms of proselytism and actions emulating the work of groups that are active on the Jihadi front. This does not exclude the chance of appeals being accepted by individuals who are difficult to identify or 'neutralise'.

The recipients of the propaganda message are individual extremists or small extremist groups, already present in western countries and mainly home grown. The phenomenon of the Foreign Terrorist Fighters (FTFs) returning from Middle-Eastern and north African areas of conflict is particularly dangerous, due to the military and operational skills that these people have acquired in the mean time and their additional violent, radicalised behaviour. According to the estimates of the European Police Office, Europol, more than 5,00o foreign fighters from Europe would have reached the Syrian-Iraqi battlefield over time.

In Italy, the threat is real and current. Our country is the subject of the hostile, propagandist activities of ISIS/Daesh, and still hosts radicalised individuals or individuals exposed to radicalisation processes. This particular phenomenon is the subject of repeated evaluations within the Anti-terrorism Strategic Analysis Committee (Comitato di Analisi Strategica Antiterrorismo - CASA), especially with regard to the consequences arising from the possible return of Foreign terrorist Fighters (FTFs). The latter in fact represent a major risk, because they may have been able to consolidate contacts, during the course of the conflict, with other militants from Europe; this could make it easier for them to relocate to countries

other than the ones where they lived before the conflict.

Individuals linked to our country in various ways, who have left for Syria or Iraq and are now about to come back to Italy, are currently being monitored. In addition, systematic monitoring has allowed us to identify FTFs that, starting from other European countries, have used Italy as a hub to get to or return from the area of conflict. No new departures of FTFs from Italy have been recorded (the last one dates back to August 2015) and currently the total number is 138 people[a], of whom 47 have died and 28 are returnees. Individuals under the Italian jurisdiction were reported to the judiciary authorities.

In light of the points described above, it is considered that even our country remains heavily exposed to the threat arising from religiously motivated terrorism, which is believed to be very significant nowadays.

International, non-religiously motivated terrorism. The activity of non-religiously motivated terrorist organisations, the majority of whom have a separatist or nationalist agenda (the Basque, *Euskadi Ta Askatasu - Na/ETA*, the Sri Lankan, the *Liberation Tigers of Tamil Eelam*/LTTE, the Kurdish, *Partîya Karkerén Kurdîstan* - PKK/KCK), represent a largely insignificant threat in Italy.

Thanks to the monitoring of the various components of the Kurdish opposition present in Italy, aimed at identifying the friction within the group and preventing any unsuitable projects, last June a Turkish citizen was tracked down and arrested under an arrest warrant for extradition, due to its participation in the terrorist group PKK.

TABLE 4.1 - THE RELEVANCE OF THE TERRORIST THREAT		
Threat	Appreciated/Perceived relevance of the terrorist threat	
	National Risk Analysis 2014	National Risk Analysis 2018
Domestic terrorism		
a. Left-wing eversion		
a1. Red Brigades area	Non significant*	Lowly significant
a2. Anarchic-insurrectionist area	Lowly significant	Rather significant
b. Right-wing eversion	Non significant	Non significant*
International terrorism		
c. Religiously motivated terrorism	Lowly significant	Very Significant
d. Non-religiously motivated terrorism	Not significant*	Lowly significant

**The judgement of 'non-significant' threat does not mean 'non-existent' or 'irrelevant' but rather that the strength of the threat is largely contained.*

IV.2 TERRORIST FINANCING

In relation to domestic (endogenous) terrorism, the terrorist groups that are typical of this area resort to forms of internal funding (e.g., self-funding). In the context of the sector survey, investigative evidence has not yet emerged, relating to the reliance on single, group and organisational funding typical of the multi-faceted subversive sphere.

With regard to international, religiously motivated terrorism, in the past few years, the terrorist threat has demonstrated itself with increasing, dramatic intensity; it has taken on new forms and has taken advantage, even in financial terms, of close relations with ISIS/Daesh forces, operating in conflict areas in the Middle East, and also with other politically unstable areas.

The threat, therefore, is imminent and "liquid": there are some terrorist organisations coexisting that still control remaining areas of land, affiliated organisations with well-structured networks, smaller groups and also individual terrorists. Essentially, the threat takes the form of an operational 'network' in which terrorists are organised in cells, i.e. flexible structures, capable of reconfiguring themselves based on contingent needs and operating in quite detached areas,

without the need of frequent contact or meetings between the various groups, as they are able to count on new forms of communication that make it even more difficult to intercept activity and the relevant financial flows[a].

Consequently, the related attitude of Islamic terrorist groups is to diversify, both in terms of the sources of funds/economic resources and methods of transferring funds.

As highlighted in the information provided by the FATF/GAFI concerning the evolution of this phenomenon[b]:

- the strategy of Daesh was based mainly on funds generated in controlled territories, resulting from the oil sale, extortion towards individuals and businesses, trafficking of cultural artefacts, the sale of gas and other natural resources, looting and robbery, kidnapping for ransom and donations. Furthermore, it is worth noting the appeal for informal channel for moving funds – Informal Value Transfer Systems (IVTS), by also using, where necessary, affiliated organisations working in western and northern Africa, Pakistan, Afghanistan and the Arabic peninsula.

In certain areas (even regarding Europe, in particular in the Balkan region), the use of official, legal structures, perceived as 'service hubs', in which obtaining financial resources and the handling of funds is frequently associated with the readiness of militants and the setting-up of logistical bases. This further confirms that the financing sources directly reflects the specific environment's nature of the groups and advantages they are able to take from different level of structuring. In a European context, the Daesh's structure named "*Immigration and Logistics Committee*" appears to be very significant. It is believed to provide support for the movement of fighters to and from Syria (as in the case of the operatives who moved through the Balkans to France to then became active in Paris in November 2015), and its logistics team also dealt with financial transfers to Europe.

This occurs in a scenario in which an 'organisational model' prevails which assigns utmost importance to the offensive actions of individuals and small groups working independently, and ensures that the funding methods are very difficult to detect as they often mover very small amounts of money.

- Conflicts in Syria and Iraq, as well as the terrorist attacks of the last few years, have focused attention on the role of foreign fighters, supported financially by individuals or by recruitment/facilitation networks that represent one of the main material support of criminal groups.

With reference to the economic resources used by *'Italian" foreign fighters* to go to the Syrian and Iraqi regions, certain information from intelligence services outline the existence of funding - even of a small amount - granted to the aspiring fighters from already deployed extremists on the spot or by radical groups present across the country. However, these cases are isolated as one can conceive that the majority of these foreign fighters have made use of their own sources. Some-

[a] It is underlined that, at this point in history, we are witnessing the evolution of ISIS from an entity founded as a "state", as a result of the territorial defeat, to a criminal organisation based on Al Qaeda's model.

[b] ISIL, Al-Qaeda and Affiliates Financing Update (FATF/GAFI, 2016 -2019).

thing that also deserves a mention are the movements (also attempted) of financial flows, mainly carried out via the money transfer systems by both foreign fighters recorded in the well-established national list, and reported extremists, even if only in transit in our country, in order to track their location and to trace their movements.

Staying on this point, it should also be pointed out that the unstoppable territorial defeat of Daesh in related geographical areas, therefore, their losing important positions, has resulted in a correlated decrease of the collection of funds and the overall liquid assets of the Islamic State.However, the recent attacks have confirmed the risks coming from the action of small terrorist groups, whose actions do not require high costs for planning and implementation and whose funding is produced mainly from the self-taxation of group members. In the same way, the lone wolves finance themselves and can give rise to 'instant' terrorist attack.

In other words, even though the implementation of hostile planning has often been characterised by modest financial charges, all the logistical aspects of the actions - renting cars, finding accommodation, the purchase and/or the creation of explosive material - require a prior, albeit minimum, financial base; therefore, the identification of the related financial flows is not only an analytical tool for defining the framework but is essential in the key reconstruction of terrorist networks and for identifying some offenders and, above all, a key element in a preventative viewpoint.

Both macro- and micro-financing are observed (*so called "fine dust financing"*).

With respect to the concept of macro-financing, one can note the use of non-profit entities (cultural associations, centres of religious culture, foundations for the creations of mosques, associations engaged in supporting activities).

In the case of Jihadist groups, the flows intended to support terrorist operations often consist of private donations; in particular, this occurs where money can be transferred without stating the reason for payment and the final recipient remains concealed. There are also charities which, in countries characterised by a noticeable socio-economic instability, combine charitable initiatives and actions aimed to support the local population with funding and recruitment activities and logistical support for terrorist organisations, which are sometimes a direct product of these charities.

Micro-financing uses Money or Value Transfer Services (MVTSs), as well as the network 'hawala'. With regard to the money transfer system, there is still currently the risk of it being used for terrorist financing. Over the last few years we have witnessed a considerable increase of the number of suspicious transactions reported by sector operators in question. In 2017 it was equal to more than 5,000 reports relating to about 111,000 transactions, and in 2018 it was equal to more than 7,000 reports relating to about 115,000 transactions. This increase shows a greater awareness of the risk in question. The vulnerability of the system, inter alia, continues to be linked to:

- The low amounts of money transferred and the difficulty in establishing their nature/destination;
- The fact that in these transactions, increasingly sophisticated techniques are used for splitting up sums of money, for preventing it from being traced.

Together with money transfer services, the *hawala* is one of the most popular and used tools in the Islamic world, especially in those areas where there is an insufficient banking/financial system. It must be considered that, in some parts of the world, it is the only option for the transfer of funds and has also been used by humanitarian organisations in areas where there the hawala is the only good-functioning system.

Also this tool, designed for lawful purposes (remittance services), continues, due to its characteristics (e.g., guaranteed anonymity of the parties involved, possibility of sending money to poor areas) to be used for moving funds for terrorist financing. This is especially the case in war zones (and in the closest areas to them) where access to banking services is often limited for terrorist groups active there and where the remittances services sometimes take on the role of the main financial establishment through which it is possible to transfer the funds across the border.

It is also necessary to outline the importance taken on by cash couriers, which physically transport cash

as an unintended consequence of the enhancement of supervision and control of operators that provide payment services. Most recently, a further scenario for financing was discovered during investigations on the trade of stolen cars. This implies that the phenomenon can avoid any preventative measures and only at a later stage be possibly noticed during the course of investigations by Law Enforcement Authorities.

There is also the need to look with greater attention, through in-depth financial analysis, even at phenomenon dissimilar from terrorist financing, including money laundering. Therefore, the methods used for terrorist financing may be the same as the typical methods used for money laundering, as in the case of false invoicing, which leads to reporting to the competent authorities, with subsequent analysis allowing us to make a link between the STR and terrorist financing.

On the subject of financing terrorism, prepaid cards and virtual assets

also present risks.

The use of electronic payment methods, which some terrorists active in the last couple of years have resorted to in Europe, highlights the crucial role of tracking financial flows as a critical factor for success in the fight against terrorism, especially in the case of individual or small cells. In the latter case, an aspect of particular risk would lie with prepaid cards, especially in the extent to which the relevant funds can be withdrawn, throughout the world, at Automatic Teller Machines, meaning it can be used for purchasing goods and services by any operator belonging to one of the main international payment companies. What should be considered is that, in some cases, cards have a high limit and the system allows third parties to top it up. Virtual assets, for their inherent characteristics, are a potential form of financing for terrorist organisations. The widespread use of these assets by terrorist organisations seems, as for now, to be low and has not yet managed to match the use that groups dedicated to organised crime make of virtual assets, in particular those active in cybercrime space. The number of known cases of virtual currencies used for financing of terrorism remains very low. Therefore, it would be a limited threat, but it is believed to have significant potentiality.

Finally, it should be noted that increasing attention, considering the current international situation, must be placed on new, digital forms of payment, carried out with a smartphone in the absence of a direct, physical contact with the client,

especially if not assisted by strong CDD measures. In relation to crowdfunding, albeit under attentive consideration, there were no cases regarding terrorist financing.

IV.3 CONCLUSIONS

Even despite being faced with sensitive elements highlighted above, one must observe the following considerations that can be made about Italy:

- unlike other European countries, Italy has not been affected by a significant number of fighters leaving for areas for conflict and, therefore, by a proportional, subsequent financial flow of from Italy to those areas, from relatives, friends and supporters;
- the nature of the Jihadist terrorist activity observed in Italy in recent years is largely confined to the broadcasting of propaganda on the Internet, to the vindication of terrorism as well as to interactions on messaging platforms with members from Jihadi organisations. With regards to international terrorism, few cases of self-funding and third-party funding emerged in order to make peoples' journeys towards areas of conflict much easier;
- the operational reorganisation, since 2015, of the Authorities responsible for prevention, Law Enforcement and repression with regard to the greater national and international terrorist threat. In particular, the establishment of specific organisational units dedicated to combatting terrorist financing as well as the strengthening of the information exchange in different phases (CASA, FSC) are now strongly consolidated in the current legal framework.

Having said that, although it is necessary to make a distinction between the terrorism threat and the terrorist financing threat, which the working group consider lowly significant, it cannot be underestimated that the scarceness of the amounts intended for terrorist financing make it particularly difficult to identify the related financial flows. Therefore, in light of the criticalities aspects of the socio-economic system are deemed very significant, it follows an overall assessment of the **inherent risk of terrorist financing** as **rather significant**.

TABLE 4. 2 - CONCISE EVALUATION OF THE INHERENT RISK OF TERRORIST FINANCING

Terrorist financing threat	Very significant				
	Rather significant				
	Lowly significant				Inherent risk of terrorist financing
	Non significant				
		Non significant	Lowly significant	Rather significant	Very significant
		Criticalities of the system: Use of cash and the unobserved economy			

Key:

- Non-significant inherent risk
- Lowly significant inherent risk
- Rather significant inherent risk
- Very significant inherent risk

V. EFFECTIVENESS OF SAFEGUARDS

The vulnerability analysis was conducted by breaking the system down into the following phases: prevention safeguards, investigative safeguards and repressive safeguards. This type of analysis is the same for money laundering and terrorist financing, except for the safeguards specifically designed to counter this phenomenon.

As a whole, the system of prevention and countering appears to be adequately responding to the threat that proceeds from criminal activities may be reintegrated into the financial and economic system. Changes in legislation and tightening of safeguards show that the system has been further strengthened and improved. In some cases, however, residual vulnerabilities which require operational intervention remain.

The cooperation between the Italian authorities is positive and further reinforced compared to 2014, continuing to serve as a strength of the system, especially among those authorities traditionally engaged in the fight against these phenomena. The Unità di informazione finanziaria (Financial Information Unit, hereinafter also UIF), the Guardia di Finanza (GdF, Financial Police), the Direzione Investigativa Antimafia (DIA, Anti-Mafia Anti-Mafia Investigation Directorate), the Supervisory Authorities and the Judiciary have effective collaboration channels, which can also mitigate certain regulatory shortcomings.

International cooperation still has room for improvement due to lack of collaboration on the part of some foreign countries.

V.1 PREVENTATIVE SAFEGUARDS

Vulnerability analysis is carried out for the sectors required to apply the anti-money laundering legislation on the basis of their ability to meet related obligations and the specific risk associated to their operations. With respect to the overall preventative anti-money laundering system, the analysis focuses on the following three pillars:

a) The customer due diligence;
b) Record-keeping of information relating to business relationships and relevant transactions;
c) Suspicious transactions Reports (STRs).

Where possible, profiles related to *organisation and internal controls* were also scrutinised.

Within the preventative system, areas of analysis include: safeguards applied by obligated parties, cross-border control and the processes of analysing suspicious transaction reports, transparency analysis of legal persons and trusts and analysis of the non-profit sector.

V.1.1 Safeguards applied by Obliged Parties

The anti-money laundering safeguards shall continue to be applied by the private sector in a non-uniform way, even though a growing awareness of the risks if there has been noticed with respect to the previous assessment (NRA 2014). The analysis shows, on the other hand, that the level of supervision exercised by the authorities over obligated persons has improved considerably as a result of the reinforcement of the risk-based approach. In general, the financial sector, professionals and non-financial operators, are performing adequately.

The private sector was analysed on the basis of two standpoints: the operational aspect of their specific characteristics and activity (so-called specific risk) and the vulnerability related to the application of anti-money laundering measures. The joint assessment of these two areas makes it possible to evaluate vulnerability in relation to the specific risks identified (e.g., relative vulnerability).

For financial intermediaries, the following should be noted.

The risk-based supervisory activity and subsequent targeted analysis by the Bank of Italy have made it possible to identify the organisational weaknesses still present among certain intermediaries, in particular with regard to the customer due diligence and the ongoing monitoring, which are instrumental to the analysis and subsequent suspicious transactions reporting activity. In this respect, inspections carried out by the UIF confirms such analysis.

Only a few remarks all related to obvious issues - were made on the correct keeping of the Unified Computerised System (*Archivio Unico Informatico -AUI*). The structurally low number of negative findings on record keeping in the Unified Computerised System, together with the absence of violations of the rules on the management of cash and bearer securities, confirms that the culture of compliance with anti-money laundering rules is now well established in these areas.

With regard to weaknesses concerning the customer due diligence, the greatest difficulties are still related to internal procedures and organisational measures. There are still critical elements in procedures for carrying out enhanced customer due diligence, correct customer profiling and ongoing monitoring of customers, which can turn out in the weakening of the overall process of active collaboration.

When verifying data about the beneficial owner of accounts and transactions, there are still areas for improvement with regard to the in-depth analysis of additional information provided by the customer during the identification process. This is especially crucial when conducting enhanced customer due diligence in case of ML high risk clients . Weaknesses often come as a result of the failure to take into account information available to the intermediary or due to the absence of sufficiently structured procedures, even after receiving reports or alerts from third party sources.

The number of findings concerning the process of detection and reporting of suspicious transactions is due to procedural weaknesses and organisational inefficiencies of previous phases of customer due diligence and monitoring, as well as - in certain cases – to the weakness of the responsible staff for assessing the transactions themselves. Further improvements of active collaboration can be achieved by increasing the capacity for analysis, concerning both computer applications and resources involved, by a suitable design and implementation of control structures and by adequate operator training.

Finally, in relation to the quality and robustness of the information support systems, the anomalies found are often linked to procedures and controls not correctly implemented or to material errors in operating instructions.

Banks and Poste Italiane have a high operational risk. Sector size, the broad spectrum of activities, the use of cash, and interconnection with foreign financial systems put them at very high risk of being used as a tool of money laundering and/or financing terrorism. Safeguards on the sector, which also benefit from the extensive use of prudential supervision mechanisms, help to reduce these risks; incisive supervision, together with a high level of awareness of possible ML/TF events (active collaboration is an indicator of the level of awareness), have a positive impact on the ability to apply averagely appropriate measures provided for by sector legislation. The vulnerabilities of preventative measures continue to be regarded as of lowly significance, with an overall judgement of **rather significant vulnerability**.

Supervised fiduciary service companies: the vulnerability of the prevention system linked to fiduciary service companies has improved compared to 2014, and it is lowly significant. However, in the face of a specific high risk, the resulting judgement is that of **relative rather significant vulnerability**. With regard to **other fiduciary service companies**, there remains a **relative very significant vulnerability**.

Adequate safeguards in line with an average operational risk are also in place for **Italian investment firms** (***SIM*** in the Italian acronym), **Asset management companies** (Società di Gestione del Risparmio – **SGR**), **Open-end investment companies** (Società d'Investimento a Capitale Variabile – **SICAV** in *the Italian acronym*), non-banking financial intermediaries (as defined in Article 106 of the Consolidated Banking Act), and the **insurance sector**. In the face of improved supervision, the resulting judgemen bears a **lowly significant relative vulnerability**.

Insurance companies and intermediaries of the insurance sector. The specific risk is at an average level and the sector is considered to be fairly well protected. However, compared to the lowly significant vulnerability of insurance companies, the vulnerability of safeguards of insurance intermediaries continues to be rather significant. Notwithstanding, it is also worth noting that more accurate information regarding the reduced number of obligated parties with substantial risk exposure is now available and a procedure of for collaboration between IVASS (the Italian Insurance Supervision Authority), the Bank of Italy and the UIF for on-site inspections has been launched. **Relative vulnerability is confirmed to be lowly significant.**

Electronic Money Institutions (EMIs) and **Payment Institutions** (PIs). A distinction should be made between Italian EMIs and PIs and foreign EMIs and PIs established in Italy. In the presence of a significant operational risk for both categories, the safeguards put in place by the former, together with the supervisory activities of the Bank of Italy and the UIF, determine a lower level of vulnerability - albeit **rather significant** - for **Italian PIs and EMIs** compared to **foreign PIs and EMIs**, which are instead marked as having a level of very **relative vulnerability very significant**. Progress may be made with the introduction of supervisory powers to oversee the central points of contact provided for by foreign PIs and EMIs, which has been brought into effect by recent legislation.

Financial agents, **credit intermediaries** and **money exchangers**. With reference to **financial agents** and **credit intermediaries**, the average specific risk assessment previously issued in 2014 remains unchanged, with the vulnerability of

preventative measures deemed as **lowly significant**. On the contrary, with regard to **money exchangers**, the evidence which emerged from investigative activities, led to the **specific risk** rising to a **medium** level, with the vulnerability of the prevention system being considered as lowly significant. The result of the relative vulnerability assessment for all operators comes out as a relative vulnerability lowly significant.

Professionals. The 2014 National Risk Assessment revealed an inadequate response, on the part of professionals, to the need for prevention of the economic and financial system being used for money laundering and terrorist financing purposes. Notably, the analysis attributed this inadequate response of the category somewhat to the fact that professionals had been involved in the preventative system successively, as opposed to the obligated parties belonging to the banking and financial system, in order to play an active role within the system as defined by the legislator. In addition, the effectiveness of the regulatory safeguards was also mitigated due to the greater difficulties encountered when controlling a category of obligated parties, such as professionals, which is numerous and wide-ranging in terms of activities and skills. This state of affairs, together with an operational risk deemed high, made the category's relative vulnerability very significant.

Italy's MER - Mutual Evaluation Report (FATF 2016) confirmed this assessment by identifying “a very inconsistent level of comprehension of the risks of money laundering and terrorist financing' and has shown the need for secondary legislation, or rules to support the Legislative Decree no. 231/2007 in force at the time, designed so as to improve risk assessment ability and thus effectively activate commensurate safeguards.

In general, it acknowledges the efforts made by self-regulatory bodies to adequately respond to the system's prevention needs together with an increased awareness of the risks to which they are exposed. However, to date, the same results of the 2014 analysis (2014 NRA) has been confirmed. **Notaries** are evaluated has having a **relative vulnerability rather significant** and the **relative vulnerability** of **chartered accountants and accounting experts** is **very significant**. However, a conclusive evaluation of the effectiveness of preventative safeguards as amended by the legislation now currently in force will be possible when such legislation is fully operational.

Finally, when referring to **lawyers**, it is still noted a low level of active collaboration. While we must agree that not all lawyers’ professional activity presents the same risk level, the need for additional data and completion of the self-assessment process will consequently require auxiliary in-depth risk assessment. The **relative vulnerability** of preventive measures can, therefore, be confirmed to be **very significant**. auditing firms in charge of auditing EPIs.

In light of the results of the inspection activities carried out by CONSOB (the National Commission for Companies and the Stock Exchange) and UIF, it is believed that the 2014 evaluation should be modified, with auditors in charge of auditing entities of public interest (EPIs) and entities subject to intermediate regime (ERI in the Italian acronym) raising the level of inherent risk to medium and rating the vulnerability of the preventive measures as of lowly significance, due to the effectiveness of the supervision exercised over the sector. Therefore, relative vulnerability was deemed as lowly significant.

Labour consultants are generally involved in an activity which, apart from any possible association with other certainly risky professions - such as that of a chartered accountant - are not considered to present problems specifically related

to money laundering (but rather to any problems of irregular work). For this reason, the specific risk of the sector is considered negligible, with **relative vulnerability lowly significant**.

The analysis of **non-financial operators** was focused on the categories that, on the basis of the findings of investigation, have proved to be more susceptible to occurrences of infiltration by criminal organisations: the gaming sector, cash-for-gold traders and real estate agencies.

The presence of criminal and Mafia organisations in the gaming sector concerns not just illegal gambling, but also significantly extends to the perimeter of the legal game activities. Given this contextual premise, the various types of game (not all currently included in the scope of the anti-money laundering legislation) **differ with regard to their specific risk and vulnerability profiles**. Among the forms of on-line gaming, gaming platforms from other EU countries operating under the freedom to provide services are very significantly vulnerable in that their financial flows go completely unmonitored by the authorities. Among the forms of gaming, *Video Lottery Terminals* (VLTs) must be reported, along with betting contests in the form of fixed odds betting because they can be used for money laundering operations.

With regard to **cash-for-gold** trading in particular, the financial crisis has led to its growing popularity. Several investigative activities have confirmed both its high operational risk and its vulnerability, which have led the EU and then the national legislators to introduce new regulation that have intensified monitoring and control activities. Therefore, the **relative vulnerability is very significant**.

The **real estate sector** is one of the ideal sectors for the re-allocation of the proceeds of criminal and Mafia organisations and of foreign illicit capital. Even though sales are detected by other categories that are more mature in the implementation of preventative measures, real estate agencies continue to have little awareness of their role as anti-money laundering gatekeepers in a context of relevant risk. Therefore, **relative vulnerability was assessed as very significant** overall.

V.1.2 Cross-border controls

These controls have a considerable strategic value both in the light of the use of cash in the country and the flows of illicit capital - normally of Italian origin - into or out of the country. In this respect, available information has shown that as money transfer control activities have increased, so has the increase in fraudulent cross-border currency transfers.

Based on models analysing cross-border cash movements, links have also been identified with flows of goods at risk. This especially concerns travellers and shipments to or from countries affected by high levels of institutional or military instability in the Middle East and Africa.

On the whole, the process appears to be safeguarded by cooperation at both a national level, with specific protocols in place, and at an international level, where both the Customs and Monopolies Agency and the Guardia di Finanza make positive use of collaborative procedures within their competencies.

V.1.3 Financial Analysis of Suspicious Transaction Reports (STRs)

Suspicious Transaction Reports (STRs) have showed a continuous and signifi-

cant increase in the ten years of UIF's operation, from 14,602 in 2008 to 71,758 in 2014 and 93,820 in 2017 (cf Table 5.1). In 2016, the flow of STRs was strongly impacted by the voluntary disclosure[a] measures for the repatriation of funds held abroad, which brought the number of reports to over 100,000 (see below).

TABLE 5 .1 REPORTS RECEIVED

	2014	2015	2016	2017
Absolute Values	71.758	82.428	101.065	93.820
Percentage changes compared to the previous year	11,1	14,9	22,6	-7,2

This trend appears to explain the remarkable ongoing increase in the level of awareness regarding the active collaboration role in the process of preventing money laundering and terrorist financing. Such awareness is expressed, above all, by banking and financial intermediaries, with the involvement of a growing number of operators belonging to other categories of obligated parties. Likewise, the quality and exhaustiveness of reports is constantly increasing.

The process of analysing STRs is proving to be largely effective. There has been a considerable increase both in the number and quality of reports by obligated parties, even if not uniformly across all categories. This provides the UIF with a fundamental wealth of information, effectively managed through the use of integrated IT systems and procedures for assigning risk levels. As a result of the process's increased efficiency and effectiveness, the number of reports transmitted to and analysed by investigative Authorities is growing. Finally, the increase in the number of STRs with relevance in judicial proceedings is a good indicator of this analysis.

V.1.4 Assessment of transparency

Transparency is understood as the ability of national authorities to have timely access to information on the beneficial owner.

Profiles of potential vulnerabilities in terms of transparency of the property remain for those entities having links with tools that can shield property (trusts set up in the Country or fiduciary companies) or foreign corporate entities, especially in jurisdictions that allow for forms of corporate anonymity or which do not have adequate forms of information gathering, or, finally, that they are little or no collaborative to any requests for information exchange.

The specific risk of legal persons is confirmed as at a **significant (relevant)** level. In relation to trusts, the specific risks of "national" E.g. trust set up in the Country) and foreign trusts were assessed in different ways. For "**national**" trusts, a **relevant** specific risk is detected, given the updated regulatory framework on the subject. As for **foreign** trusts, the risk remains at a **high** level.

As far as regulatory measures are concerned, the renewed regulatory framework increases the level of transparency of legal persons and, in particular, of trusts, especially for legal persons and national entities.

These elements contribute to the view that as far as transparency is concerned, **national** legal persons and trusts have a **rather significant vulnerability**

level. With regard to **foreign** trusts, in view of the high risk and persistence of very significant vulnerability to transparency, the vulnerability of foreign trusts is still **very significant**.

V.1.5 Analysis of The Non-Profit Sector and Risk of Abuse for Purposes of Terrorist Financing

In the first NRA, the overall risk of abuse for terrorist financig was assessed in relation to the entire NPOs sector. Given that the non profit sector as whole was deemed as not exposed to the risk to be abused for terrorist financing such risk was considered as negligibleSince 2014, an analysis of the sector as a whole has been carried out, in order to identify the part of the non-profit sector exposed to the risk of terrorism financing. The analysis was also carried out in order to assess the effectiveness of the existing safeguards and controls in preventing, investigating and detecting abuses for terrorist purposes.

In general, it confirms 2014's findings regarding the effectiveness of the prevention system: the various types of checks carried out by the competent public authorities were considered to be pervasive and, while covering multiple aspects, ensured an adequate level of transparency in the sector, despite its fragmentation and the many authorities responsible for oversight.

In its entirety, the non-profit sector whose potential is limited to non-governmental organisations (NGOs) has a low risk of being abused for the purposes of terrorist financing. This is particularly true in the case of NGOs that operate at an international level in crisis areas such as in Iraq and Syria in particular, and with Islamic associations. At the same time, it acknowledges the positive and fundamental impact of the authorities' monitoring of the system. Therefore, the vulnerability of preventative measures applied to the non-profit sector are evaluated as of having low significance.

V.2 INVESTIGATIVE SAFEGUARDS

The in-depth investigative analysis of STRs. For the Guardia di Finanza (GdF) and the Direzione investigativa antimafia (DIA), Suspicious Transaction Reports and financial analyses from the Financial Intelligence Unit (UIF) bear a wealth of information and are considered instrumental in their operations. This is testified by the significant number of STRs related to criminal proceedings or considered of investigative interest.

Legislative Decree no. 90/2017 confirms the methodology according to which in-depth analysis of STRs transmitted by the FIU is carried out by *GdF* - Nucleo Speciale Polizia Valutaria (Special Currency Police Unit, NSPV) and *DIA*. The Decree also strengthens the role and functions of the Direzione Nazionale Antimafia e Antiterrorismo (National Anti-Mafia Directorate, DNA) that becomes the recipient of up-to-date "informative knowledge" aimed at linking to pre-existing or new criminal proceedings those Suspicious Transactions Reports presenting subjective recurrences (i.e. natural/legal persons), and/or those STRs the characteristics of which enable the anti-mafia prosecutor to solicit specific indictments.

Unlike the analysis carried out in 2014, there is currently a distinction between investigations concerning STRs for money laundering (GdF and DIA) and

those regarding STRs for terrorist financing (GdF). With reference to the process of in-depth investigation of STRs, the vulnerabilities identified in the previous NRA are considered to have been eliminated. Overall, this process is considered to remain effective, with its vulnerabilities assessed as bearing low significance.

Investigative activity in the fight against money laundering. In general, the tools and instruments of the judicial police facilitate highly effective investigative action (interceptions, searches, undercover operations, suspect arrests, and precautionary measures). More pervasive investigative tools can then be used when the offence of money laundering or re-use of illicit capital is linked to organised crime offences.

In light of the numerous investigations that have been successfully completed, the overall process can be considered as effective, even though some vulnerabilities still remain.

The criticality identified in the previous NRA regarding the lack of criminalization of self-laundering were overcome with the introduction of this offence into the Italian Criminal Code.

Also, the criticalities identified both at the level of international cooperation and stemming from Italy's national failure to implement provisions for the so-called 'Joint Investigation Teams' were resolved in 2016 with a measure regulating the setting up and functioning of the 'Joint Investigative Teams'. There are no known vulnerabilities that could compromise the effectiveness of the investigative processes focusing on money-laundering and self-laundering in a significant way (namely non-significant vulnerabilities).

Investigative activity in the fight against terrorist financing. The investigative activity carried out reveals different experiences among the police forces, including the work carried out by the GdF, with specific regard to aspects related to terrorist financing. On the international cooperation front, formerly highlighted issues regarding the lack of adequate cooperation on the part of countries experiencing phases of socio-political or institutional instability are reiterated.

V.3 REPRESSIVE SAFEGUARDS

Ability to prosecute offenders in the fight against money laundering. Over time, effective anti-money laundering mechanisms have been developed, including the introduction of the offence of self-laundering.

Ability to prosecute offenders in the fight against terrorist financing. The introduction of the penal provision, Law no. 153 of 28 July 2016, relating to the financing of terrorist conduct, further strengthened the sanctioning system established by the law, thus helping to strengthen a system already considered effective in the aforementioned analysis. Furthermore, the experience of the police forces, even in the face of adversity regarding international cooperation, suggests a vulnerability of low significance, even if exogenous in respect to our system.

Activities of seizure and confiscation in the fight against money-laundering. Firstly, the criminalisation of self-laundering has facilitated the overcoming of operational difficulties occurring in the previous NRA, concerning the implementation of measures for the seizure and confiscation of assets.

International cooperation has also seen improvements in the form of judicial collaboration between States. This allows for the recognition of foreign judicial titles by the State where the assets involved are located and brings the principle

of mutual recognition of confiscation orders into force. The Italian system is a mixed system, in which the rules of the Criminal Code coexist with those on the subject of prevention measures. These measures allow the residual criticalities to be controlled in such a way as that the system as a whole is considered effective and its vulnerability non-significant.

V.4 SPECIFIC MEASURES REGARDING THE FIGHT AGAINST TERRORIST FINANCING

The system for combating terrorist financing makes use of the preventive, investigative and repressive activities typically used against money laundering and organised crime. Furthermore, the system enforces specific measures deriving from the resolutions of the United Nations Security Council and domestic transposition measures and related national measures, where needed. At an organisational level, the key to the implementation of these measures is the Financial Security Committee (FSC).

The vulnerability relating to the timeliness with which EU regulations incorporate UN sanctions has been resolved with the introduction of national freezing measures, which stipulate that, pending the adoption of EU regulations, the listing decisions of the UN shall be enforced at a national level with a decree adopted by the Minister of Economy and Finance on the proposal of the FSC.

VI. CONCLUSIONS AND ACTION LINES

The updated national analysis of the risks of money laundering and terrorist financing testifies that Italy is still exposed to such risks.

In particular, in the context of threat analysis, the inherent risks of money laundering and terrorist financing are very significant and rather significant respectively.

The system as a whole is deemed as satisfactory. The legislative changes and the improvement in prevention measures that have been implemented since the first national risk assessment have shown that the system has been further strengthened and improved. The same observation can be made for the effectiveness with which the preventative, investigative and repressive processes are effectuated. The objective is to identify action lines that can further support the strategy already jointly pursued by the authorities with a view to increasing the effectiveness of the system.

The action lines highlighted reflect the characteristics of sectoral analysis, broken down into:

1. Safeguards applied by obligated parties
2. Legal persons and trusts
3. Specific measures to combat terrorist financing

VI.1 SAFEGUARDS APPLIED BY OBLIGATED PARTIES

In relation to the level of relative vulnerability identified by assessing the specific risk profile of each operator, desirable interventions are marked by different levels of priority as indicated in Table 6.1. The following is an analysis of obligated parties: financial intermediaries, non-financial operators and professionals.

Financial intermediaries

As far as financial intermediaries are generally concerned, the supervisory and preventative system remains well-equipped to deal with a significant volume of customers and operations throughout the country. First and foremost, the implementation of the risk-based approach by the authorities supervising financial intermediaries has resulted in greater overall effectiveness of the system. In addition to the internal controls required by law and the supervision carried out by the Bank of Italy, IVASS and CONSOB, it should be noted the institutional activities of the UIF and of those GdF Units which identify and challenge administrative violations within their respective areas of responsibility.

In the long term, the existing control mechanisms and the human resources dedicated to them should be maintained. In addition, it is necessary to promote, together with dedicated associations, adequate and pervasive training interven-

tions to eliminate procedural failings in the performance of enhanced due diligence, correct profiling and continuous monitoring of customers, as well as continuous updating and sharing of abnormal patterns identified by the UIF.

Due to the nature of their activity, trust companies present a high risk of opacity, which the preventative system is already aware of. Therefore, this category of intermediaries must continue to be very closely monitored, with a specific focus on trust companies that are not subject to the supervision of the Bank of Italy.

For brokerage companies (*Società di Intermediazione Immobilia - SIM*) and asset management companies (*Società di Gestione del Risparmio – SGR*), it is necessary to use the existing safeguards, with particular attention to operations evaluated as being at risk (e.g., the transfer of real estate).

As far as Electronic Money Institutions (EMIs) and Payment Institutions (PIs) are concerned, there is still a need to strengthen supervision activities, especially on those which are foreign but established in Italy. The new regulations that provide for the extension of supervisory powers over foreign PIs and EMIs established in Italy, through affiliated entities and agents, are a step in this direction.

Agents, credit brokers and foreign currency exchangers are sectors in which there is a regulated system of access, but control mechanisms must be strengthened across the nation. Inspections have confirmed that the distribution network is the weakest link in the service. In relation to currency exchange, it is necessary for operators to report mandatory data to the OAM in order for it to obtain an adequate representation of the sector's features. Moreover, on the basis of a wider information set, it considered a priority to strengthen the system of monitoring and supervision.

The insurance industry is considered to be fairly well covered. However, there are still some vulnerabilities regarding customer due diligence, the correct identification of beneficial owners and suspicious transactions reporting. Consequently, it is necessary to continue to urge insurance companies to strengthen corporate safeguards aimed at acquiring more reliable information for risk assessments and ensure prompt reporting of suspicious transactions. With regards to insurance intermediaries, investigations have shown that the formalities required by the legislation are accomplished by using tools and procedures made available by the head insurance companies.

Professionals

The regulatory changes that have taken place at a primary and secondary level show that the prevention system is being strengthened. In addition, the increasing number of suspicious transaction reports sent out reveals professionals' increased awareness of money laundering risks, which is less than their awareness of the risk of terrorist financing. It is believed that there is room for improvement in terms of both customer due diligence and the quality of reports submitted. It is fundamental that the authorities maintain a constant dialogue with professional categories. In particular, it is also considered necessary to further improve analysis of the lawyers by identifying the typical professional practices most susceptible to the risks of money laundering and terrorist financing and, finally, to assess the overall level of exposure. As a result of this analysis, the Guardia di Finanza's risk based inspection activities will be directed in a even more coherent and efficient manner.

With regard to the statutory auditor profession, there is still the need to promote more dialogue and training, particularly in light of the fact that persons normally regulated by other means may gain access to this professional category if they acquire appointment by a PIE.

With regard to labour consultants, although their area of operation is not considered to present problems specifically related to money laundering (rather to any problems of irregular work), Legislative Decree no. 231/2007, as amended by Legislative Decree no. 90/2017, has included them among the subjects required to fully comply with the rules on anti-money laundering and terrorist financing. It is considered necessary to launch awareness-raising and training activities for persons belonging to his category.

Non-financial operations

For non-financial operators, due to being subject to potential and definite infiltrations of organised crime, further harmonisation and supervision interventions should be pursued.

In this sector, STRs also continues to bear strategic importance. Reports from persons different from financial intermediaries may offer various hints for gaining more insight into and knowledge of a certain category of obligated parties. It is desirable not only to further strengthen supervisory measures, but above all to increase understanding of the features of the sector.

With regard to **cash-for-golds** operators, legislative changes introduced by Legislative Decree no. 92/2017, together with the specific nature of the new regulations, prompt us to consider the regulatory safeguards as more efficient. In addition, the registration of cash-for-gold operators allows for a constant census of the number and type of operators in the sector. However, given the current economic function of operators in the country, out-reach interventions are necessary to increase awareness of their obligations, not least by also establishing guidelines and continuous monitoring.

With regard to gaming operators, the recent introduction of primary and secondary legislation facilitates the mitigation of risks connected to the sector. With regard to supervision, existing safeguards in the currently most vulnerable sectors can be improved, together with the following-up and strengthening of monitoring processes.

The overall analysis carried out thus far can be summarised in the following table.

TABLE 6.1 - PRIORITY OF INTERVENTIONS FOR CATEGORIES EXAMINED			
	Dialogue and training	Operational/ regulatory/ legislative interventions	Strengthening activities of analysis, supervision and control
FINANCIAL INTERMEDIARIES			
Banks and Bancoposta			
domestic EMIs and PIs			
foreign EMIs and PIs			
Finance companies under article			
106 SIM and SGR			
Insurance companies			
Insurance intermediaries			
Trust companies (BI),			
Trust companies (MISE)			
Agents, brokers and currency exchangers			
PROFESSIONALS			
Notaries			
Avvocati			
Chartered and expert accountants			
Statutory auditors			
Employment consultants			
NON FINANCIAL OPERATORS			
Gaming and betting operators			
Cash-for-gold operators			
Real estate agencies			

Key for intervention priority levels:

- Low Priority
- Low-Medium Priority
- Medium-High Priority
- High Priority

VI.2 LEGAL PERSONS AND TRUSTS

Different levels of priority are assigned to interventions according to the level of relative vulnerability identified against the specific risk profile.

In relation to the criticalities identified in the category of legal persons and trusts, the following are necessary:

- the systematic identification of the final beneficiary related to the enterprises, and the necessary European and international collaboration, allowing the authorities to have timely access to this information.

Regarding the legislative framework, it is necessary to finalise the implementation of the Fifth Directive, which requires the sharing of national registers at a European level. Following the mentioned implementation, the adoption of the decree on the centralised register will be required.

- the implementation of safeguards regarding the customer due diligence on the part of obligated persons (professionals) when they provide services to companies.

These considerations apply to both categories examined, with a greater emphasis on the trust sector, which is increasingly used for illicit purposes, in particular for the commission of tax, money laundering and bankruptcy offences. In this regard, the need to acquire information about both professionals who have played a role in the establishment and/or management of domestic and foreign trusts, and trustees with the residence, registered office or administrative centre of their activities in Italy and abroad, is essential for the mitigation of critical issues related to this legal instrument.

In relation to the more problematic nature of trusts, a distinction must therefore be made between "domestic" trusts and foreign trusts (EU, at present, and non-EU trusts). With regard to the latter, supervision and control activities need to be strengthened and reinforced.

The analysis above regarding the priority of interventions for the categories of legal persons and trusts, can be summarised in the following table.

TABLE 6.2 - PRIORITY OF INTERVENTIONS FOR LEGAL PERSONS AND TRUSTS

	Analytical activities	Dialogue and training	Operational/ regulatory/ legislative interventions	Strengthening of supervision and control
Legal persons				
National trusts				
Foreign Trusts (EU and non-EU)				

Key for intervention priority levels:

- Low Priority
- Low-Medium Priority
- Medium-High Priority
- High Priority

VI.3 SPECIFIC SAFEGUARDS FOR THE FIGHT AGAINST TERRORIST FINANCING

Given the criticalities identified, it is necessary to:

- encourage the reporting of suspicious transactions on the part of the more at-risk categories, and to do so also through specific training activities;
- ensure the fulfilment of disclosure obligations by Designated non-financial Business and Professions (DNFBPs) and to reinforce control measures through the relevant supervisory bodies.

The non-profit sector. Greater coordination between the relevant authorities in charge of the various aspects of the sector is desirable, in order to promote the dissemination of information on the specific issue of terrorist financing and related risks of abuse of the non-profit sector. This should aim to be achieved also through guidelines, workshops and targeted activities to raise awareness among associations.

Interventions have different levels of priority in relation to the level of risk identified.

TABLE 6.3 – LINES OF INTERVENTION

	Analytics activities	Operational interventions	Regulatory interventions	Legislative interventions
Listing, de-listing and freezing				
The non-profit sector				

Legenda sui livelli di priorità degli interventi:

- Priorità bassa
- Priorità medio-bassa
- Priorità medio-alta
- Priorità alta

THEMATIC FOCUSES

I. THE RISK OF ABUSE OF VIRTUAL ASSETS FOR PURPOSES OF MONEY LAUNDERING AND TERRORIST FINANCING

The Analysis of money laundering and terrorist financing risks, on the basis of current investigative evidence, has revealed that virtual assets have been used, in a limited number of cases, for the following: the purchase of drugs and weapons, extortion and computer fraud and money laundering. It should also be noted that these activities can be made possible through the use of prepaid cards. As far as the risk of terrorist financing is concerned, the use of crowd-funding platforms aimed at collecting virtual assets to be used to support terrorist organisations, is known to Law Enforcement and investigating authorities.

Although virtual assets can potentially lend themselves to being used for the purposes of money laundering and terrorist financing, at present, the evidence resulting from both analysis of suspicious transaction reports and investigations, together with the new regulations introduced into the Italian legal system, are such as to lead one to believe that, even if in the presence of a potentially high risk, the inherent risk of using virtual assets for money laundering and terrorist financing is, as for now, of lowly significance.

Rather, more attention needs to be paid to the use of virtual assets supported by the constantly evolving technology (so-called FinTech).

In accordance with the Ministerial Decree being adopted under Article 17 of the Legislative Decree no. 141/2010, virtual assets providers must notify the Ministry of Economy and Finance their functioning in Italy. The aim of this provision is to carry out the first in-depth census of providers in the sector. Such disclosure is a precondition for the business of these providers to be considered legal. On the basis of the above mentioned Ministerial Decree, cooperation between the Ministry of Economy and Finance and Law Enforcement Authorities is also established, in order to prohibit the provision of services related to virtual assets by providers who do not comply with the disclosure (notification to the Ministry of Economy and Finance) obligation.

II. ITALIAN AND EU PIS/EMIS: TYPES OF MONEY LAUNDERING IDENTIFIED BY UIF INSPECTIONS

During the two-year period of 2015-2016, the UIF carried out inspections to ensure that payment institutions operating within the money remittance sector were complying with their obligations to report suspicious transactions. Companies inspected by the UIF were those with a significant share of the market (more than 80%).

Widespread irregularities and shortfalls in the organisational structures of some intermediaries were found. Larger intermediaries demonstrated a high level

of awareness to the risks of money laundering and terrorist financing, and provided good cooperation, but difficulties were encountered in monitoring their networks of agents. Fraudulent splitted money transfers are confirmed as the most significant risk and take on increasingly complex forms that are not easy to identify. The quantitative thresholds established by the intermediaries to control and mitigate this risk are often high. Furthermore, automatic controls have not always been operational or have presented malfunctions such as to render them ineffective. These fraudulent techniques work by sending remittances of a unit amount just below the legal threshold by groups of people who, over several days, act one after the other within a short time frame; they are 'lists' of people who send money to a small group of beneficiaries by repeatedly acting in the same sequence or in reverse order. Individual agents input transactions into the PI management systems at such a rate that it is plausible that they have been arranged in the absence of customers; in some cases, remittances are entered at times or days when the operations centre is likely to be closed.

Irregularities have emerged in the acquisition of the data necessary for the agents' identification of customers and in the related intermediaries' controls. In some cases, the reliability of the identification documents and the tax code has been seriously undermined. Some computer systems used by PIs operate on technological web-based platforms, accessible using dedicated Internet sites, which allow one to pass orders remotely. This, together with the intervention of the agents' collaborators, often unknown to the PI, who use the access credentials assigned to the agent, is beyond the control of the payment institutions and exposes them to high risks. The inspection analysis confirms that the distribution network is the weakest link of the service. Agents make a very marginal contribution to active cooperation; indeed, their direct involvement in the execution of fraudulent transfers charged to unaware or non-existent persons or to proxies often emerges. Safeguards in place to prevent terrorist financing were also deemed inadequate. In some cases, there was poor matching with the lists issued by the UN and the European Union for the purpose of freezing funds and economic resources. Repeated remittances of foreign citizens operating in areas with a high crime rate towards far-away countries, and also in areas adjacent to conflict zones, had not been the focus of due consideration.

In light of the findings of the inspections, the UIF initiated sanction proceedings for the offences over which it had jurisdiction, and informed the Public Prosecutors concerned of irregularities detected. It also notified the Directorate General for Financial Supervision and Regulation of the Bank of Italy and the Special Currency Police Unit (NSPV) of the Guardia di Finanza of possible initiatives particularly towards intermediaries and agents, also in cooperation with the Organismo Agenti e Mediatori (OAM) and the foreign Supervisory Authorities. The results of the UIF's inspections led to the issuing of cease and desist orders by the appropriate authorities. In three cases, the Italian or foreign supervisory authorities withdrew the intermediary's authorisation to operate. In one case, however, the intermediary avoided ceasing operations through structural changes in the company's organisation.

In some cases, the problems were indicative of wider flaws in the organisational structure, in the internal control system and in company policies. With regard to the in-depth analyses of the issuing of electronic money carried out, the shortcomings in organisational controls have highlighted, in some cases, the misuse of prepaid cards, with arrangements that are not consistent with the standard

payment purposes of these instruments.

The shortcomings detected, which in some cases have led to the permeability of intermediaries for money-laundering purposes, assumed different levels of seriousness. This ranged from the lack of an effective internal control system aimed at combating money-laundering and terrorist financing, to the insufficient supervision of the agent network, up to the active involvement of the intermediary in criminal conduct in the most serious cases.

The inspections carried out also revealed, in the corporate sector, underestimation of inherent risks within the service provided, the ways that the intermediary can be implicated in the transfer. Both of these factors make it more difficult to trace back concerned subjects involved inti the transfers of money.