BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2019
Italy's Financial Intelligence Unit

Rome, May 2020

year 2019

number 12

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2019
Italy's Financial Intelligence Unit

Rome, May 2020

The Unità di Informazione Finanziaria per l'Italia (UIF) is Italy's Financial Intelligence Unit, the national body charged with combating money laundering and the financing of terrorism. It was formed at the Bank of Italy pursuant to Legislative Decree 231/2007, in compliance with international rules and standards requiring all countries to institute their own financial intelligence units, independently run and operating autonomously.

The Unit collects information on potential cases of money laundering and financing of terrorism, mainly in the form of reports of suspicious transactions filed by financial intermediaries, professionals and other operators. It conducts a financial analysis of the reports, using the sources at its disposal and the powers assigned to it, and assesses the results with a view to transmitting them to the competent investigative and judicial authorities for further action.

The regulations provide for exchanges of information between the UIF and supervisory authorities, government departments and professional bodies. The Unit cooperates closely with the investigative and judicial authorities to identify and analyse anomalous financial flows. It is a member of the global network of the financial intelligence units that share the information needed to combat cross-border money laundering and financing of terrorism.

Bank of Italy, 2020

Unità di Informazione Finanziaria per l'Italia

Director
Claudio Clemente

Address
Largo Bastia, 35 00181 Rome -Italy

Telephone
+39 0647921

Website
http: //uif.bancaditalia.it

ISSN 2385-1384 (print)
ISSN 2284-0613 (online)

Index

List of boxes

FOREWORD

All the UIF's areas of activity registered further expansion in 2019. The number of suspicious transaction reports received from obliged entities rose to nearly 106,000. The Unit began collection and analysis of threshold-based communications and stepped up cooperation with foreign FIUs, Italian authorities and magistrates, and the systematic exchange of information with the National Anti-Mafia Prosecutor's Office became fully operational. A special commitment was the UIF's contribution to the development of global, European and domestic anti-money laundering rules. A major reorganization of the Unit itself was completed, in effect as of January 2020, to adapt the operational structures to the new tasks assigned to the Unit.

The COVID-19 pandemic that struck Italy in the early months of 2020 caused serious loss of life, with a dramatic, direct impact on the UIF itself – it claimed the life of our highly professional and wonderfully creative colleague, Pierpaolo De Franceschis. The epidemic resulted in a collapse in economic activity and heightened the risks of criminal infiltration of capital markets, public tenders, and civil society.

Given the important role that combating money laundering can play in preventing criminal deviations while achieving public economic support, the UIF acted to ensure even closer monitoring of reports and faster, more efficacious cooperation, with a significant increase in overall activity. Operators were alerted to the special risks stemming from the measures to cope with the health emergency and the necessity to calibrate verifications so as to intercept any suspicious situations in this regard. The response, overall, has proven to be rapid and effective.

Again in 2019, active cooperation made significant progress, not only in the volume of reports but also in the number and diversification of reporting entities. The UIF continues in its work to sensitize the obliged entities, improve their contribution, and monitor the contents and quality of reports to avert a deterioration due to the application of automatic reporting mechanisms or the adoption of a purely precautionary attitude, even at major intermediaries. The Unit undertook wide-ranging action, designing a specific reporting scheme for easier and more accurate representation of suspicious transactions in the sectors of gaming, payment cards and virtual currencies.

Once again, the STRs analysed and transmitted to the investigative bodies outnumbered those received, confirming the Unit's capability to handle a larger volume of reports while continuing to reduce the backlog. To deal with the increased workload while maintaining high quality, the UIF exploited technological innovation, relying on the increase in the data available and the automation of data flows and processes of data enrichment in support of analysis of the reports. One most significant result, to the benefit of all players within the system, was the realization of automated procedures for information exchange with the DNA, as introduced by the legislative reform of 2017. A more effective and more comprehensive system of quality control on reports was instituted, and an electronic channel was installed to guarantee the security of communications with the obliged entities.

The Unit's assessments of the individual transactions reported have generally been corroborated by subsequent analyses by the Finance Police and the Anti-Mafia Investigation Department, once again demonstrating the high degree of synergy that has developed within the AML prevention apparatus.

Changes to the procedures for processing and monitoring aggregated STRs and gold transaction reports enabled the Unit to identify anomalous positions, which were then investigated by law enforcement bodies. Strategic analysis continued on a reinforced basis with a view to identifying anomalies in financial flows and devising operational indications for preventing and combating money laundering.

In April 2019, with threshold-based communications, the Unit began to pick up cash transactions with a high likelihood of being used for illicit purposes, as was reiterated in the Supranational Risk Assessment completed during the year. This new database is an important instrument enriching the analysis of STRs, and it can also detect split transactions that can escape the notice of individual reporting entities. Effective exploitation of this information requires higher quality for the data transmitted, which still suffer from errors of classification and measurement.

Inspections during the year at operators in highly innovative sectors of finance brought out risks of money laundering in connection with their characteristics, which produce a segmentation of financial flows that hampers the reconstruction of movements of funds.

Exchanges of information with the judicial authorities and investigative bodies increased sharply by comparison with previous years. There were recurrent requests in connection with proceedings against cross-border mafia-style criminal organizations. A good many cooperative initiatives were undertaken together with supervisory and sectoral authorities. In September, a new memorandum of understanding was signed with the National Anti-Corruption Authority.

Information exchanges with foreign FIUs increased substantially in volume and in variety, allowing a more complete approach to further analysis of STRs and more effective response to the needs of the judicial authorities. The perception of the extent and impact of international money laundering has strengthened greatly, leading to a reconsideration of the real adequacy of the AML systems of individual European countries, the common rules and their practical application. As regards particularly important cases involving various countries, the UIF promoted joint analyses, which were able to reconstruct intricate illegal phenomena that were then brought to the attention of the competent investigative bodies.

There is no denying, however, that the Italian legislation recently transposing the Fourth and Fifth AML Directives, which in practice has further complicated and restricted access to investigative information, has thereby had a negative impact on the capacity for timely and efficacious cooperation with foreign FIUs. On the domestic front as well, the new rules represent a step backward, further limiting the set of authorities with which information can be exchanged, which threatens to reduce the overall efficacy of the Italian AML system.

The need for still broader and closer cooperation among authorities, also cross-border, has been emphasized further in Europe with the issue of Directive EU/2019/1153, extending the roster of authorities that can have access to the financial data and analyses of FIUs, which in their turn can draw on an ample range of law enforcement information.

The world that awaits the UIF will present a host of challenges, rendered all the more difficult by the complexity of the present historical period. The dynamic approach taken by the Unit to risk identification and analysis, interaction with reporting entities, technological innovation, staff training, and domestic and international cooperation will prove crucial to

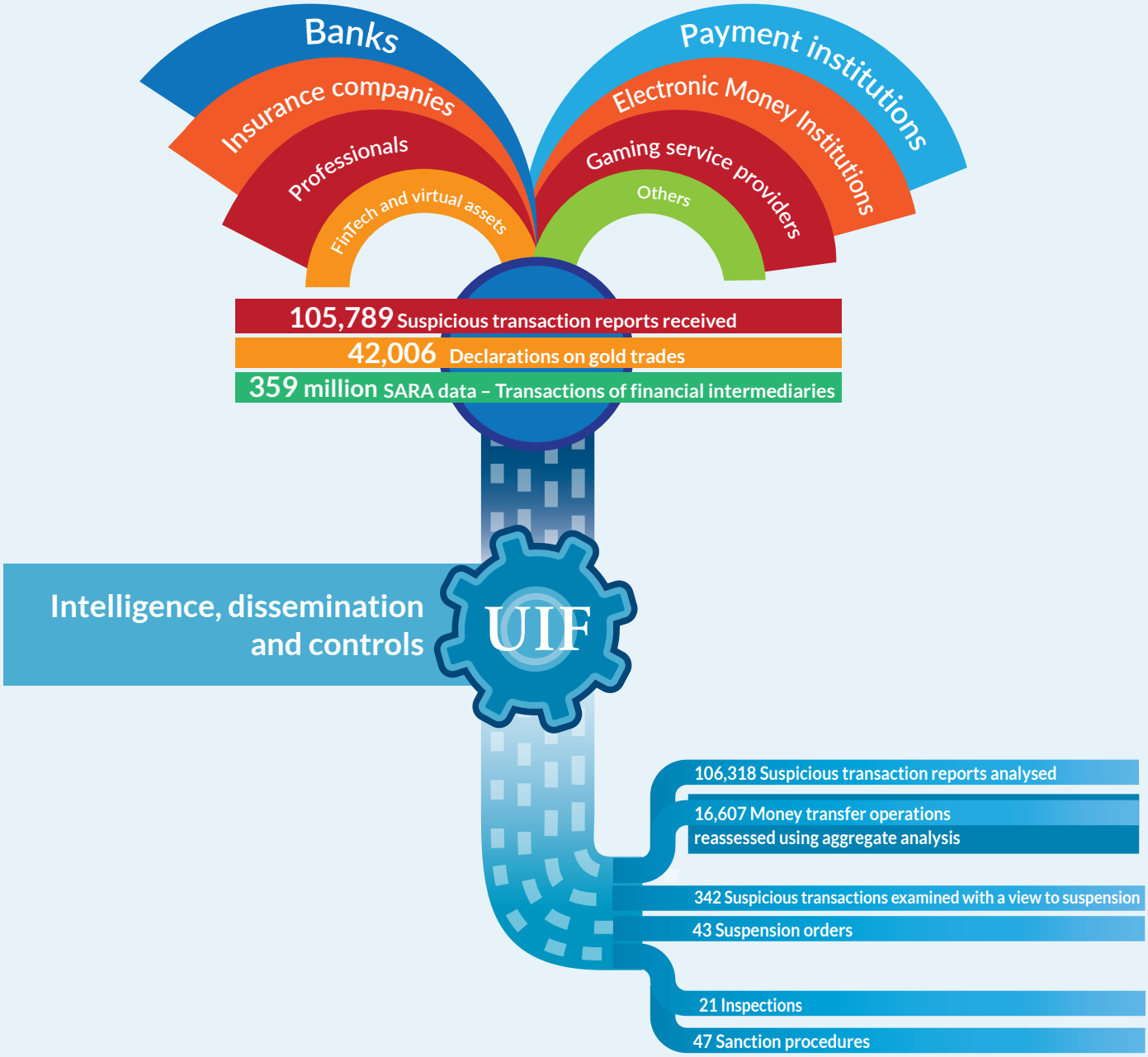
dealing effectively with the new threats. This with the certainty that preventing and combating money laundering and the financing of terrorism remains indispensable to defending our economic and financial system in the trials to come and the attendant risks that they will face.

The UIF will not fail to make its contribution of ideas, professionalism and determination.

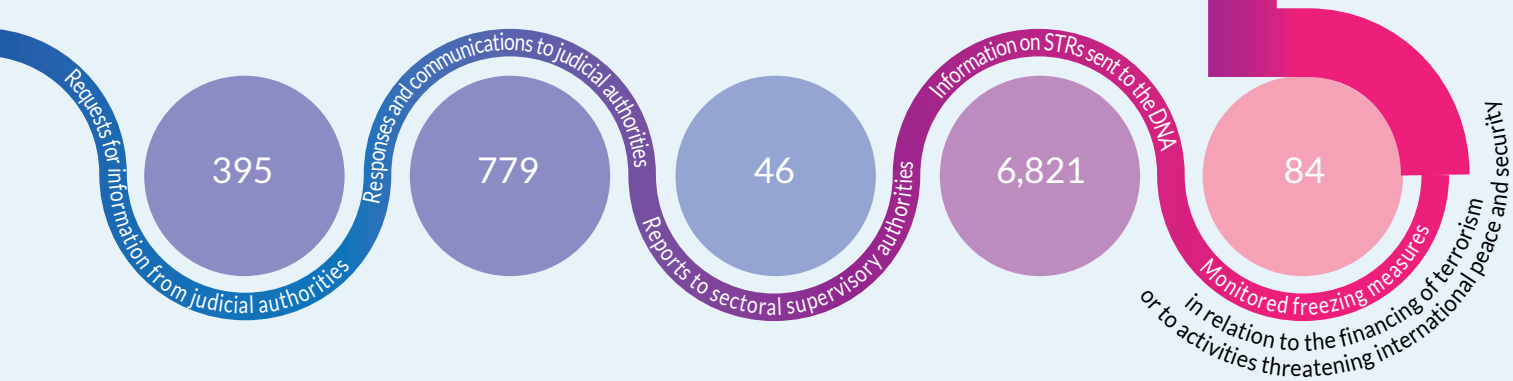
The Director

Claudio Clemente

Financial analysis



Cooperation with investigative bodies and national authorities



FOREIGN FIUs

1,350
Requests and spontaneous communications received

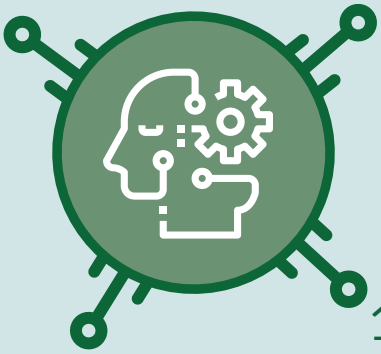
50
Exchanges on possible freezing of funds

963
Requests sent to foreign FIUs

2,533
Communications from foreign FIUs sent to investigative bodies

DISSEMINATION

of knowledge about money laundering



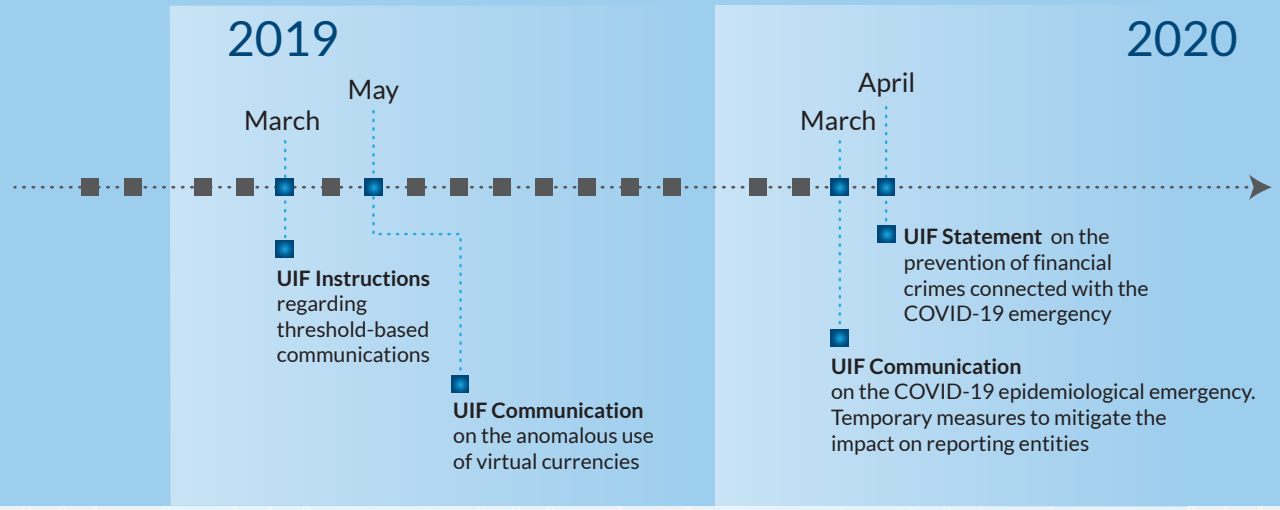
2
Workshops organized by the UIF with universities

87
Speakers at conferences and workshops on money laundering at universities and other institutions

25
Training interventions at regional bodies and other general government offices

15
Publications in *Quaderni dell'antiriciclaggio* and in scientific journals

Secondary legislation and UIF communications



IT Infrastructure

Downloading of the **official printed version** of STRs directly from the Infostat-UIF portal

Re-engineering of the portal for enhanced security

Launch of the system for collecting **threshold-based communications**

New controls on STRs received to improve data quality

Creation of a secure transmission channel for **exchanges of confidential information** with reporting entities

1. ACTIVE COOPERATION

The Unit is the institution appointed to investigate suspicious transactions that may involve money laundering, financing of terrorism or financing of the proliferation of weapons of mass destruction, on the basis of reports from financial intermediaries, professionals and other qualified operators who are required to collaborate actively, detecting and evaluating such transactions and promptly notifying the Unit of them.

Centralizing the flow of information at the Unit means that the evaluations can be standardized and integrated in order to identify subjective and objective links, trace financial flows even across national borders, through information exchanged with the network of foreign FIUs, reconstruct innovative methods of money laundering and select those cases with a higher level of risk.

The Unit sends the results of its analyses to the competent law enforcement bodies – the Special Foreign Exchange Unit of the Finance Police (NSPV) and the Anti-Mafia Investigation Department (DIA) – for further investigation. The reports and analyses are sent to the judicial authorities if crimes are involved or if the authorities themselves request the reports. The results of the analysis may be sent to the supervisory authorities if important cases are detected. The UIF sends data and information to the National Anti-Mafia Directorate (DNA) in order to check for possible links to criminal contexts and enable prompt action.

The body of information acquired is also used to develop anomaly indicators and identify patterns of anomalous behaviour to guide reporting entities in detecting suspicious transactions.

The Unit also receives threshold-based communications, which report cash transactions, including split transactions, in excess of €10,000, calculated on a monthly basis. This additional information tool enhances the analysis of suspicious transaction reports.

1.1. Reporting flows

In 2019, the unit received 105,789 suspicious transaction reports (STRs),[1] 7,759 more than in the previous year (+7.9 per cent; Table 1.1).

Table 1.1

Reports received

	2015	2016	2017	2018	2019
Number of reports	82,428	101,065	93,820	98,030	105,789
Percentage change on previous year	*14.9*	*22.6*	*-7.2*	*4.5*	*7.9*

[1] Detailed information on suspicious transaction reports can be found in the *Quaderni dell'antiriciclaggio*, Dati statistici, published on the UIF's website.

The increase, almost double that recorded in 2018, derived mainly from the growth in reports from intermediaries and other financial operators (+52.7 per cent) and from gaming service providers (+27.7 per cent). These increases more than offset the slight decrease of 4 per cent in reports from banks, which in part reflected the transfer of activity from a parent company to a subsidiary electronic money institution (Table 1.2; see below).

As a result of that transfer of activity and of the increase in the contribution of the other obliged entities, the share of reports transmitted by banks and Poste Italiane spa (hereinafter simply 'banks') fell to 64.5 per cent, from 72.5 per cent in 2018. Intermediaries and other financial operators again ranked second among the categories of reporting entity by number of reports, their share of the total rising from 16.5 to 23.3 per cent. The share received from gaming service providers also rose, from 5.2 to 6.1 per cent. As in the previous year, professionals transmitted a relatively small share of the total (4.8 per cent). The number of communications from general government was again extremely small,[2] coming mostly from local government bodies such as municipalities and chambers of commerce, with 9 and 8 reports, respectively. At the central government level, the Revenue Agency stood out with 10 communications.

Table 1.2

STRs by type of reporting entity

	2018		2019		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2018)*
Total	**98,030**	**100.0**	**105,789**	**100.0**	**7.9**
Banks (incl. Poste Italiane spa)	71,054	72.5	68,236	64.5	-4.0
Non-bank financial intermediaries	16,139	16.5	24,648	23.3	52.7
Companies managing markets and financial instruments	11	0.0	11	0.0	-
Professionals	4,818	4.9	5,074	4.8	5.3
Non-financial operators	898	0.9	1,303	1.2	45.1
Gaming service providers	5,067	5.2	6,470	6.1	27.7
General government offices	43	0.0	47	0.0	9.3

Financial intermediaries other than banks

Among non-bank financial intermediaries, the year saw further increases in the number of reports submitted by electronic money institutions (+241.9 per cent, from 2,699 to 9,227) and by payment institutions and points of contact of EU payment service providers (+15.5 per cent, from 9,006 to 10,399; Table 1.3). For the former, after the decreased concentration of reports observed in 2018, a single operator once again accounted for the bulk of the

[2] As of 4 July 2017, general government is no longer among the obliged entities, as it is not included in Article 3 of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017. The new rules, set out in Article 10(4) of the above-mentioned decree, provide, however, that 'in order to enable financial analyses to be made, aimed at uncovering money laundering and financing of terrorism activities, general government entities shall communicate to the UIF any data or information concerning suspicious transactions that come to their attention in the course of their institutional activities (...)'. See '*Istruzioni sulle comunicazioni delle Pubbliche amministrazioni*', published by the UIF in 2018.

growth, partly owing to the above-mentioned intra-group reorganization.

Within the category of payment institutions and the related contact points, the contribution of money transfer operators declined slightly to 83.8 per cent from 87.3 per cent in 2018. Although to a lesser extent, the total for the category was boosted by the greater number of STRs received from insurance companies (+13.8 per cent), financial intermediaries under Article 106 of the 1993 Banking Law (+20 per cent) and asset management companies, SICAVs and SICAFs (+27.6 per cent).

Table 1.3

STRs by category of banking and financial intermediary

	2018		2019		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2018)*
Banks, intermediaries and other financial operators	**87,193**	**100.0**	**92,884**	**100.0**	**6.5**
Banks and Poste Italiane spa	**71,054**	**81.5**	**68,236**	**73.5**	**-4.0**
Non-bank financial intermediaries	**16,139**	**18.5**	**24,648**	**26.5**	**52.7**
Payment institutions and points of contact of EU payment service providers	9,006	10.3	10,399	11.2	15.5
Insurance companies	2,412	2.8	2,745	3.0	13.8
Electronic money institutions and points of contact of EU electronic money institutions (1)	2,699	3.1	9,227	9.9	241.9
Trust companies - Article 106 of the 1993 Banking Law	595	0.7	546	0.6	-8.2
Financial intermediaries – Article 106 of the 1993 Banking Law	799	0.9	959	1.0	20.0
Asset management companies, SICAVs and SICAFs	351	0.4	448	0.5	27.6
Investment firms	60	0.1	58	0.1	-3.3
Intermediaries and other financial operators not included in the previous categories (2)	217	0.2	266	0.3	22.6

1) This extremely sharp increase was due to the intra-group transfer of activity from a parent company to a subsidiary electronic money institution - (2) The category comprises the entities listed in Article 3(2) and (3) of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017, not included in the previous categories.

Professionals

The number of STRs received from professionals grew by 5.3 per cent, again mainly reflecting the increase in those sent by notaries (+6.6 per cent). The contributions of the other categories of professionals remained marginal, although the number of reports from accountants and lawyers turned upwards (from 319 to 327 and from 38 to 48, respectively). Relatively more important was the increase in reports from auditing firms and auditors, up from 13 to 30. STRs from law firms, law and accounting firms and law practices continued to decline, falling from 81 to 18 (Table 1.4).

Almost all reports from notaries (98.2 per cent) are submitted through the National Council of Notaries. Accountants and bookkeepers likewise submit the bulk of their reports through the National Council of the Order of Accountants and Bookkeepers (CNDCEC), the share sent in this fashion increasing to 73.4 per cent from 72.3 per cent in 2018. It is hoped that this reporting modality, together with the technical rules adopted by both bodies in 2019 concerning due diligence and record keeping, will have the expected encouraging impact in terms of active cooperation.

The number of reports sent by non-financial operators also continued to grow. The increase was driven by the rise in the number of those sent by cash-in-transit and valuable items transport companies (+61.4 per cent) and by gold traders and manufacturers of and dealers in precious stones and metals (+24.1 per cent). The number of reports submitted by virtual assets operators (exclusively exchangers), though still marginal, rose from 2 in 2018 to 20 in 2019.

Table 1.4

STRs received from professionals and non-financial operators

	2018		2019		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2018)*
Non-financial obliged entities	**10,783**	**100.0**	**12,847**	**100.0**	**19.1**
Professionals	**4,818**	**44.7**	**5,074**	**39.5**	**5.3**
Notaries and Nat. Council of Notaries	4,345	40.3	4,630	36.0	6.6
Law firms, law and accounting firms and law practices	81	0.8	18	0.1	-77.8
Accountants, bookkeepers and employment consultants	319	3.0	327	2.5	2.5
Lawyers	38	0.4	48	0.4	26.3
Auditing firms and auditors	13	0.1	30	0.2	130.8
Other professional services providers (1)	22	0.2	21	0.2	-4.5
Non-financial operators	**898**	**8.3**	**1,303**	**10.1**	**45.1**
Gold traders and manufacturers and traders of precious stones and metals	432	4.0	536	4.2	24.1
Cash-in-transit and valuable items transport companies	425	3.9	686	5.3	61.4
Virtual assets operators (2)	2	0.0	20	0.2	900.0
Other non-financial operators (3)	39	0.4	61	0.5	56.4
Gaming service providers	**5,067**	**47.0**	**6,470**	**50.4**	**27.7**

(1) The category comprises the entities listed in Article 3(4) letter (b) of Legislative Decree 231/2007. - (2) The category comprises the entities listed in Article 3(5) letters (i) and (i) bis. - (3) The category comprises the other entities listed in Article 3(5) of Legislative Decree 231/2007 not included in the previous categories.

The reporting flow from gaming service providers, which had surged by 94.9 per cent the previous year, continued to grow in 2019, albeit at a slower pace (+27.7 per cent), with the number of STRs rising from 5,067 to 6,470. The increase was entirely ascribable to the flow from physical network gaming operators (+58.7 per cent, from 2,728 to 4,330 STRs), while the number of reports sent by online gaming operators fell by 8.5 per cent, from 2,265 to 2,072. The number of STRs from casinos also declined, from 74 to 68.[3]

Overall, these developments confirm that an increasing share of all reports come from operators in the gaming sector and payment services. The recent creation within the Unit of a division specialized in processing the STRs from these categories is aimed at extracting the greatest possible value from the particular properties of the related information flow (see Chapter 10, 'Resources and organization'). Benefits are also expected to come from the recent issue of an STR form tailored to gaming service providers (as well as to payment card issuers and to virtual currency exchangers; see Section 10.4, 'IT resources') in order to facilitate more accurate representation of the typical suspicious transactions encountered by such entities.

STRs in the first four months of 2020

The number of suspicious transactions reports has continued to grow in 2020. In the first four months of the year, the Unit received 35,927 STRs, 6.3 per cent more than in the same period of 2019. The number of STRs transmitted to investigative bodies grew by 9 per cent. In March 2020, the inflow of reports contracted only very slightly, despite reporting entities' widespread adoption of remote working methods.

New reporting entities

The number of reporting entities continued to increase in 2019, rising to 6,708 thanks to 503 new registrations (424 in 2018). In 2019, 22.7 per cent of the newly registered entities sent at least one report during their first year of registration, broadly in line with the previous year's figure (23.6 per cent), but their aggregate contribution to the reporting flow for the year rose to 1,460 STRs, compared with 1,047 in 2018. This result is largely ascribable to newly registered payment institutions and points of contact of EU payment institutions, which transmitted 1,204 STRs.

Professionals again accounted for the largest share of new registrations (279). The majority of these were accountants, bookkeepers or employment consultants (155) or lawyers (42). There was again a significant number of newly registered gold traders (52). The category of virtual currency operators increased with the addition of seven exchangers; no digital portfolio managers were registered, but they only became obliged entities in November 2019 pursuant to Legislative Decree 125/2019. Finally, there was a further increase in the number of general government offices registered in order to comply with the communication requirements of Article 10(4) of Legislative Decree 231/2007, although this was not accompanied by an appreciable growth in transmissions: in 2019, with 39 new registrations, the number of communications rose from 43 to 47.

1.2. Suspicious transactions

As in previous years, the vast majority of suspicious transaction reports received in 2019

[3] The prevalence of STRs from physical network operators with respect to the other categories of the same group stems from the reclassification of some online gaming operators as physical gaming operators. The data presented here reflect that reclassification for both the periods referred to.

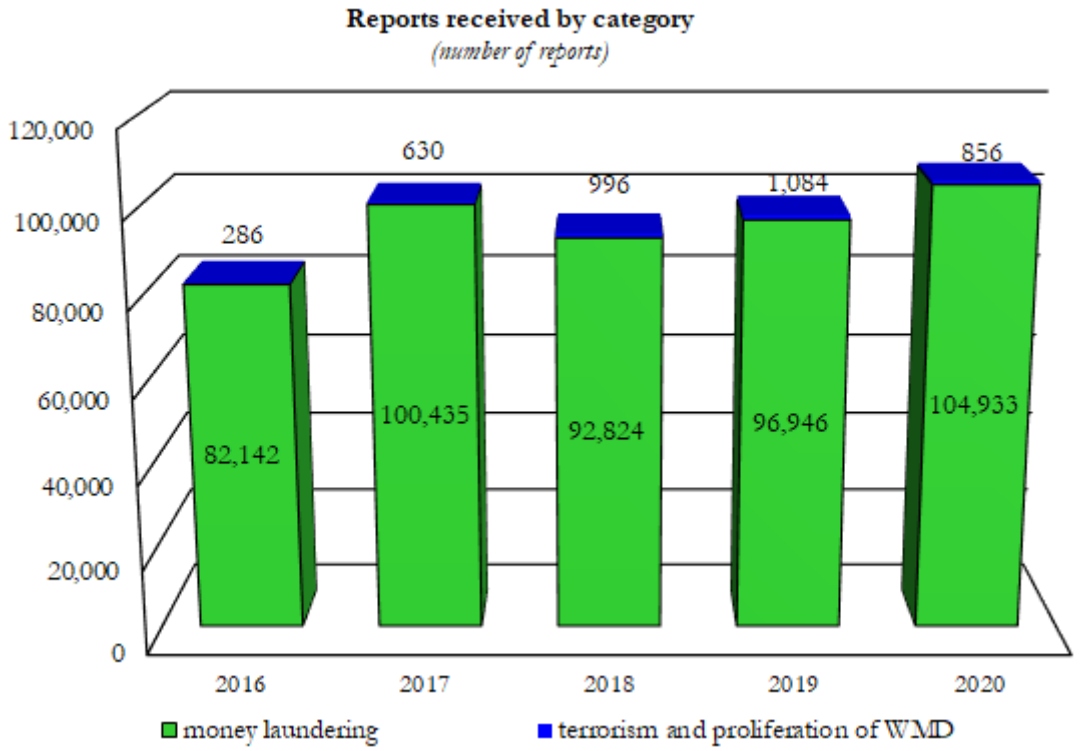
concerned money laundering (99 per cent). Reports linked to the voluntary disclosure measure dwindled to barely 961, or 0.9 per cent of the total.

The skew in the distribution was reinforced by the increase in the number of reports of suspected money laundering (+8.2 per cent, from 96,946 to 104,933) and the further decline of 27.8 per cent in those concerned with terrorist financing, which fell to 770 (see Chapter 4, 'Combating the financing of terrorism'). The number of reports regarding financing of proliferation of weapons of mass destruction rose from 18 in 2018 to 86 in 2019 (Table 1.5 and Figure 1.1).

Table 1.5

Distribution of STRs by category					
	2015	**2016**	**2017**	**2018**	**2019**
	(number of reports)				
Total	**82,428**	**101,065**	**93,820**	**98,030**	**105,789**
Money laundering	82,142	100,435	92,824	96,946	104,933
Financing of terrorism	273	619	981	1,066	770
Financing of proliferation of WMD	13	11	15	18	86

Figure 1.1



The distribution of the reports by region largely resembled that of 2018. Lombardy was again the leading region, with 19.8 per cent of the total flow, followed by Campania and

Lazio (12.2 and 10 per cent, respectively; Table 1.6). Among the regions with the largest absolute increases in STRs, Sicily recorded the highest percentage growth (+26.3 per cent), followed by Emilia-Romagna (+10.8 per cent), Lazio (+10.7 per cent) and Puglia (+10.6 per cent). Though the numbers were smaller in absolute terms, there were also significant percentage increases for Molise (+23.8 per cent), Basilicata (+17.4 per cent) and Sardinia (+16.9 per cent). The provinces of Prato and Milan again ranked first and second, respectively, for the number of transactions reported (Figure 1.2*)*. The provinces of Imperia and Naples again placed high on the list, and were joined by Trieste. Finally, in 2019, the provinces with the fewest STRs were again those of the south of Sardinia and Nuoro, with 36 and 50, respectively.

Table 1.6

Distribution of STRs received by region where transaction occurred

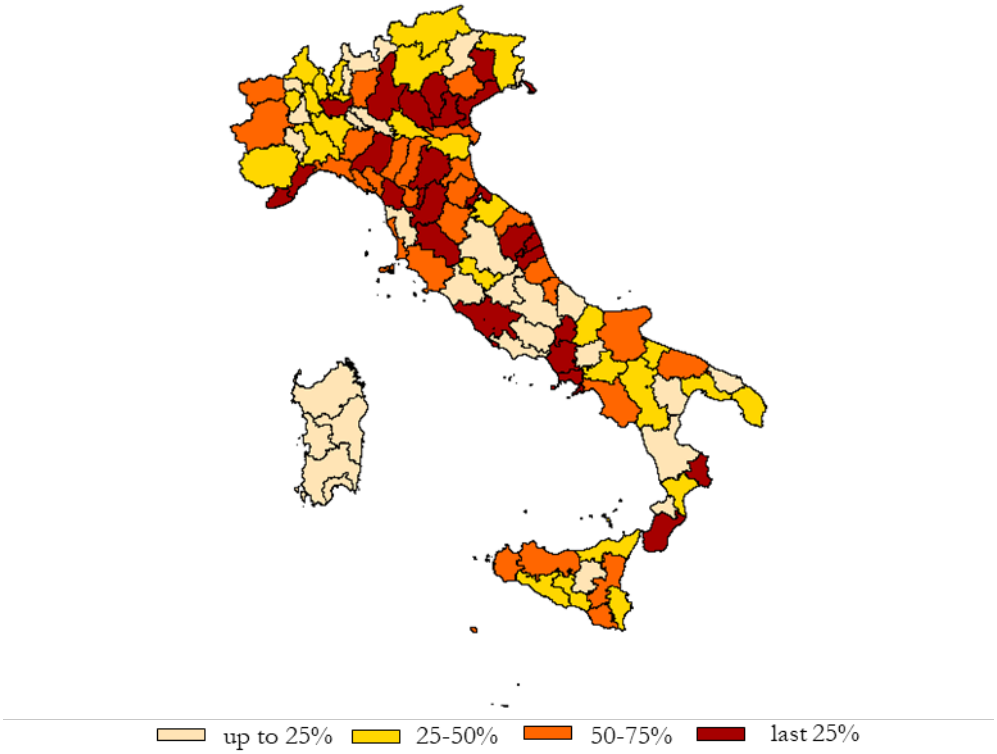
	2018		**2019**		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2018)*
Lombardy	19,440	19.8	20,934	19.8	7.7
Campania	12,183	12.4	12,929	12.2	6.1
Lazio	9,545	9.7	10,567	10.0	10.7
Veneto	8,254	8.4	8,788	8.3	6.5
Emilia-Romagna	6,887	7.0	7,631	7.2	10.8
Sicily	5,857	6.0	7,399	7.0	26.3
Tuscany	6,977	7.1	6,863	6.5	-1.6
Piedmont	6,341	6.5	6,312	6.0	-0.5
Puglia	5,157	5.3	5,705	5.4	10.6
Liguria	2,854	2.9	2,873	2.7	0.7
Calabria	2,696	2.8	2,812	2.7	4.3
Marche	2,426	2.5	2,458	2.3	1.3
Friuli Venezia Giulia	1,935	2.0	1,986	1.9	2.6
Abruzzo	1,312	1.3	1,518	1.4	15.7
Trentino-Alto Adige	1,317	1.3	1,510	1.4	14.7
Sardinia	1,215	1.2	1,420	1.3	16.9
Umbria	1,006	1.0	973	0.9	-3.3
Basilicata	592	0.6	695	0.7	17.4
Molise	365	0.4	452	0.4	23.8
Valle d'Aosta	207	0.2	198	0.2	-4.3
Abroad	1,464	1.5	1,766	1.7	20.6
Total	**98,030**	**100.0**	**105,789**	**100.0**	**7.9**

In 2019, the total value of reported suspicious transactions that were actually executed amounted to €91 billion, compared with €71 billion the previous year. Taking into account the STRs on transactions attempted but not executed, the total value of the year's reporting

flow came to €97 billion, against €91 billion in 2018, with reported but unexecuted transactions falling from €20 billion to €6 billion.[4]

Figure 1.2

Distribution in quartiles of reports received per 100,000 inhabitants from the province where the reported transaction took place

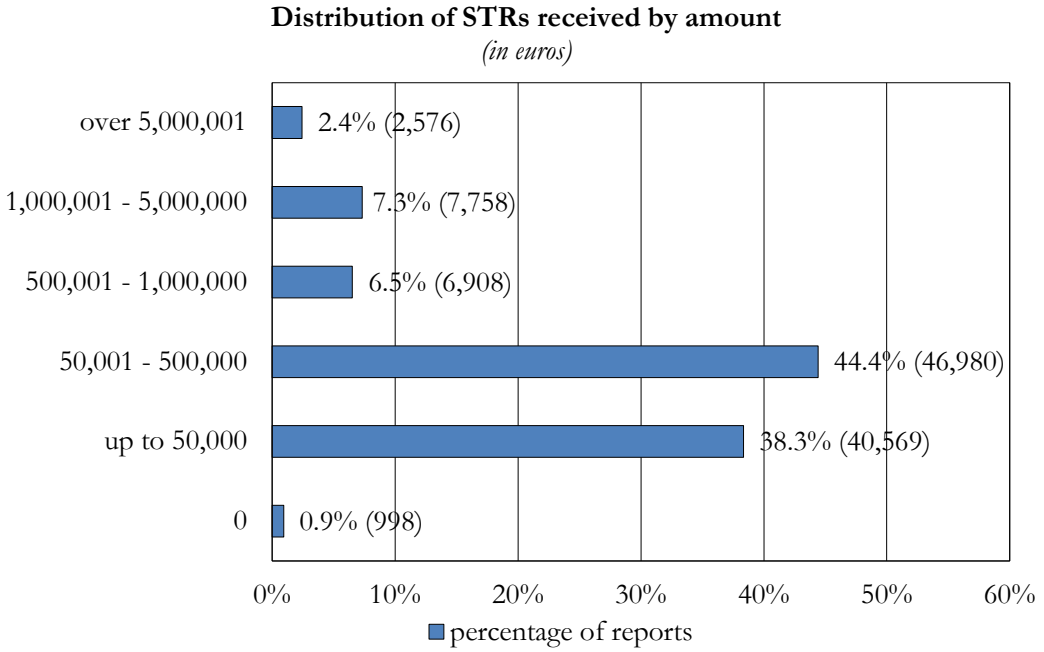


Interpretation of the aggregate of unexecuted transactions is not straightforward, since failure to carry out a transaction may be due to a number of heterogeneous factors, sometimes exogenous with respect to the intermediary (for example, a customer's decision not to carry out the transaction proposed earlier or a transaction request not aimed at seeing the transaction carried out but instrumental to attempted fraud or the establishment of false claims). In any event, the UIF closely tracks the trend of STRs concerning unexecuted transactions, as it is an important indicator of reporting entities' ability both to intercept and refrain from carrying out transactions with a high risk profile and to detect grounds for suspicion solely on the basis of the elements available when the transaction is proposed, thereby facilitating the UIF in its use of the power to suspend transactions. For these reasons, daily monitoring of reported transactions that have yet to be carried out is now standard practice in the processing of STRs (see Section 2.5, 'Suspension orders').

There were no significant changes in the distribution of reports by amount in 2019; 44.4 per cent (46 per cent in 2018) fell in the intermediate bracket (€50,001 to €500,000) (Figure 1.3).

[4] The estimates of the total value of the suspicious transactions reported must be treated with caution. The reporting entity can actually limit the area of suspicion to a subset of the transactions structured in the STR. The calculation of the total value of the suspicious transactions is therefore decisively influenced by such assessments on the part of reporting entities. In addition, the same transaction may be reported by more than one entity, multiplying the amounts.

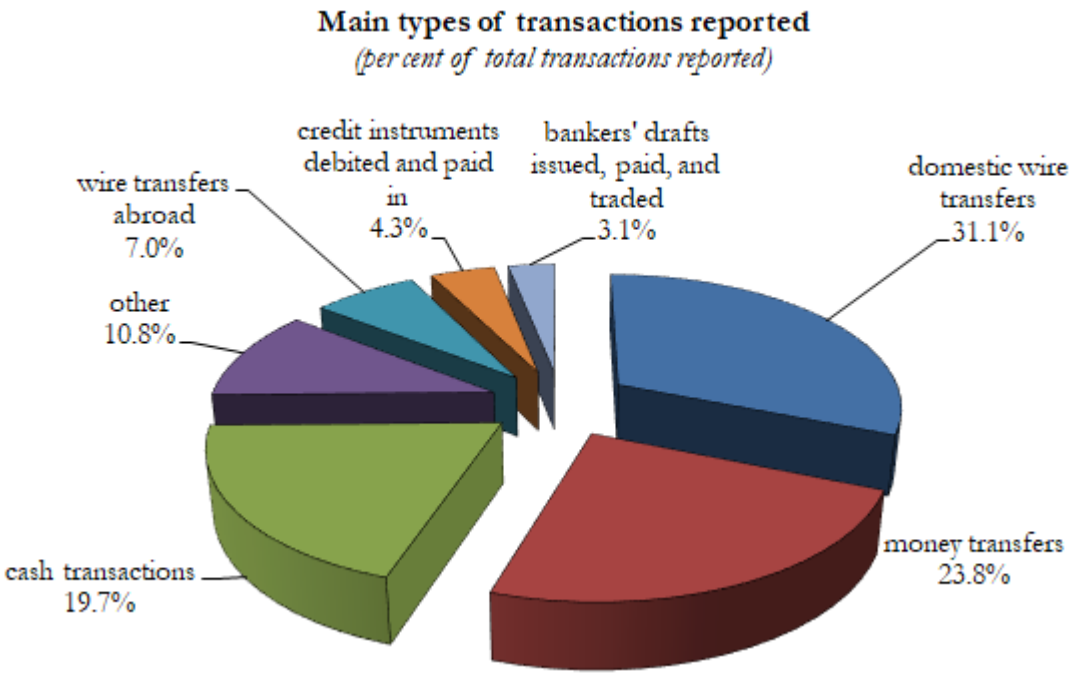
Figure 1.3



Types of transactions reported

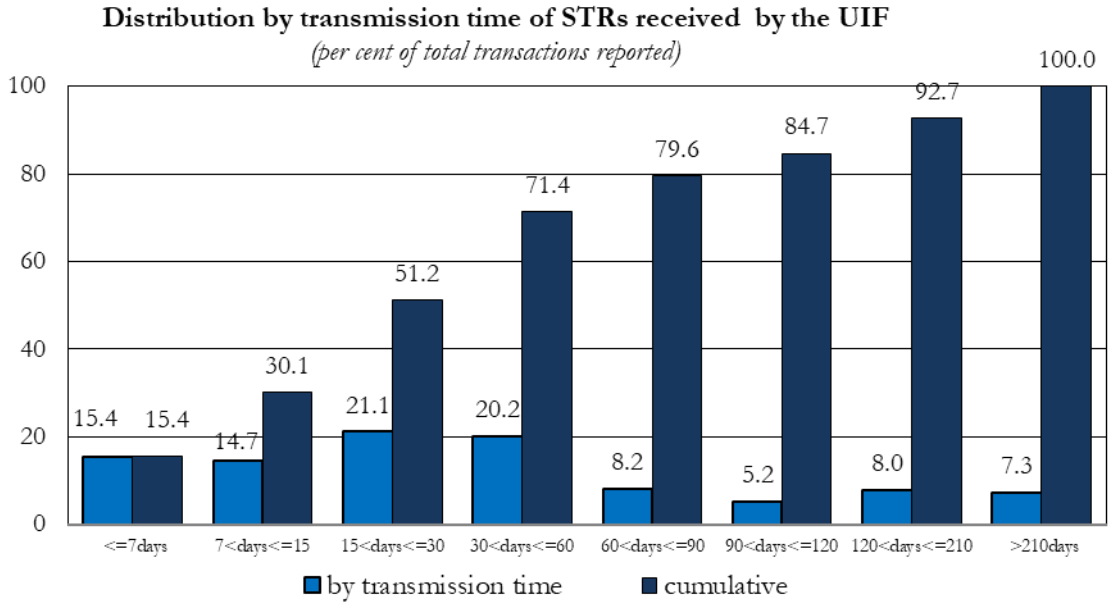
The distribution by type of transaction reported in 2019 does not show any new developments. Domestic credit transfers ranked first again, making up 31.1 per cent of the total, compared with 29.6 per cent in 2018. The relative importance of cash transactions and money transfers remained practically unchanged, at 19.7 and 23.8 per cent, respectively. The share of credit transfers abroad likewise held broadly stable, at 7 per cent (Figure 1.4).

Figure 1.4



There was some further improvement in transmission times compared with the previous year: 51.2 per cent of all reports were received within one month of the transaction (50.4 per cent in 2018), 71.4 per cent within two months (68.6 per cent in 2018), and 79.6 per cent within three months (77.7 per cent in 2018; Figure 1.5).

Figure 1.5



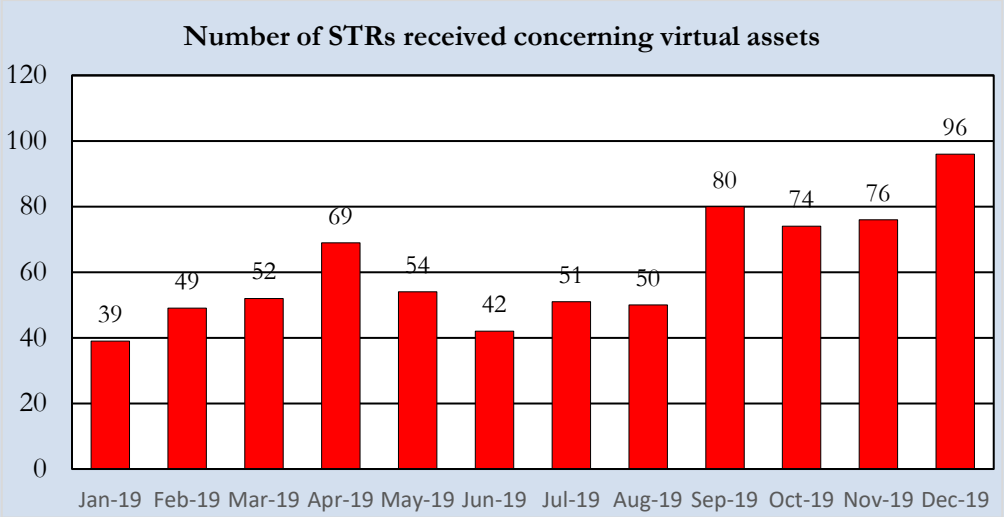
Transmission times for STRs

With regard to the category of reporting entity, banks' performance was similar to that of the previous year, with 32.4 per cent of reports transmitted in the first two weeks following the transaction. There was an improvement, instead, on the part of financial intermediaries and professionals, whose share of reports within that time band rose, respectively, from 15.8 to 21.3 per cent and from 55.2 to 58.1 per cent. As to the communications received from general government, only 12.8 per cent were transmitted within the first 15 days and 27.7 per cent within the first 30 days, while half of them concerned transactions dating back more than seven months.

Suspicious transaction reports concerning virtual assets

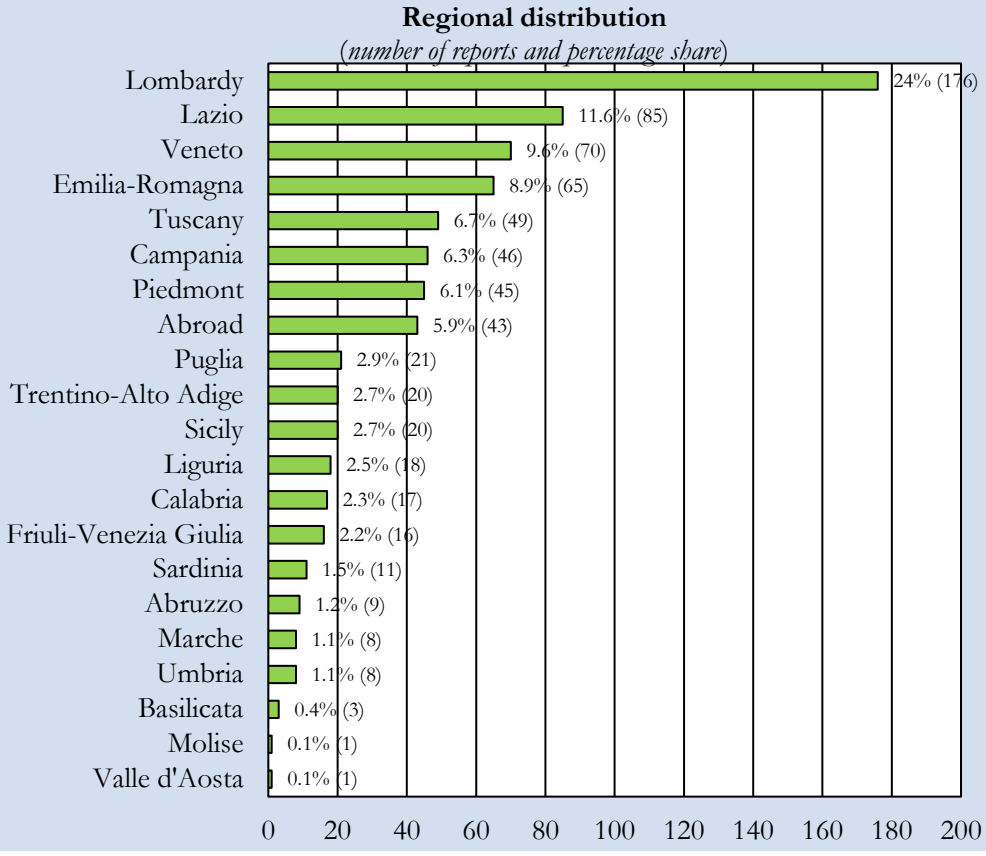
In 2019, the UIF received 732 reports regarding virtual assets (Figure A), 46.7 per cent more than in the previous year.

Figure A



The geographical distribution of these reports (Figure B) basically replicates that of total STRs: the largest share came from the region of Lombardy (24 per cent), followed by Lazio (11.6 per cent), Veneto (9.6 per cent), Emilia-Romagna (8.9 per cent), Tuscany (6.7 per cent), Campania (6.3 per cent) and Piedmont (6.1 per cent).

Figure B



The bulk of reports involving virtual assets continued to come from traditional financial operators, who are affected by the new phenomenon at the time of conversion from or into fiat currency. Banks and Poste Italiane spa submitted 84.4 per cent of such reports. Next came electronic money institutions (9.8 per cent), virtual currency exchangers (2.7 per cent), payment institutions (2.2 per cent) and other reporting entities (0.8 per cent).

The contribution provided by operators of the sector has therefore remained modest, despite the steps taken by the Unit to encourage them to submit reports: on 28 May 2019 the UIF issued a Communication concerning the anomalous use of virtual currencies, with an annex containing supplementary indications for completing the related suspicious transaction reports. In January 2020, a new functionality was made available to operators of the sector to support them in entering reports; it is expected to produce benefits in terms of data quality and completeness.

At 31 December 2019, 11 entities operating in the virtual currency segment were registered with the STR reporting system (4 registered in 2018 and 7 new operators registered in the course of 2019). In this two-year period, these reporting entities sent a total of just 22 reports (2 in 2018 and 20 in 2019).

The expected contribution from the operators in the sector is considered crucial for financial analysis of transactions involving virtual currencies: the blockchain forensic analysis software tools used by this category of reporting entity allow identification of the transactions with other specialized operators and above all with persons active on the dark web, overcoming at least part of the problems of traceability of flows in virtual currencies. Nevertheless, the analyses conducted on the reports show they are of rather poor quality. In many cases, they lack information that is essential for reconstructing the financial flows and identifying the parties involved. They often lack the information details needed to identify the account of the counterparty or the counterparty itself, generically identified as a company that operates in virtual currencies. In some cases, it is not even possible to reconstruct precisely the amount exchanged in virtual assets. To obviate these shortcomings, in January 2020, new formal controls on the contents of reports were introduced, requiring reporting entities to conduct more stringent checks on the structured data they submit to the UIF.

1.3. The quality of active cooperation

The entities subject to reporting obligations play a crucial role in the system for preventing and combating money laundering and the financing of terrorism. Their active cooperation with the UIF must always be characterized by the adequate quality, timeliness and completeness of the information transmitted.

The initiatives of dialogue undertaken in 2019, differentiated in their content, were addressed to different types of operator.

Thematic meetings

Two thematic meetings were organized. The first concerned the impact of the expansion of FinTech payment services on the activities at risk of money laundering; the second, held on the occasion of the presentation of the UIF's *Annual Report for 2018*, was a forum for sharing experiences, methods, organizations and strategies adopted by some intermediaries to ensure the effectiveness of reporting. Both meetings involved a good number of operators and were important occasions for discussion of the safeguards put in place.

Money transfer operators

The Unit promoted other initiatives based on the results of its monitoring of the reporting entities by means of specific quality indicators. Some aspects warranting further discussion emerged with regard to money transfer operators.

A meeting was held with one of the main operators of the sector, focusing on its internal organizational structure for analysis and evaluation of the contexts to be reported. In addition, four other intermediaries in the sector received recommendations regarding problems found in the information content of their reports (description and motivation of the suspicion, assessment of the risk). Nine others, whose reporting contributions seemed disproportionately small with respect to their transaction volumes, were invited to provide details on their internal compliance procedures and on the parameters they employ to identify suspicious transactions.

Gaming, payment cards, virtual currencies

The Unit paid special attention to the operators in the gaming, payment card and virtual currency sectors, to whom it addressed an important project to integrate and standardize the information content of their reports. Three specific meetings were held with the principal reporting entities of each sector to present the new reporting procedures, laying the basis for more effective cooperation whose results will materialize once the new procedures are fully phased in by all the entities concerned.

Feedback reports

The Unit provided banks, Poste Italiane spa and money transfer operators with the customary feedback reports on their respective reporting activity.

The feedback reports provide some indicators that gauge the profile of each operator with regard to specific reporting aspects in relation to others in the same reporting category. They can therefore offer suggestions for strengthening the tools for selection and analysis of the contexts to be reported. The indicators are calculated with respect to a benchmark and concern the following aspects:

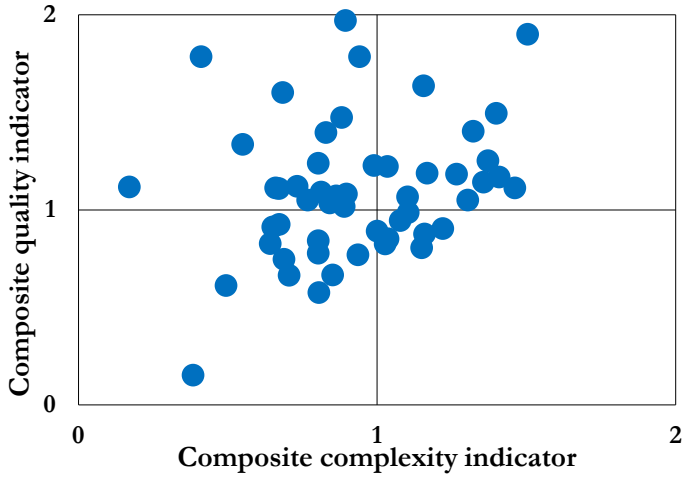
- *the extent of the cooperation*, measured by the number of reports submitted by the reporting entity in the relevant time period in relation to the total number of reports sent by the reference group. This provides a parameter for quantitative evaluation of the operator's reporting activity;
- *timeliness*, shown by the percentage distribution of reports by time period and by median transmission time. This allows assessment of the reporting entity's speed of response to emergent suspicious elements;
- *quality*, measured by indicators that capture the importance of the reports (risk level, results of financial analyses and interest on the part of investigative bodies). This summarizes the ability of the reporting entity to intercept transactions that pose an effective money laundering risk compared with elements of objective risk;
- *complexity*, measured for reporting entities belonging to the 'banks' category, gauges the ability to describe suspicious activities adequately, completely and efficaciously. The indicator is based on the number of persons and significant transactions referred to in the reports and on the degree of structuring of the elements provided.
- *emergence of anomalies,* an indicator calculated for money transfer operators, which measures the ability to identify anomalies in a multiplicity of spheres (operations, customers' subjective profiles, conduct of the territorial sales network).

Evaluation of reports' quality and complexity

Figure 1.6 shows the positioning of the main reporting entities of the 'banks' category in the four classes of quality/complexity of active cooperation. Each entity was compared with the average values for the category. The calculation was performed for 52 entities that sent more than 100 STRs in 2019. The reduction in the number of entities observed – from 60 in 2018 – primarily reflects the mergers of subsidiaries into a major bank parent company.

Figure 1.6

Scatter graph based on the quality/complexity of the reporting entities in the 'Banks' category that submitted more than 100 reports in 2019 (1)



(1) For each index, the average value for the category is 1.

Specifically, 13 of the intermediaries scrutinized submitted reports of above-average quality and complexity compared with the benchmark for the group (25 per cent of the sample, against 31.7 per cent in 2018). Another 19 operators submitted reports of below-average complexity but above-average quality (36.5 of the sample, compared with 23.3 per cent in 2018.

The reports of 8 operators (15.4 per cent of the sample, against 16.7 per cent in 2018) were of below-average quality but above-average complexity. Another 12 operators (23.1 per cent of the sample, against 28.3 per cent in 2018) fell in the worst-case group, with reports below average in both quality and complexity.

It must be observed, however, that the current year has seen marked signs of deterioration in the quality of reports, including those submitted by the most well-established and largest reporting entities. The information content of STRs displays increasing use of elements of an automatic nature, derived from inadequately tested new applications. Given the lack of careful scrutiny of the automatic data, this development is undermining the completeness and intelligibility of the reporting flow. A more careful revision of the criteria for using applications is needed, to prevent the new safeguards from impairing the quality of the reports.

1.4. Threshold-based communications

Legislative Decree 90/2017 introduced the possibility of asking obliged reporting entities to transmit to the UIF, alongside suspicious transaction reports, so-called threshold-based communications containing data and information identified on the basis of objective criteria concerning transactions at high risk of money laundering or terrorist financing.

Under these provisions, in September 2019, the Unit began surveying cash transactions carried out from April 2019 onwards. The communication obligation applies to financial intermediaries (banks and Poste Italiane spa, EMIs and contact points of EU EMIs, pay-ment institutions and contact points of EU payment institutions) and concerns all cash trans-actions for amounts of €10,000 or more, calculated on a monthly basis, carried out in instal-ments of €1,000 or more. The communications must be sent to the UIF by the 15th day of the second month following the reference month.

The Unit's decision to focus on cash reflects the particular risks bound up with the instrument. The ease of using cash and the untraceability of cash transactions can facilitate money laundering. Italy is one of the euro-area countries where recourse to cash is most widespread. [5] With the introduction of threshold-based communications, Italy has joined the group of countries that survey cash transactions for the purpose of preventing money laundering.

The communications received enrich the body of information at the UIF's disposal for examining suspicious operations and are useful for conducting analyses of the use of cash and for identifying flows potentially traceable to money laundering.

At the end of 2019, 570 operators were registered with the threshold-based communications transmission system. Of these, 135 filed a waiver request because they had handled no cash transactions or had only handled transactions for amounts below the thresholds ('inactive' reporting entities). The remaining operators consisted of banks (415), payment institutions and contact points of EU payment institutions (17), and electronic money institutions and contact points of EU EMIs (3).

The first months of the collection of threshold-based communications brought to light problems in the ability of even the system's foremost actors to correctly record data of particular importance for the prevention of money laundering: difficulties or the impossibility of recording transactions of less than €5,000, confusion between real-cash and virtual-cash transactions and systematic errors in payment details; in several cases there were considerable problems of data correction, despite the comments of the Unit. This revealed shortcomings in internal safeguards that in some cases could adversely affect customer assessment and even the ability to identify suspicious transactions.

In the light of these findings, operators were asked to make a special effort to improve their ability to have a complete vision of the data in the firm's possession. The UIF is introducing further controls to identify shortcomings in intermediaries' threshold-based communications and will monitor, including by inspection, the effectiveness of operators' commitments to remedy such shortcomings.

The communications for the first nine months of the threshold-based collection (April-December 2019), whose data, to be considered provisional, are being checked for quality,

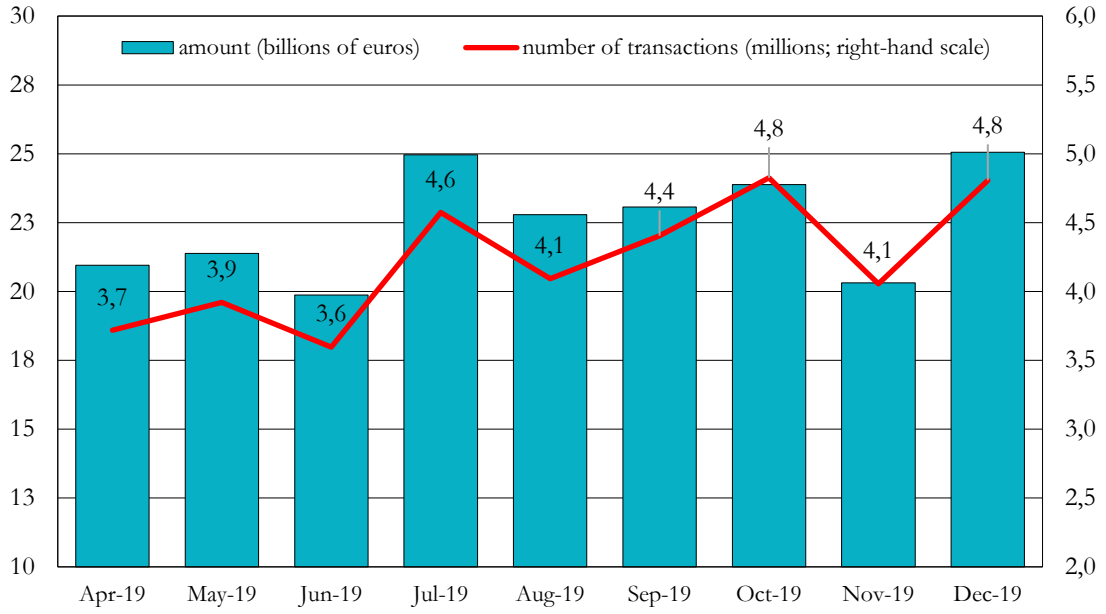
[5] See the ECB's surveys on payments at points of sale, *'The use of cash by households in the euro area'*; for Italy, 86 per cent of the number of transactions and 68 per cent of their total value are made in cash.

showed a monthly average of 4.2 million transactions (about 326,000 withdrawals and 3.9 million deposits), carried out by just over one million persons, for an average monthly amount of €22.5 billion (Figure 1.7).

Figure 1.7

Threshold-based communications

(April-December 2019)



A first overview of threshold-based communications

Threshold-based communications are a valuable source of information on the use of cash; they support the analysis of suspicious transaction reports and make it possible to extend the range of analysis beyond the anomalous transactions being reported.

This enlargement of the perimeter of observation concerns not only the identification of additional cash transactions by the same persons already recorded in the STRs but also other transactions carried out by other individuals connected in some way to the persons reported.

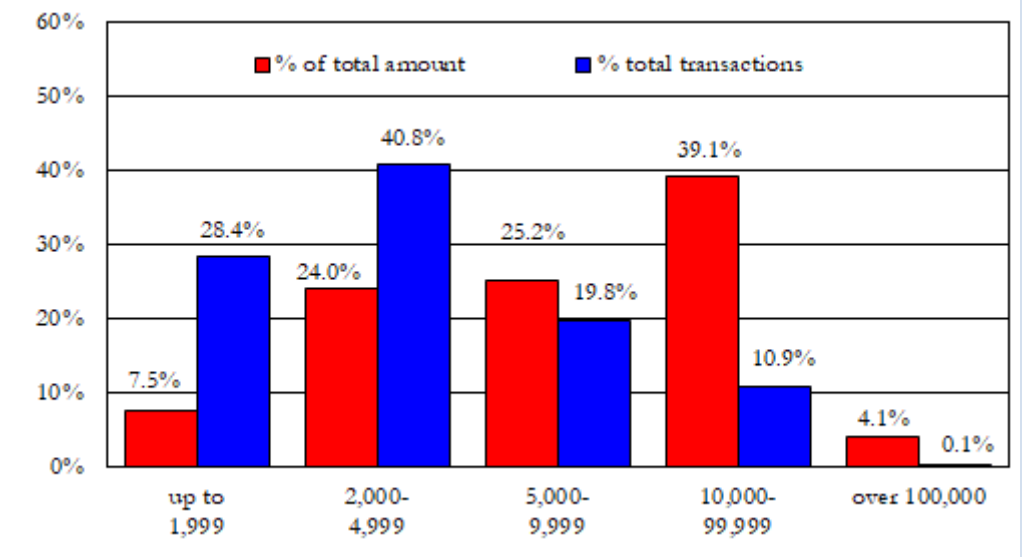
Furthermore, the size and systematic nature of the threshold-based communications information flow make it an important analytical tool for distinguishing activities linked to money laundering from those that are a normal part of the activity of specific operators. In addition, the size and level of detail of the new database assists identification of new and less well-established money laundering operations.

The provisional data for the period April-December 2019 show a concentration of the number of transactions in the €2,000-€4,999 interval and of the amount of transactions in the €10,000-€99,999 interval (Figure A).

Figure A

Threshold-based communications classed by amount

(April-December 2019; amounts in euros and percentage shares)

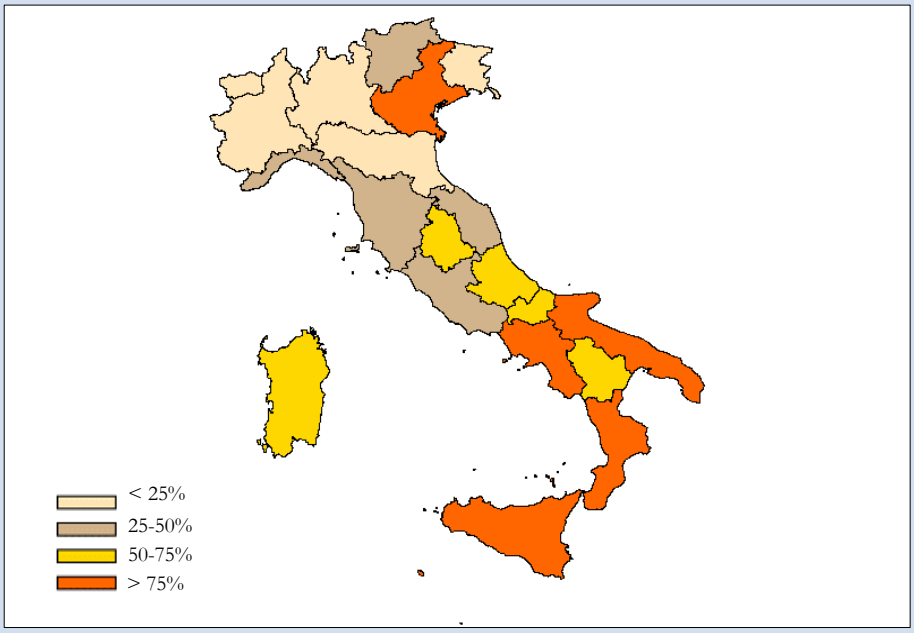


The median transaction amount was about €2,000 for withdrawals and €3,198 for deposits. At regional level, the total transaction amount was highest in relation to nominal GDP in Veneto, Campania, Puglia, Calabria and Sicily (Figure B).

Figure B

Threshold-based communications – amount by region

(as a percentage of nominal GDP; quartiles)



There were some 34,000 transactions of over €100,000 in the period for a total amount of about €8.4 billion.

Deposit transactions vastly outweighed withdrawals during the period, as is confirmed by the aggregate data in the SARA reports (see Chapter 6, 'Strategic analysis'). Deposits accounted for 92.3 per cent of the total number of transactions and 94.5 per cent of their total value. The difference in the size of the two flows appears to reflect, on the one hand, the need for households and firms to reduce the cost and risks of holding large sums for making purchases and, on the other, the large size of the deposits made by major retailers, who receive a high volume of small payments in cash.

Nearly all these cash transactions – 85.9 per cent of the withdrawals and 98 per cent of the deposits – were transactions involving bank accounts. The remaining transactions comprised an array of different types, from the collection in cash of credit transfers to the purchase of securities with cash payments to transactions at money transfer operators.

On average, the cash transactions communicated involved more than one million persons a month. More than 28,000 accounts registered in the threshold-based communications are also recorded in suspicious transaction reports received in the last three years.

2. OPERATIONAL ANALYSIS

The financial analysis conducted by the UIF is aimed at identifying transactions and situations linked to money laundering or the financing of terrorism. The information contained in the suspicious transaction report is integrated with the elements present in the Unit's various databases in order to redefine and expand the context reported, identify persons and relationships, and reconstruct the financial flows underlying the operations described.

The analysis, preceded by automatic enrichment of the data provided by reporting entities, is carried out using the UIF's dataset and makes it possible to classify the reports according to the risk and the phenomenon entailed. The most important contexts are then selected, handled in the most effective way and disseminated for subsequent investigations. The process follows a risk-based approach as defined by international standards and allows the Unit to adapt its work in light of the threats and vulnerabilities identified in the course of risk assessments and taking account of the results of strategic analysis.

2.1. The data

In 2019, the Unit analysed and transmitted 106,318 suspicious transaction reports to the investigative bodies, 8.4 per cent more than in 2018 (Table 2.1).

Table 2.1

Reports analysed by the UIF

	2015	2016	2017	2018	2019
Number of reports	84,627	103,995	94,018	98,117	106,318
Percentage change on previous year	*11.6*	*22.9*	*-9.6*	*4.4*	*8.4*

The number of reports analysed and transmitted during the year was again slightly higher than that of reports received, offsetting the increase in the latter and further reducing the backlog of reports to be processed.

2.2. The analysis process

The collection and management of STRs are supported by RADAR, a computerized system operating on the Infostat-UIF platform. Originally devised as the channel for acquiring the reporting flow and its first source of enrichment, over time RADAR has been enhanced with additional functions and applications, becoming a complex and diversified ecosystem whose compass extends to the exchange of supplementary documentation for the analysis of STRs.

One of RADAR's basic functions is the initial classification of reports. Each report is assigned a system rating, which, together with the risk level indicated by the reporting entity, is a tool for selecting flows and graduating priorities.

Processing time

Despite the growing number of STRs received, average processing time shortened from 22 to 20 days. The share of reports sent to investigative bodies within 30 days of receipt by the Unit rose from 77.5 to 79.5 per cent. Speed of processing increases with the riskiness of reports: 46.2 per cent of those with a higher risk profile are analysed and sent on within 7 days and 90 per cent within 30 days of receipt.

Information exchange with reporting entities

The exchange of information with reporting entities remains an essential juncture of the activity of analysis in which it is necessary to reconcile promptness with data security and confidentiality. During the year new functionalities were created that enable follow-up requests for information on STRs to be transmitted to the reporting entities registered with RADAR by means of the Infostat-UIF portal (see Section 10.4, 'IT resources'). The additional data acquired are protected by the platform's security safeguards and immediately enhance the information available to the Unit.

Threshold-based communications

The Unit's information assets, already supplemented by a multiplicity of databases acquired over time, were further enriched during the year by the start of collection of threshold-based communications. According to initial findings, the new information flow, though yet to realize all its potential, is already proving to be useful in providing a more immediate mapping of the financial relationships connected to those brought to light by suspicious transaction reports. As a consequence, it is possible to identify more accurately the subjective perimeter of the transactions analysed, taking account of additional natural and legal persons involved and often evidencing links between the different actors that cannot be recognized on the basis of an STR alone. With a view to increasing the utilities associated with the new database, the Unit is testing a special tool that will permit its analysts to better interpret the overall dataset made available by threshold-based communications sent by different reporting entities (see Section 10.4, 'IT resources'). Paths of analysis and monitoring of potentially anomalous flows are being prepared.

2.3. Risk assessment

Appropriate risk assessment of STRs is important both for financial analysis and in the subsequent investigative phases.

An initial appraisal is made by the reporting entity itself, on the basis of the information in its possession, by assigning a rating on a scale from 1 to 5.

As soon as the STR arrives at the Unit, it receives an automatic rating, again on a scale of 1 to 5, by means of an algorithm structured on mainly quantitative variables. This rating incorporates the additional elements in the Unit's databases regarding the context and the persons reported. Its rating takes account of the reporting entity's assessment, but it may diverge from the latter in relation to the wider spectrum of information used. Its accuracy also depends on correct and complete compilation of the STR by the reporting entity.

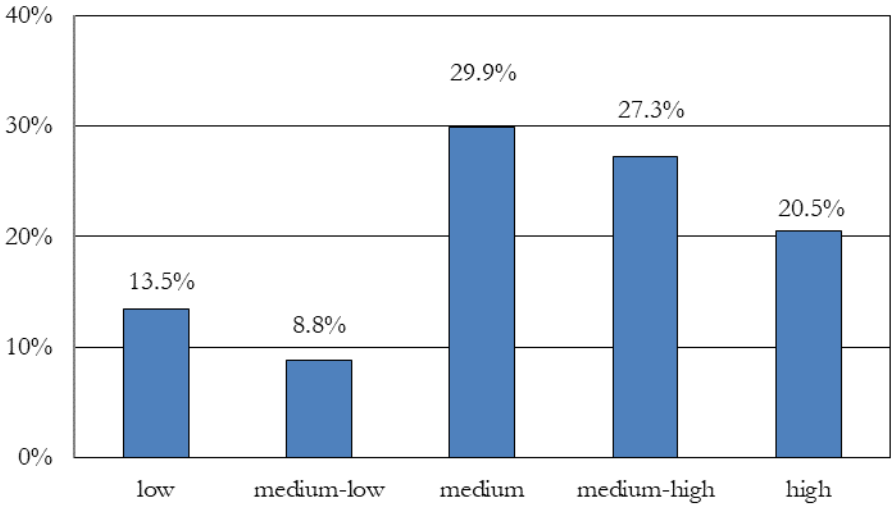
An automatic rating system, however sophisticated, obviously cannot always truly capture the typically qualitative possible risk factors that can be detected by financial analysis. The automatic rating may therefore be confirmed or modified in the various phases of processing by the UIF. Upon completion of the analysis, the report is assigned a final rating, which is then transmitted to the investigative bodies.

The distribution of the final ratings assigned to the reports analysed and processed in 2019 shows a slight accentuation of risk compared with the previous year: 47.8 per cent of the reports were considered to be medium-high or high risk, compared with 45.5 per cent in 2018 (Figure 2.1).

Figure 2.1

Reports analysed: distribution by final rating

(per cent)



Against this increase, the share of reports that received a medium risk rating declined from 34 to 29.9 percent, while that with lower risk ratings remained stable as a whole at 22.3 per cent.

Again in 2019 the reclassifications made following analysis mainly involved reports initially rated by the RADAR system as low or medium-low risk: 38.3 per cent of these STRs received a final rating of medium and 5.9 per cent one of medium-high or high risk. As in the previous year, there were fewer reclassifications in the opposite direction: of the reports initially rated as medium-high or high risk, 11.5 received a final rating of medium and 5.2 per cent one of low risk.

There was significant convergence between the risk assessments of the reporting entities and of the UIF: 43.9 per cent of reports (42.7 per cent in 2018) received a final rating in line with the reporting entities' assessments (37.9 per cent of those in the low or medium-low risk category and 73 per cent of those with high or medium-high risk ratings; Table 2.2).

Table 2.2

Comparison of STR risk ratings of reporting entities and the UIF's final ratings
(percentage composition)

		Risk indicated by the reporting entity			
		Low and medium-low	**Medium**	**Medium-high and high**	**Total**
UIF rating	**Low and medium-low**	16.8	4.2	1.3	**22.3**
	Medium	15.6	8.8	5.5	**29.9**
	Medium-high and high	12.0	17.5	18.3	**47.8**
	Total	**44.4**	**30.5**	**25.1**	**100.0**

Correct evaluation of STR ratings is essential for the efficacy of the Unit's entire action. Identification of the reports with a low risk rating is important for determining which reports require no further action. This judgment takes account of the indicators of investigative interest associated with each report (see the section 'Methodology,' below) and is communicated to the reporting entities periodically (feedback flows on negative results). At the same time, the assignment of higher risk ratings is important both for the development of analysis by the UIF and for the subsequent investigative phases.

The process therefore requires constant monitoring in order to verify that it is always capable of capturing the changes in the external context and in the pertinent databases. The algorithm that governs the calculation of the automatic rating is now being revised to ensure a better balance among the weights attached to the different variables in connection with the progressive enlargement of the data sources.

2.4. Methodology

Every suspicious transaction report received by the Unit undergoes a first-level analysis aimed at assessing the actual degree of risk and determining the most appropriate treatment. On the basis of the information acquired during automatic enrichment or from other sources, the grounds for suspicion of money laundering or terrorist financing and the need for further action are evaluated. Where the automatic rating does not seem to correspond to the effective level of risk, the analyst revises it.

If several prerequisites are met (full description of the activity and the grounds for suspicion; suspicion based on a well-known typology; impossibility of proceeding with further investigations; and the need to share the information quickly with the investigative bodies), the STR can be accompanied by a simplified report, thus optimizing processing time.

When further investigation is necessary to reconstruct the financial trail of suspect

funds, the STR undergoes a second-level analysis, ending with the assignment of a final risk rating and with a document accompanying the report to the investigate bodies that details the results of the financial checks carried out.

At this stage, the analysts have many investigative options and tools at their disposal. They can contact the reporting entity or other obliged entities to obtain further information, access the Revenue Agency's database, and consult the foreign FIU network, as well as make use of all the information retrievable from the UIF's own database.

The STR analysis process envisages a third level of evaluation, on an aggregate basis, for some typologies of reports (at present, money transfer reports). This assessment examines large sets of reports characterized by multiple small-value transactions, by the large number of persons involved, and by geographical dispersion in order to detect significant links and patterns even where the transactions, considered individually, appear unimportant.

Indicators of investigative interest

The integration of investigative data into the process of analysis plays an important role, helping to orient analysts' selection of cases for further examination towards contexts of potential interest in view of the criminal records of the persons reported. Given the persisting de facto constraints on the prompt acquisition of investigative information by the UIF, the linkage is supplied by the indicators of investigative interest that the UIF receives from the Finance Police. These help anaysts rank the effective risk of STRs.

Exchange of data with the DNA

The suite of investigative information available to the Unit has been enhanced since 2018 by the exchange of personal data between the Unit and the National Anti-Mafia Directorate (DNA), designed to flag the names of persons reported to the UIF that also appear in the DNA's records inasmuch as they are involved in ongoing penal proceedings. In 2019 the records exchanged were made more detailed, with the indication of the level of involvement for each person. During the year the DNA, after cross-checking with its records, provided positive verification for nearly 11,000 names reported in the more than 6,800 suspicious transaction reports. Some 39 per cent of the persons had a more pronounced criminal profile, according to a classification system shared with the DNA. Given that such information is proving to be highly useful in the various phases of analysis, full incorporation of the results of these information exchanges into the STR-handling process is under development.

Threshold-based communications

As part of the ongoing effort to strengthen the tools and sources of information, in 2019 analysts began making use of threshold-based communications, which afford new information synergies thanks to the integration of their information with the STR dataset. The objective is to highlight these transactions, which intrinsically present no elements of suspicion, where they are correlated with contexts of anomaly inferred from STRs.

Use of the Central Credit Register

In 2019, the Unit made better use of databases devised for ends other than the fight against money laundering but whose information is available to the UIF for analytical purposes. In this regard, steadily more integrated and versatile use was made of the Central Credit Register, a database managed by the Bank of Italy containing records, provided by intermediaries, on the loans granted to customers and on the guarantees provided by or received from customers. Consultation of the Central Credit Register more and more frequently enriches the financial analysis of a suspicious transaction report, contributing to the definition of the reported customer's relational perimeter through examination of the guarantees granted and received. The subjective links recorded by the Central Credit Register can

thus amplify those already shown in the report.

The Central Credit Register makes it possible to detect if the person reported has loans from other intermediaries, enabling the analyst to expand the mapping of the obliged entities that may be contacted in order to enhance the financial analysis.

Use of the Central Credit Register also assists identification of firms in crisis, which is among the factors determining their degree of susceptibility to pressure from organized crime and their exposure to the risks of embezzlement or usury. In addition, the Central Credit Register also provides data on customer debts that are two months past due, making it possible to evaluate the party's financial health even in the absence of financial statement data, which in any event tend to be older.

Aggregate analysis

Alongside detailed analysis of individual reports, the Unit employs a well-established method of aggregate analysis of STRs from money transfer agents. By means of massive examination of the information contained in the reports for a given time frame or specific operating modalities, aggregate analysis aims at picking up relationships and links between persons and transactions that are not immediately evident in the examination of individual reports.

In particular, specific risk indicators are used to detect the most critical positions with regard to the behaviour of money transfer agents, the operational characteristics of the customers and the anomalies found in the money transfer routes between the Italian province where the transfer is sent or received and the counterpart country. The results have been shared with the investigative bodies through the creation of an exchange channel parallel to that for the transmission of STRs.

Agents

For money transfer agents, the most common profiles of anomaly concern the safeguards of due diligence, which have often been found inadequate to detect dubious situations as regards the origin or destination of the funds transferred. The transactions that emerged frequently displayed an inconsistency between the place of origin of the customer and that of the counterparties, sometimes located in multiple foreign countries. Moreover, among the customers of some money transfer agents we find individuals with significant subjective anomalies, in some cases investigated for ascertained crimes. From the operational point of view, the Unit found frequent recourse to transaction splitting in order to circumvent the legal limits for money transfer operators. Another irregularity concerns money transfer agents who send money in their own name or manage money flows outside the traditional money transfer channel through the anomalous use of other instruments, such as prepaid payment cards.

Customers

In aggregate analysis, the identity of customers assumes importance mainly in relation to such risk indicators as number of transactions carried out and counterpart countries. Multiple movements within Italy, evidenced by the different places where the remittances are executed, are another risk indicator.

Payment instruments

The indicators also highlight the co-presence of suspicious transactions on more than one payment instrument, for example within the money transfer circuit, bank credit transfers and prepaid cards. This brings out contexts distinguished by a multiplicity of card top-ups or credit transfers ordered by counterparties in various countries and immediately withdrawn in cash.

Money transfer routes

The risk indicators for money transfer routes between an Italian province and a foreign jurisdiction are designed to pick up transfers that fall outside typical emigrants' remittances

and detect possible organizations, Italian or foreign, established in Italy engaging in opaque activities. The principal aspects examined are geographical inconsistency between the place of origin of those executing the transfers and the countries where the counterparties are located. Significant transaction volumes and a large number transactions and counterparties round out the set of risk indicators for the analysis of this profile.

Aggregate analysis and foreign criminal organizations

In 2019, the Unit also employed the aggregate analysis methodology to check on the possible interference of foreign criminal organizations in the use of money transfer circuits. The analysis, conducted on suspicious transmissions and receptions of money according to the customer's home country over a span of 30 months, enabled the Unit to profile the grounds for suspicion of the contexts reported, identify the originators' locations in Italy and determine if they were involved in activities in common with foreign nationals. The results were compared with the known operating characteristics and the main crimes ascertained for the non-indigenous mafias operating in Italy. Many points in common emerged, especially for several of the countries examined, such that criminal aspects or instances of commingling of foreign and local criminal activities cannot be ruled out.

The Unit is also extending this method of analysis to other sectors where there are typically a large number of low-value transactions and a multitude of customers, for example transactions with payment cards and virtual assets. This approach will be facilitated by the recent issuance of the specific reporting format for operators of the sector, which will permit the collection of more extensive, detailed and targeted data (see Section 1.1, 'Reporting flows' and Chapter 10, 'Resources and organization').

Joint analysis

Joint analysis of important cross-border cases continued to be conducted within the EU FIUs Platform (see Chapter 8, 'International cooperation'). During 2019, the Unit promoted two new initiatives of joint analysis that are still under way, one of which focuses on far-flung fraud and money laundering connected with the importing of goods from China at prices well below their real value.

2.5. Suspension orders

The UIF, on its own initiative or at the request of the Special Foreign Exchange Unit, the Anti-Mafia Investigation Department, the judicial authorities or foreign FIUs, may suspend transactions that are suspected of involving money laundering or terrorist financing for up to five working days, provided this does not jeopardize the investigation. Evaluation with a view to the possible issue of a suspension order is generally initiated autonomously upon receipt of STRs that show significant profiles of suspicion with regard to transactions not yet carried out or in response to unsolicited preliminary communications from intermediaries that provide advance information on the contents of suspicious transaction reports.

This power is particularly effective in delaying the execution of suspicious transactions for a limited period of time, until further precautionary measures can be taken by the judiciary.

There were 342 investigations with a view to the possible issue of suspension orders, as against 329 in 2018, with a significant rise in the value of the transactions examined, up by 53 per cent to €234 million. The increase in such examinations, a development already seen in the previous year, was basically due to the greater number of evaluations undertaken by

the Unit on its own initiative, which almost doubled, from 30 to 55, thanks to a new procedure for the systematic monitoring of reported high-risk transactions whose execution is pending (see Section 1.2, 'Suspicious transactions').

Overall, grounds for the issue of a suspension order were found in 43 cases (12.6 per cent of those evaluated, compared with 14.3 per cent in 2018, for a total value of €11.4 million; Table 2.5). In 9 of these cases, the order stemmed from evaluations begun by the Unit on its own initiative, which produced a higher rate of positive outcomes than those undertaken at the prompting of a reporting entity (16.4 against 12.6 per cent).

Table 2.5

Suspensions

	2015	2016	2017	2018	2019
Number of transactions	29	31	38	47	43
Total value of transactions (*millions of euros*)	16.7	18.9	66.4	38.8	11.4

As in 2018, the majority of the investigations concerned transactions being carried out at insurance companies or, to a lesser extent, at banks (respectively 83 and 13 per cent of the total). Nearly all of the transactions evaluated concerned policy surrenders or payouts at maturity traceable to persons under investigation for corruption or close to organized crime. One case involved a policy payout to a foreign national whose expulsion from Italy had been ordered for reasons of religious radicalization.

As for bank transactions, the most important case involved the ordering of foreign credit transfers by an individual who appears on the lists of the US Treasury Department's Office of Foreign Assets Control (together with relatives and a network of companies) due to formal charges for international corruption and money laundering. The transactions covered by the suspension order in this case amounted to €1 million. There ensued a court order for the seizure of an even larger amount. Among the other significant cases were two suspension orders issued for attempted tax fraud, one of which was brought to the UIF's attention by a municipality. In both cases, the attempted fraud involved filing for refunds of mistakenly paid taxes by means of offsets with non-existent tax credits.

2.6. Information flows on investigative interest

The Unit receives feedback from the investigative bodies on the level of interest of the STRs sent to them. This communication concerns the overall results of the further investigations conducted on the basis of the reports and financial analyses sent by the Unit.

Verification of the investigative interest of the reports transmitted is especially important for the UIF, in that while it also reflects factors unrelated to the Unit's work, it provides the Unit with important indications as to the efficacy of its enrichment of STRs and enables it to refine the criteria for selecting and assessing future reporting flows.

For the STRs sent to the investigative bodies in the two years 2018-19, as of the beginning of May 2020 the Finance Police had sent more than 37,400 positive feedback reports, of which 81.8 per cent concerned STRs classified as high or medium-high risk; only 2.9 per cent involved STRs rated as low or medium-low risk. Similar results were registered for the nearly 3,700 positive feedback reports received from the Anti-Mafia Investigation Department during the reference period, of which 88.4% referred to STRs with a high or medium-high risk rating.

3. RISK AREAS AND TYPOLOGIES

The UIF's operational analysis of suspicious transaction reports enables it to identify typologies characterized by recurring elements of relevance for assessing the risks of money laundering or terrorist financing. This allows the Unit to classify STRs and to disseminate updated indications in order to facilitate obliged entities' identification of suspicious transactions.

3.1. The main risk areas

In 2019, the first update of the *National Risk Assessment* confirmed the prime importance of the risk areas constituted by organized crime, corruption and tax evasion, whose intertwining makes it impossible to identify clear-cut lines of demarcation. In particular, recurring use is made of the toolkit typical of tax evasion both for money laundering by organized crime and for the creation of slush funds for purposes of bribery; organized crime habitually uses corruption to secure the complaisance of public administrators and officials. This makes it necessary always to adopt methodological approaches directed at transversal examination of the information contained in the reports.

The National Risk Assessment also emphasized that the panorama of organized crime is not limited to home-grown organizations; increasingly, account must be taken of the massive presence of foreign criminal bands which, regardless of cultural background or sector of underlying illegal activity, are all active on the money laundering front.

3.1.1. Organized crime

About 10 per cent of the suspicious transaction reports that the Unit received in 2019 pertained, at least potentially, to the interests of organized crime, broadly in line with the findings for the two previous years.

From the typological point of view, often these reports do not present financial anomalies different from those that may be detected in ordinary business transactions, owing to organized crime's penetration of the business sector. There are frequent cases of invoicing fraud, used by criminal organizations also for purposes other than tax evasion. Operations of this kind, found in about a fifth of the reports classified as potentially pertaining to mafia interests, ordinarily go together with intensive use of credit transfers, prepaid cards and cash. Among the main economic sectors involved are business services, fuel, car dealerships, transport and porterage.

There are also cases of blatant irregularities in the management of public funds obtained under public procurement contracts that constitute, often irrefutably, violations of the rules on the traceability of payments.

In 2019, again, significant domestic movements of funds designed to conceal resources from the tax authorities, commingled with apparently lawful flows, were often followed by the channelling of funds to foreign financial accounts. These resources are used to feed transfers between foreign accounts, withdrawals of cash (in some cases to be smuggled back into Italy), withdrawals on domestic ATMs using credit cards issued abroad, loans for business and real estate undertakings (both in Italy and abroad) and payments for goods and services supplied abroad to Italian firms and individuals.

The gaming and gambling sector (both physical and on-line gaming operations and casino management) is attractive to organized crime, which is present in almost the entire sector, including the management and leasing of slot machines and other gaming equipment.

The Unit further strengthened its approach of fully exploiting the information and data in the UIF archives, integrating them with those made available through systematic information exchange with the DNA. Almost all of the reports selected proved worthy of scrutiny: more than 84 per cent received a medium-high risk rating and 18 per cent underwent targeted inquiries, up from 16.1 per cent in 2018.

The criteria used for processing and analysis enabled the Unit to detect, fairly regularly, instances of fictitious conveyance of financial or real assets, often in anticipation of the imminent issue by the competent bodies of precautionary measures or orders in respect of assets. In such contexts, financial analysis makes it possible to identify, with a reasonable degree of certainty, the actors who, in various capacities, substitute for the real owners in management of the assets and in representation vis-à-vis third parties; further, analysis can also provide the investigative bodies with useful information about criminal organizations' more or less extensive networks of complicity, including persons who, though not part of the organizations, have willingly and knowingly abetted them.

As in the preceding years, the distribution of reports by region, calculated on the basis of first transaction reported, reveals a basic overlap with the regional distribution of mafia organizations mapped by the DIA and the DNA.

Heading the geographical distribution of the firms reported were businesses based in Campania (19.3 per cent), followed by firms based in Lombardy (18.8 per cent) and Lazio (14.5 per cent). The regions of Tuscany, Piedmont, Calabria, Sicily, Veneto and Emilia-Romagna were each home to between 4 and 7.5 per cent of the firms reported.

The ability to screen reports benefited from the activities conducted by the Unit as part of its institutional cooperation, defined by the legislative framework, with the investigative bodies and, more in general, with the judicial authorities. The resulting substantial qualitative improvement of analysis has made it possible to identify and understand contexts of ever greater complexity.

Among other examples of this were the analyses aimed at identifying potential uses of the international financial circuit by criminal groups that also avail themselves of foreign hackers through credit transfers and triangulations, the use of credit cards, prepaid cards and sham online transactions set up merely to transfer funds between two or more parties. There also emerged activities concerning an operational scheme apparently relating to mechanisms of tax fraud that were actually part of a larger operation designed to launder illicit proceeds on behalf of a complex criminal network through import/export activity. A closer examination was made not only of the instances of corruption detected in the domestic sphere, which involved members of mafia organizations, but also of cases of international laundering of the proceeds of crime (especially drug trafficking) carried on by mafia-like associations through corporate arrangements of varying complexity.

Foreign criminal organizations

During 2019 analysis was also directed to identifying contexts and operations ascribable to foreign criminal organizations. These kinds of STRs were often distinguished by a pronounced granularity of the transfers and by large numbers of persons involved, indicative of simpler modes of operation than those employed by the Italian mafia organizations. Those characteristics appear to be correlated with the ascertained tendency to operate by means of

money transfer agents and at the same time to use payment cards and, more recently, virtual currencies.

Among the most significant findings were those concerning Nigerian criminal associations. The transactions picked up most frequently were symptomatic of scams, marked by transfers of considerable sums ordered by senders located abroad to destinations concentrated in the North of Italy (especially in Piedmont, Lombardy and Veneto), and, as regards the South, in Campania (Naples and Castel Volturno) and Sicily (Palermo and Ragusa). The analysis often found the presence of persons who operate as collectors of funds originating partly abroad through credit transfers and top-ups of prepaid cards. Card reloads are paid for mostly in cash at merchants and post offices by a multitude of persons, prevalently Nigerians, or through credit transfers, with 'loan' or 'aid' declared in payment details, ordered by account holders at intermediaries, chiefly banks, based in Europe. The prepaid cards that receive the funds are used by persons most likely other than the nominal holders to make rapid series of withdrawals at ATMs located in some countries of sub-Saharan Africa, such as Togo and Benin, and, recently, to make payments at POS units of merchants located in Nigeria.

The recurrence of this scheme on a multitude of prepaid cards, often recently issued, appears consistent with the hypothesis of a structured organization, extremely difficult to map precisely, working throughout Italy to make massive funds transfers, suitably split up, to Africa and especially sub-Saharan Africa. Faced with such a network composed of a great many cards and persons, in-depth analysis identified anomalous transfers, including transfers abroad, traceable to a limited number of persons, some involved in judicial proceedings, potentially at the top levels of the organization.

It cannot be ruled out, therefore, that the prepaid cards were used to transfer proceeds of Nigerian organized crime, including scams tied to the disbursement of 'easy loans', as is suggested by the reasons given for some funds transfers. In theory, this hypothesis would be compatible with the practice of *osusu*, rooted in the southern regions of Nigeria, which consists in the pooled management of illicit resources by some members of a clan. Such an arrangement would create a network of deposits, systematically transferred throughout Italy among various accounts formally in the name of other persons in order to guard against attacks by rival clans or seizures by the judicial authorities.

Analysis resulted in further corroboration of the ability of Chinese criminal organizations to adapt their modus operandi in response to anti-money-laundering efforts. Last year's Report discussed the large flows of credit transfers from Italy to Hungary in connection with textile imports from China. More recent analyses confirm the transnational nature of the phenomenon, with the flows of financial resources and goods shifting to additional European countries (Germany, France, Spain, Slovenia, Czech Republic and Slovakia) and presumably a further change in the ports of customs clearance. To counter these new dimensions and operating procedures, the Unit has promoted a project of cooperation with the European FIUs for a joint study to achieve a fuller reconstruction of the financial flows and of the network of persons involved (see Section 8.4, 'The EU FIUs Platform').

3.1.2. Corruption and misappropriation of public funds

In analysis of the contexts ascribable to this risk area, in which identification of the significant cases of suspicion is traditionally more complicated, the communications of general government offices take on particular importance, alongside the suspicious transaction

reports coming from the private sector.

Although the legislative perimeter of active cooperation on the part of general government offices was diminished by Legislative Decree 90/2017, public offices remain an important element in the overall efficacy of the AML system. However, the sector's potential, which is considered vital especially as regards developments involving corruption or the misappropriation of public funds, remains largely untapped.

The communications transmitted by general government offices following the entry into force of Legislative Decree 90/2017, though few in number, show that some offices have organized and acted efficaciously, setting an example that can be replicated by those that so far have failed to budge.

In particular, several communications of interest derive from controls conducted as part of the activity of municipal one-stop shops for productive activities following receipt of certified declarations of commencement of activity. This suggests that there is no conflict between AML compliance and the instruments of administrative simplification and liberalization introduced by the reform measures taken in recent decades, since those instruments can well be a factor facilitating the recalibration of controls for AML as well as for other purposes.

The communications received from general government appear to fit together well with the STRs from other obliged entities, which are based on an informational framework that mainly valorizes financial information of a kind that is not normally in the possession of the public administrations involved. On the other hand, there is no lack of potential, fruitful overlap, for example where the suspicion pertains to the subjective profile, also detectable by general government offices on the basis of the anomaly indicators attached to the UIF's *Instructions* of April 2018.

Reception centres

The analyses carried out by the Unit found some anomalies with regard to the beneficiaries of public grants disbursed by prefectures as part of the reception system for migrants and asylum seekers. In these cases, the analyses of the flows downstream of the disbursements depict an essentially predatory situation characterized by: sizeable monetizations recorded on the accounts of the firms awarded the contracts or of recurring counterparties of those firms, often linked to the firms' beneficial owners (or their relatives); credit transfers on the part of the awardees with counterparties that operate in sectors with no apparent connection with the purposes of the expenditure charged to the government budget or that are barred from public contracts by anti-mafia measures; credit transfers ordered by awardee firms to beneficiaries active in the reception sector but under judicial investigation, in some cases by the competent Anti-Mafia District Directorate.

The most frequently detected anomalies include links between awardee firms and political office-holders (or former office-holders) in local government jurisdictions where some of the reception centres managed are located. Another anomaly consists in the exclusion of companies from the tender procedure owing to evident connections such as to suggest a management of the reception services traceable to a single nexus of interests.

Consulting firms

In some contexts connected with the management of large amounts of public funds, the suspicion concerned the involvement of consultancies with anomalous elements generally having to do with the subjective profile of the firm, often recently established and traceable, via figureheads, to politically exposed persons (PEPs). Sometimes the object of the consulting contract also appeared to be inconsistent with the consulting firm's activity and

with the subjective profile of its covert owner. More in general, recourse to firms that are formally unconnected to a PEP is a recurring element that serves to make it difficult to reconstruct the connections between the different persons that intervene in transactions with general government, thereby concealing links or conflicts of interest that could decisively affect the good outcome of the transactions.

Corruption

The provision of benefits to holders of important public offices was inferred in some cases from the payment of utilities of various kinds (trips, for example, or renovation expenses) arranged, perhaps only partially, by the interested parties or, more often, by companies or third parties linked to them. In such situations, therefore, the direct transfer of goods from the corrupter to the corrupted is absent, given payment to third parties in the latter's interest, making it harder to trace the utility conferred back to the public office-holder.

In other cases, the suspected corrupter provided the utility directly to the PEP through transactions which, while formally lawful, were concluded on more favourable than market terms and conditions (as in the case of real estate purchases or sales or renovation work).

Frauds on regional funds

Analysis brought out transactions indicative of possible frauds regarding the allocation of regional funds for the incentivization and growth of small and medium-sized enterprises in the service sector. The scheme is based on the ad hoc creation of companies and business networks to take part in public tenders for funds for restructuring projects which turned out to be fictitious. Once the grants are awarded, a system of false invoicing is used to transfer them to companies in eastern Europe, presumably engaged for restructuring work but actually shell companies owned by the same Italian entities. Subsequently, after various passages, including between foreign jurisdictions, the funds are transferred back to Italy and put at the disposal of the same entities through figureheads. Analysis detected frequent possible conflicts of interest deriving from the links between the heads of the companies awarded the funds and the control bodies of the contracting entities.

'Citizen's income'

In 2019 the Unit received some STRs bearing on possible anomalies in the management of prepaid cards for the receipt of funds disbursed under the anti-poverty measures of Decree Law 4/2019, converted into Law 26/2019. Among the amonalies most often detected were the preventive drawing down to zero of current account balances, generally through cash withdrawals, preparatory for subsequent applications for 'citizen's income' benefits. The card holders, some of them at the centre of judicial proceedings or close to criminal organizations, were often found to have other accounts with the Italian banking system.

3.1.3. Tax evasion

Suspicious transaction reports pertaining to possible tax evasion remained broadly unchanged in number from 2018, but their share of STRs received diminished slightly to about one fifth. The majority of such reports (around 75 per cent) again concerned familiar schemes involving transfers of funds between connected natural and legal persons, possible false invoicing, the use of personal accounts for the transit of what appear to have been business transactions, and cash withdrawals from companies' accounts. In addition, a fifth of 'tax-related' STRs involved cross-border transactions potentially ascribable to international carousel fraud.

Assignments of VAT credits and assumptions of tax liabilities

Reporting entities continued to intercept anomalous transactions attributable to assignments of VAT credits and assumptions of tax liabilities potentially designed to obtain improper offsets of tax and/or social security contribution credits under ad hoc schemes also involving the participation of complaisant professionals who, for very substantial fees, act as

tax consultants or sometimes as escrow agents.[6]

In several cases, anomalies were found in the subjective profiles of the companies taking over the tax position (including numerous changes of registered office, corporate officers, shareholders, etc.) as well as prejudicial information on their shareholders or corporate officers. Widespread accounting anomalies were also found, such as sudden, significant increases in turnover or purchases, set against a relatively modest financial position, with little or no outlays for personnel or for the use of third parties' goods. As a whole, the anomalies detected suggested that many of the credits involved in the contacts for the assumption of tax liabilities were non-existent, confirming the risk inherent in such cases.

Carousel fraud

The inquiries conducted on the reports received from banks regarding numerous companies operating in a variety of sectors (steel, electronics, sale of plastics) brought to light recurring operating schemes for the most part directed at channelling large financial flows abroad, especially towards central and eastern Europe. At times, one finds a sequence of credit transfers to apparently unrelated firms, followed by the transfer of sums to common counterparties abroad, who in turn pass the sums on to other companies attributable to Italian persons and holders of bank accounts in another country of eastern Europe. At the completion of this circuit, the funds are used to make credit transfers for the payment of invoices to the benefit of the same Italian companies from which the financial flows had originated.

Withdrawals with foreign credit cards

The repatriation to Italy of funds deriving from tax frauds continues in all likelihood to be achieved in part by means of withdrawals of cash at Italian ATMs using foreign credit cards. Cash withdrawals via cards issued by foreign banks remain a significant phenomenon. An analysis of reports regarding withdrawals at ATMs in Italy in the period May-September 2019 showed that those with cards issued by Hungarian banks amounted to more than €46 million, followed by Slovakia with €2.8 million, Poland with €1.1 million, the United Kingdom with €800,000, the Czech Republic with €500,000 and the United States with €300,000. Most of the ATMs at which the withdrawals were made are located in the North, with those in Lombardy and Veneto accounting for about 65 per cent of the total volume.

Laundering of proceeds of tax fraud

In the reports motivated by suspicions of tax fraud, the monetization of funds deriving from presumably unlawful acts is a particularly frequent feature, especially in the sectors of trade in fuels and trade in metals. In some cases, a network of apparently unconnected sole proprietorships and partnerships was found to be interposed between the suppliers of funds and the persons responsible for their monetization. These interposed parties carried out a series of transfers for amounts far in excess of their potential economic capacity by means of credit transfers in round figures and with generic payment details, sometimes referring to advance payments of emoluments.

Tax havens

During 2019 the Unit devoted special attention to the analysis of STRs regarding closed-end investment funds based in countries at risk. Cases of particular interest included one involving very large investments carried out with loans granted by a special-purpose vehicle wholly owned by a closed-end fund, both of them headquartered in tax havens, to a group of Italian companies active in the purchase of receivables. The group of firms receiving the investments proved to be attributable, via a foreign holding company, to an Italian person previously arrested on charges of laundering money by transferring funds abroad via false invoicing and subsequently paying over the money in cash to the network of businessmen involved.

[6] See Chapter 5, 'Controls'.

The money laundering risks emerging from the COVID-19 pandemic

The COVID-19 pandemic has given rise to new money laundering risks and accentuated others already widespread in the economy. Aware of the need for adequate safeguards against these risks, the UIF has focused on some recurring areas and modalities both during the lockdown and during the reopening of economic activities.

The most severe risk, given its long-term consequences, pertains to the impact of the crisis on the productive economy, threatened by criminal infiltration that can distort the operation of the markets and competition. The liquidity crisis afflicting many of the idled firms is a fertile terrain for **acquisitions of ownership or control of sizeable portions of the productive economy**, especially on the part of organized crime, which has ample reserves of funds deriving from illegal activities.

Businesses are also particularly vulnerable to offers of **usurious loans**, aimed both at profiting from higher-than-legal interest rates and at business takeovers, facilitated by repayment difficulties. The risk of usury could also involve individuals with precarious employment situations due to business shutdowns.

Significant risks can also derive from the **unlawful acquisition of various public subsidies** intended to help individuals and firms ride out the economic crisis generated by the pandemic. In this sphere, there can emerge forms of **corruption** of public officials, of politically exposed persons or of firms connected to them, aimed at gaining an inside track of access to public funds even where the requisite qualifications are lacking. There could also be an increase in **fraud against the State** by means of false attestations of possession of the requirements for the subsidies.

The **healthcare sector** is highly vulnerable, particularly to possible **fraud and corruption in the procurement of supplies** to deal with the emergency (protective equipment, medical equipment and devices, medicines). The emergency situation can induce hospitals and local administrations to turn to unknown suppliers who offer products that turn out to be non-compliant with the standards or are never shipped.

A field of crime that is expanding with the pandemic is **fraud to the detriment of the private sector**, carried out primarily online and represented by two main types of cases. The first exploits the high demand for healthcare equipment by offering private individuals counterfeit or non-existent products. The second solicits donations for charitable or support interventions during and after the health crisis, donations that are never used for the declared purposes.

The restrictions on personal movement introduced especially in the most acute phase of the pandemic heighten the risks of the **use of the Internet to engage in illegal activities or to launder the proceeds of crime.** Growing exploitation of the dark web, of social media and, in general, of online marketplaces to sell illegal products or to carry out scams to the detriment of individuals can be expected. The migration of financial transactions and funds transfers from intermediaries' branches to online platforms, which entail greater monitoring problems, is also foreseeable.

Between January and April 2020, obliged entities sent more than 200 suspicious transaction reports linked to the COVID-19 pandemic. An initial survey of these STRs showed numerous cash withdrawals associated with fears of measures imposing social contain-

ment and confinement, withdrawals which in some cases could hide illicit purposes. Another pattern pertains to the supplying of personal protective equipment (PPE) to both private sector customers and public sector entities. In such cases, the grounds for suspicion generally lie in the absence of the technical requisites mandated by health regulations and incongruence between the size of the procurement order and the entrepreneurial standing of the supplier, or its non-involvement in the PPE sector. In a still very limited number of STRs, the subjective profile of the persons reported appears to suggest the possible involvement of organized crime in usury-like arrangements.

The Unit has developed a dialogue with the authorities, the judiciary and the investigative bodies, and it has formulated proposals for amendments to the emergency legislation with the aim of reconciling the essential need for speed in delivering public support with that of safeguarding legality. In April 2020, the Unit issued a Communication to heighten reporting entities' awareness of the risk profiles connected with the pandemic and its train of economic consequences.

3.2. Further case studies

Pyramid schemes

In 2019, analytical activity again turned up contexts of financial anomaly classifiable as pyramid schemes. The distinguishing features of this form of fraud are the offering of investment plans, which in reality are non-existent, with the promise of high returns, generally far above those achievable with traditional forms of investment; and continual recruitment of new investors by those at the top of the pyramid or by persons who have invested, in order to remunerate the persons already involved in the scheme.

This type of fraud was found in diverse sectors of activity. The Unit received numerous reports regarding suspected pyramid schemes carried out by means of unauthorized online trading platforms. Our analyses made it possible to reconstruct a complex and sophisticated system whose transnational nature is evinced both by the nationalities of the victims and by the registered offices of the companies involved in the anomalous flows. In several cases, virtual asset service providers and FinTech payment institutions figured among the companies involved in the fund transfers.

The analysis of some reports underlined suspected pyramid schemes in the intermediation of wholesale telephone traffic. Some Italian companies, most of them formally owned by possible figureheads, collected funds from natural persons on the basis of profit-sharing contracts. Analysis of the transactions on the accounts highlighted: the absence of return flows to the great majority of investors, accompanied by flows to only some investors that could be interpreted as remuneration at a very high rate, the absence of credit entries hypothetically attributable to revenues, and debit entries apparently unconnected with business activity. In some cases, significant transfers abroad were found, including flows to companies with the same beneficial owners as the Italian companies or attributable to individuals already known for engaging in unauthorized financial activity and money laundering.

Indications of possible pyramid schemes also emerged with reference to the credit recovery sector, mostly in connection with real estate. In these cases, networks of professionals or firms propose advantageous investment opportunities through profit-sharing partnership contracts for the recovery of defaulted real estate loans. The funds collected for investments, often through accounts seemingly held by companies specialized in debt collection but actually traceable to the professionals themselves, are used to make payments partly to previous

investors and partly to other persons belonging to the network, some of them already referred to in previous STRs or involved in penal proceedings. In some of these cases, alongside the profiles typical of scheme, there emerged elements indicative of possible unauthorized financial activity, given the lack of the required authorizations for the companies that collect the associates' capital with the promise of repayment plus a significant return.

Concerted trades of securities

As in the previous year, the Unit received reports of suspicious securities transactions carried out in various financial markets and involving both relatively illiquid instruments and liquid securities with a high number of daily trades. The cases observed were characterized by cross trades carried out with suspicious procedures and timing for order entry and originating from a prior agreement between the parties involved. Analysis of the transactions found frequent recourse to the so-called double-cross technique, with the parties concluding two consecutive contracts in which they switch sides as buyers and sellers and which are concluded at different, sometimes non-market, prices, generating systematic capital gains or losses for one of the parties. The ultimate objective of these trading schemes appears to be to transfer liquidity, sometimes for large aggregate sums, to the party that realizes the capital gains. Often, the trades are between relatives or persons with business relationships, corroborating the suspicion of concerted trading.

Potential cases of market manipulation were also detected, albeit for modest amounts, by the analysis of cross trades on illiquid securities concluded by the same person simultaneously with two intermediaries (so-called wash trading).

In other cases, the transactions examined were considered to be potentially aimed at achieving tax optimization in light of the possibility of offsetting artificial trading gains and losses between securities portfolios held with the banks involved.

Frauds on SDD

A number of cases were detected of fraudulent use of the SEPA Direct Debit service (SDD), which makes it possible to collect euro-denominated payments within the Single Euro Payments Area on the basis of a preliminary agreement ('SEPA mandate') whereby the debtor authorizes the creditor to debit the debtor's payment account.

Attempts to perpetrate fraud by means of SEPA direct debts, targeting dormant or rarely used accounts, had already been uncovered in the past.[7]

The fraudulent activation of the SDD debit was carried out against unwitting bank account holders (who were then found to have been swindled). The anomalous uses observed more recently are attributable to attempts to commit fraud at the expense of the banks where the presumed creditor's account is established. In some cases, the creditor is a new customer of the bank or a company that has had a recent change of ownership. In others, the creditor is a long-standing customer in evident economic difficulty or one whose account shows no transactions in the last year. In the cases examined, the presumed creditor presents to his own bank the commercial documentation in support of the collection, including the SEPA mandate signed by the presumed debtor. The amounts generated by the creditor bank via the collection service are immediately used by the 'creditor' by means of urgent credit transfers, sometimes ordered online. Within the first two business days following the interbank settlement of the direct debit, the creditor bank receives the debtor bank's rejection message, often owing to cancellation of the IBAN or to insufficient funds on the debited account. The

[7] See UIF *Annual Report for 2017*, p. 60.

debtor is often a foreign company or else an Italian company whose beneficial owners present profiles flagged for attention.

During 2019 the Unit analysed numerous STRs from leading domestic financial intermediaries following an extensive internal survey of triangulated financial flows on accounts with foreign banks which were reported in the press to be involved in international money laundering.

Baltic banks

The Unit reconstructed a highly structured international money laundering operation carried out by means of newly established Italian and foreign companies in a complex chain of corporate ownership set up for the specific purpose of making investments in Italy. The very substantial amounts of capital that flowed to the accounts with Italian banks were invested in Italy to buy farms and expensive properties. The funds in question originated from a major fraud perpetrated against a foreign bank through a series of loans received by multiple companies. The reconstruction of the complex operation traced the ownership of these funds of illegal origin to foreign PEPs or to East European nationals previously investigated for money laundering. The supervisory authorities of some of the Baltic banks involved in triangulating the flows had adopted measures against them for presumed violations of AML/CFT legislation.

Prepaid cards and IPTV

Transactions on prepaid cards emerged that appear to be correlated with the illegal supply of Internet Protocol Television services (IPTV) whereby subscribers receive unlawfully acquired, copyright-protected content. On the financial plane, the operation entails the reception, through the diverse channels available, of hundreds of reloads to prepaid cards carried out by a multiplicity of natural persons located in different parts of Italy. The funds thus accumulated are used not only to purchase electronic equipment, presumably for acquiring the content and retransmitting the pirated signal, but also to make significant payments to foreign suppliers of Internet data transmission services through the leasing of high-capacity servers. With regard to these transactions, carried out by numerous persons in different areas of Italy many of whom are officially not employed, the existence of centrally directed networks cannot be ruled out. Should further investigation confirm this, the case in point, which originally emerged from the financial analysis, would become a criminal matter, involving at least the possible offence of receiving stolen property for the subscribers to the illegal service, and at the same time would constitute an important violation of private law, involving substantial losses for the owners of the protected content.

Analysis of transactions symptomatic of financial fraud brought out a money laundering scheme centred on the promise of loans on the part of self-styled consultants to persons in financial difficulty. In return for the promises, which proved to be false although they were formally contractualized, the potential borrowers were asked for sums in advance to guarantee the positive outcome of the operation. According to the story offered by the 'consultants,' the loans were to be disbursed drawing on the enormous stock of liquidity of foreign investment companies upon presentation of documentation which was later ascertained to be counterfeit (for example, transaction records of SWIFT wire transfers with IBANs which either did not exist or were not those of the accounts held by the foreign companies that were supposed to supply the funds). In the cases examined, the names cropped up of Italian individuals who are already receiving attention from the investigative bodies for violations of financial and insurance laws involving the use of foreign companies.

Purchases and sales of compensatory building rights

Some transactions in compensatory building rights potentially aimed at laundering funds of dubious origin were detected. Such rights are awarded as compensation to owners of tracts

of land that are transferred free of charge to the city in which they are located. They entitle the beneficiaries to build in any part of the city, but they may also be transferred to other persons interested in doing so. From the information available, it emerged that only a small percentage of these rights were used for actual building; the unutilized remainder were in the hands of a few individuals. The remaining building zones are limited and situated far from city centres, so the market in these rights would not seem to promise particular advantages for the seller. Nevertheless, it was found that multiple transactions in such rights had taken place in a short span of time, in some cases resulting in considerable capital gains. The grounds for suspicion consist in the possibility that the transactions in rights may be connected with the laundering of capital of dubious origin or are somehow directed at creating a sort of local monopoly in building by concentrating the limited supply of rights still available in the hands of a few persons.

3.3. Emerging risk sectors and areas: virtual assets

Beside known and long-established risks, the Unit also pays constant attention to emerging and innovative sectors that may be harbingers of new risks and opportunities for unlawful use.

During 2019 the UIF continued to carefully monitor reports of suspicious transactions involving virtual assets. The results of the analysis of these STRs confirmed several general trends already observed in the past. Very often, these reports appeared to have been submitted not so much on definite grounds for suspicion but because of the high level of risk held to be inherent in the instrument.

In more well-defined contexts of anomaly, virtual assets come into play with some frequency downstream of suspected swindles, cyber fraud or unauthorized financial activity: in such cases, the purchase of virtual currencies represents the first employment of the proceeds. Cases of virtual currencies being used in connection with phishing, ransomware, corporate embezzlement and tax evasion (often tied to invoicing fraud) were also reported.

In this regard, a possible anomalous use of virtual currencies emerged in the course of ongoing monitoring of the larger phenomenon of anomalous financial flows connected with the under-invoicing of textile imports from China in order to evade VAT and customs duties.[8] On the basis of information supplied by the Customs and Monopolies Agency, it was found that the declared taxable value of these goods at the time of customs clearance was often lower than their real value. From the financial viewpoint, such under-invoicing means that the Italian importers have to pay their Chinese suppliers the difference between the invoiced value and the real value of the goods by means of systems and procedures that are less readily traceable compared with the banking channel. The in-depth analyses conducted in 2019 ascertained that growing use is made of virtual currencies to transfer the flows connected with this phenomenon out of the country.

A number of reports concern the persons who operate in the capacity of collectors. In many cases, they promote their activity via the Internet (blogs, websites, etc.), collecting funds through reloads to prepaid cards, credit transfers and cash deposits that are individually small but cumulatively significant. This activity is comparable to that of a professional ex-

[8] See UIF *Annual Report for 2018*, pp. 40-41.

changer but is presumably carried on without an adequate organizational structure to guarantee customer protection and compliance with AML laws and regulations. The activity of collectors entails evident risks of money laundering in that it creates an interposition that prevents the trading platforms used from knowing the beneficial owner of the sums invested in virtual currencies. In this regard, some STRs report an activity of fund-raising by means of reloads to prepaid cards, originated by numerous non-EU nationals, which are used to purchase virtual currencies with funds of illicit provenance.

The Unit reconstructed suspicious transactions which were unrelated to the type of arrangements mentioned above, also assisting in investigations conducted by the judicial authorities. Thanks to blockchain analysis, it was possible to identify payments in bitcoins to alphanumeric addresses attributable to a dark web site used for acquiring stolen credit card credentials or to virtual currency payment platforms on the dark web that make it possible to buy and sell illegal goods and services.

One case brought to light a network operating in several countries to launder money through the use of virtual assets in which an Italian citizen was involved. This person had made transfers of significant amounts, in different virtual currencies, which were not compatible with his subjective profile. Analysis of the transactions found: the use of virtual currencies with counterparties active in the dark market; interaction with foreign exchangers who do not appear to have adequate safeguards against money laundering or are involved in investigations for money laundering; and peer-to-peer trading on virtual currency trading platforms, presumably intended to obstruct the traceability of the financial flows. The overall operation also featured the use of money transfers and prepaid cards to support the purchases and conversions of virtual currencies by the persons belonging to the network.

Examination of the financial flows attributable to a group of foreign nationals active in Italy and under investigation for mafia association, money laundering and fraud detected a possible channel for money laundering, namely the use of virtual currencies, purchased by Italian citizens who were reported to the Unit on several occasions as collectors and are also under investigation. The in-depth analysis found possible recourse by said persons to a foreign wallet provider and exchanger through which they apparently converted virtual currencies into legal tender, which they then sent back to their home country.

The Unit brought to light the operations of a foreign company that in an initial phase received substantial sums on its foreign account from Italian investors, acting without the required authorizations, and purchased virtual currencies through an Italian exchanger, with the declared purpose of realizing high profits through arbitrage and revaluation of its virtual currency holdings. In a second phase, the funds from the Italian investors were raised directly in virtual currencies. In particular, the analysis pointed up the risk that at least part of the funds acquired had been transferred to wallets of the company's presumable owners.

Furthermore, there emerged many instances of transactions in virtual currencies connected with unauthorized financial activity. These cases involved foreign companies, lacking authorization to operate in their home country, already sanctioned by Consob for unlicensed offering of investment services online to the public in Italy. Frequent attempts to clone or duplicate the names and corporate information of some authorized operators were recorded on the websites of these unauthorized operators.

4. COMBATING THE FINANCING OF TERRORISM

The activity of the UIF in preventing the financing of terrorism is framed in an international setting that in 2019 saw the threat of jihadist terrorism change shape, reflecting the vicissitudes of the so-called Islamic State. In these circumstances, it remains important to monitor the activity of small groups (cells) or individuals (lone wolves) that stand ready to act. These micro-formations are not only made up of former foreign fighters back from the theatre of war in the Middle East (returnees); increasingly, they also include people with no previous experience of warfare, often self-radicalized through exposure to forms of online indoctrination that incite terrorist attacks with a low organizational profile, relying exclusively on individual initiative and personal means.

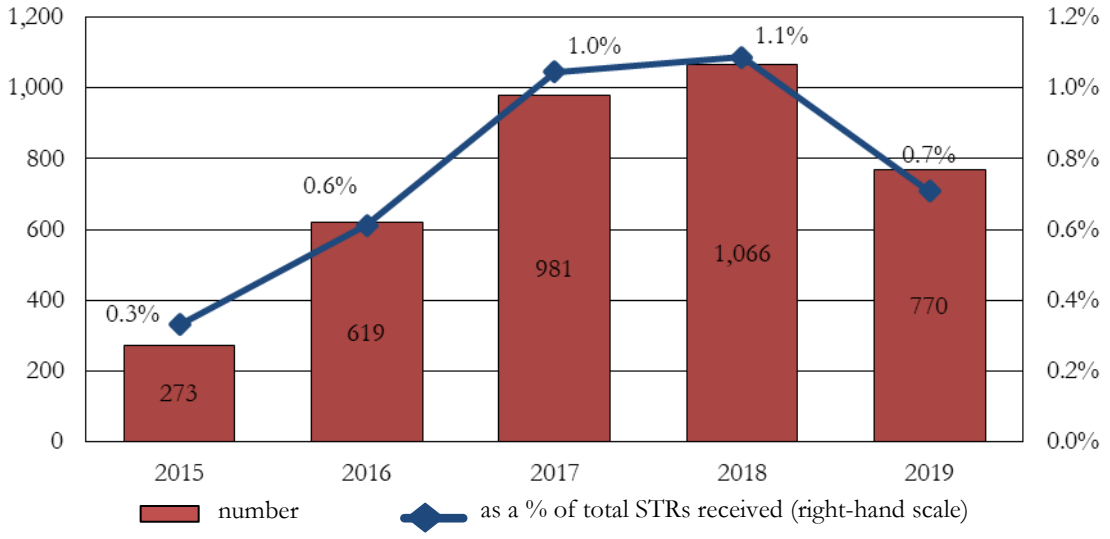
4.1. Suspicious transaction reports

The STRs classified by reporting entities as suspected terrorist financing numbered 770 in 2019, or 0.7 per cent of all the STRs received by the Unit, down by more than a quarter (-27.8 per cent) from 1,066 in 2018 and by about a fifth (-21.5 per cent) from 981 in 2017 (Figure 4.1). The rising trend for this category of STR thus came to a halt, although the number of reports was still higher than before the onset of the terrorist attacks in 2015, a sign of well-established attention on the part of the system.

Figure 4.1

Financing of terrorism reports received

(*number of reports and share of total STRs*)



The decline in STRs for financing of terrorism is also due to more stringent selection of the contexts considered to be at risk, partly in response to the indications contained in the UIF Statements on the matter.

The breakdown by type of reporting entity was basically unchanged: payment institutions were again the leading contributors, sending nearly half (49.1 per cent) of the reports. The decline in the share transmitted by banks and Poste Italiane spa and the increase in that sent by electronic money institutions partly reflected a major corporate reorganization (see

Section 1.1, 'Reporting flows'). The contribution of other financial intermediaries and of non-financial entities remained modest.

Table 4.1

Reports on financing of terrorism by type of reporting entity

	2018		2019	
	(number)	*(% share)*	*(number)*	*(% share)*
Banking and financial intermediaries	**1,031**	**96.7**	**736**	**95.6**
Payment institutions and contact points	514	48.2	378	49.1
Banks and Poste Italiane spa	480	45.0	267	34.7
EMIs and contact points	17	1.6	72	9.3
Other intermed. and fin. operators (1)	20	1.9	19	2.5
Non-financial obliged entities	**35**	**3.3**	**34**	**4.4**
Notaries and Nat. Council of Notaries	12	1.1	14	1.8
Other non-financial entities (2)	23	2.2	20	2.6
Total	**1,066**	**100.0**	**770**	**100.0**

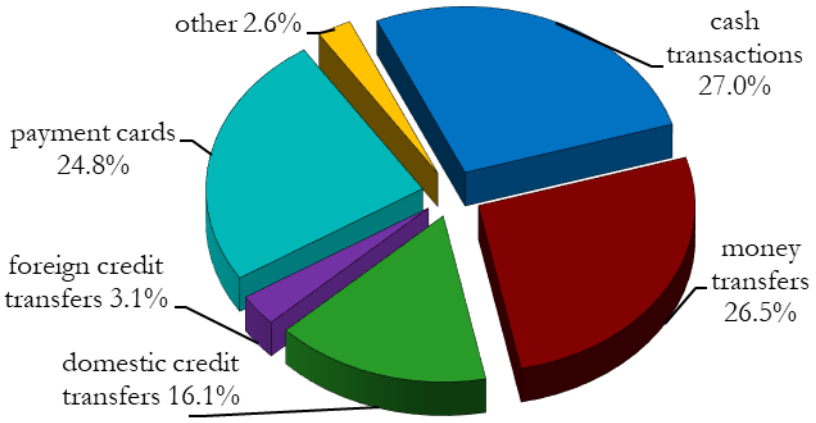
(1) Financial intermediaries and entities not included in the above categories. - (2) Non-financial entities not included in the above category.

The 770 reports covered some 62,000 transactions, 10.3 per cent fewer than in the previous year. The large number of transactions reflects the particular nature of the reports by money transfer operators, which refer to often very complex networks of remittances: the STR does not just refer to the transactions strictly connected with the grounds for suspicion but extends to the rest of the transactions of the persons ordering the transfers and of those with whom they have dealings.

Compared with 2018, cash transactions fell from 34.3 to 27 per cent of the total number reported, while the share of transactions carried out using payment cards rose to about 25 per cent. The percentage shares for the other categories of transaction were broadly unchanged (Figure 4.2).

Figure 4.2

Technical forms of reported financing of terrorism transactions (1)
(*percentage shares of reported transactions*)



(1) The data refer to the actual number of transactions, including those cumulated in single reports.

The greater incidence of reports of suspicious transactions carried out with payment cards in part reflects sensitization activity on the part of the Unit, which in recent years has called reporting entities' attention to the possible use of payment cards to finance terrorism not only in its published Statements but also in a number of representative *case studies* of other illegal phenomena potentially exposed to this risk. These include migrant trafficking, exploitation of human beings and recourse to *hawala* – activities in which even very large financial flows can be channelled by means of cards, which afford considerable flexibility of use.

Geographical distribution

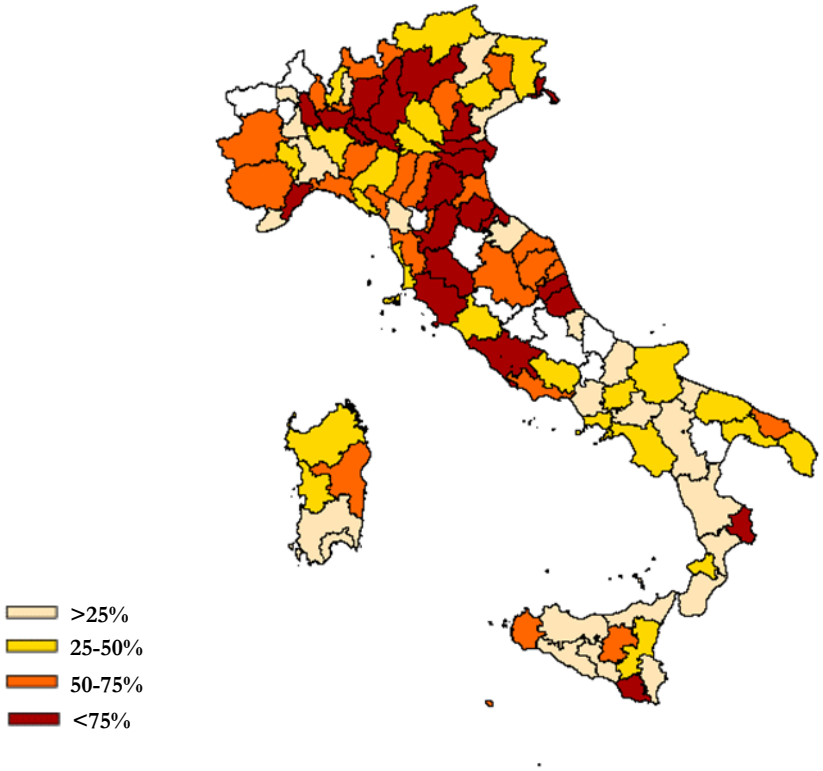
The geographical distribution of terrorist financing STRs was the same as in 2018. The concentration in the regions and provinces of the Centre and North can be explained by the presence of larger communities of persons from countries affected by phenomena related in various ways to jihadism (theatres of war, theatres of terrorist attacks, foreign fighters' home countries, countries with zones under the control of jihadist organizations). However, it also reflects a different perception of the risk associated with the presence of immigrants on Italian soil.

The effect of a heightened perception of some risk factors can also explain the concentration of reports in several provinces of Calabria (Crotone) and Sicily (especially Ragusa, to a lesser extent Trapani and Enna) located close to the transit places of migratory flows (Figure 4.3).

Figure 4.3

Reports on financing of terrorism received by province

(number of reports per 100,000 inhabitants; quartiles)



4.2. Types of transactions suspected of financing terrorism

Qualitative analysis of the terrorist financing STRs that the Unit received in 2019 found a similar array of report types to that of the previous years. Apart from the reports submitted for precautionary purposes, two macro-categories can be identified: the first, in which the element triggering the report is subjective (often vitiated by the existence of different people with the same name); and the second, numerically residual, where the trigger has to do with the characteristics of the financial transactions.

Within the first category, many reports are triggered by the explicit involvement of a person in an investigation for terrorism that the reporting entity has learned of owing to a request on the part of the investigative bodies or judicial authorities, from information available on open sources, or consequent to data crossing (usually automatic) with lists of designation issued by official organizations or with databases of names investigated for the offence in question

For the most part, these reports come from money transfer service providers, whose contact with customers is episodic. Often, the suspicion originates with information requests from domestic or foreign investigative bodies. The intermediaries reconstruct the overall transnational network of the transfers, starting from the persons named in the request, and communicate the transactions carried out in Italy to the UIF.

The STRs belonging to the second category come, instead, from reporting entities that establish a continuing relationship with their customers and are therefore in a position to

conduct a more wide-ranging analysis by monitoring the movements on their accounts and changes in their status. The suspicion can arise from the incompatibility of the declared reasons for the inflows or outflows with the customer's economic profile or with the financial movements themselves, particularly if they involve jurisdictions at risk of terrorism.

In these cases, the recurrence of operating models already found in financial analyses or investigations with reference to contexts and economic sectors where there have been episodes of functional or instrumental contiguity with the financing of terrorism can be decisive for the identification of transactions potentially associated with it in the different financial channels.

An important type of report, cutting across the two categories described, concerns non-profit organizations (NPOs) that exhibit anomalous flows in cash with jurisdictions at risk or suspected for various reasons of being close to circles of violent radicalism. In this case, domestic movements, such as fund-raising from believers, can also prove anomalous. News reports significantly influence reporting entities' risk assessment of the transactions of NPOs and therefore their possible decision to send an STR to the Unit. The decline in the frequency or prominence of cases of this kind in the media appears to explain the decrease in these reports in 2019 (Table 4.2).

Table 4.2

Reports on non-profit religious entities (1)

	2015	2016	2017	2018	2019
Number of reports	50	125	81	71	54
Percentage share of the total reports classified as financing of terrorism	16.8	16.8	7.3	6.0	6.5

(1) The number and share include STRs originally filed on grounds of suspicions of money laundering and reclassified after the UIF's analysis as linked to financing of terrorism.

For that matter, the indications reaffirmed in 2019 in various national and international fora[9] continue to highlight the risk that NPOs may, perhaps unknowingly, be used as a cover for the transfer of funds directly or indirectly to terrorist organizations. Certain characteristics of NPOs make them particularly vulnerable to exploitation for illegal purposes. For one thing, their collecting of money can involve a large number of affiliates (crowdfunding) who are motivated by the fulfilment of a religious duty (*zakat*) and not always aware of the final use of the donations. Also, the transmission of funds for charitable purposes is often directed to countries in a humanitarian emergency where jihadist military organizations are in the field. In these circumstances, there is an unavoidable residual risk that the money may be diverted to the latter by accomplices who have infiltrated the decision-making chain on the spot; a risk aggravated by the fact that in such countries there are none of the safeguards

[9] For an analysis of the risks linked to the use of NPOs as a tool for financing terrorism, see the *National Risk Assessment* of July 2019, the European Union's *Supranational Risk Assessment* of June 2019 and the FATF's *TF Risk Assessment Guidance* published in July 2019.

offered by official financial systems, whose place is taken by informal systems such as *hawala.*[10]

4.3. The UIF's analyses

The manner of financial inquiry by the UIF's analysts depends on the type of report and the individual context involved.

In reports submitted for subjective reasons (the first category of STR described above), the set of individual ID data is decisive, as it determines the possibility of obtaining further information that unequivocally refers to the same persons, first of all from the databases available to the UIF and obliged entities. When the transactions take the form of a network, the widening of the operational context needs to be reconciled with the need to make sure that the new links are significant. Consequently, the network is not extended indiscriminately but only in promising directions, identified, for example, on the basis of operating schemes already found in similar contexts or by using network analysis techniques.

Reports regarding mere financial anomalies are more challenging for the financial analyst. In these cases, where analysis is properly preventive, the Unit has sought to grade the operational contexts according to a risk-based approach, identifying economic sectors and milieus more vulnerable to the risk of being exploited for the financing of terrorism. For that matter, even in its anticipatory phase of financing, terrorism is chiefly a social phenomenon that may leave financial traces, not an intrinsically financial phenomenon like money laundering.

In this area, reports concerning payment card transactions grew significantly in 2019 and continued to make an important contribution of information, offering promising leads for investigative follow-up. The existence of a continuing relationship, transaction payment descriptions and, more in general, the frequent intersection of flows transiting on bank cards and accounts (credit transfers, POS payments) enable analysts to supplement the traditional approach of enrichment, typically applied to bank transactions, with the more innovative one of network exploration. The reorganization of the UIF at the start of 2020 represents an institutional response to this opportunity. With a view to extending the techniques of network analysis and pattern recognition, already successfully applied to the money transfer channel, to the payment cards and gaming sectors, it assigns them to a new Division (Special Sectors and Terrorist Financing), which integrates the expertise developed in analysing the financing of terrorism with specific techniques for the financial sectors most vulnerable to exploitation for that objective.

The analyses performed by the Unit also drew on the information acquired in exchanges of personal data with the DNA, which in a good number of cases contributed to the selection of promising contexts for in-depth examination or to the identification of significant persons within the networks. In some 16 per cent of the reports received in the two years 2018-19, at least one match was found with personal data in the records of the DNA.

The majority of the reports analysed by the Unit presented interesting leads that warranted investigative follow-up. Of the nearly 1,500 STRs received in 2018-19 for which the

[10] See UIF *Annual Report for 2018*, pp. 58-59.

feedback from the investigative bodies is known, around 62 per cent obtained a positive response.

With a view to not only increasing the number of financial channels monitored but also expanding the analysis of the socio-economic sectors at risk of terrorist financing, during 2019 the UIF drew on its own analyses of trade-based terrorist financing to contribute to the FATF working group on the wider phenomenon of trade-based money laundering.

Adopting a pattern recognition approach analogous to that used for profiling migrant trafficking and transnational car sales, the study started out from the financial analysis of investigative cases combining money laundering and the financing of terrorism by means of businesses used as cover for the financial flows and eventually identified sets of red flags for each phase of the financing process, as is detailed in the box below.

The analysis of trade-based terrorist financing

The purpose of the analysis was to define risk indicators (red flags) useful for identifying possible cases in which financial flows destined to terrorist organizations are routed through businesses, and to provide operational indications for identifying the most promising lines of analysis, with special attention to cases involving both money laundering and terrorist financing.

In a first phase, taking a bottom-up approach, the analysis selected some investigations of terrorist financing whose findings attested to the trade mechanism in question and for which there were sufficiently detailed suspicious transaction reports. Next, the financial and subjective anomalies were highlighted, particularly those relating to business, classifying them according to the relevant stage in the operational cycle of money laundering (placement, layering, integration) or terrorist financing (collection, transfer, use).

Then, with a top-down approach, two 'ideal types' were elaborated for money laundering and terrorist financing, by seeking to derive the characteristics of the commercial intermediation most functional to the purpose of each of the two phenomena and identifying their distinctive features for each of the above-mentioned stages. One of these features, for example, is the different role of shell companies: these are intrinsic to many money laundering schemes, but they tend to be avoided in the financing of terrorism, since they may raise suspicions about the entire chain of transfers and therefore about the final use of the funds, even in cases where that use would not be found to be anomalous in and of itself.

The examination led to the drafting of a list of distinct risk indicators for each stage of the operational cycle of terrorist financing (fund creation, transfer, use), and a methodological guide for financial analysis.

Downstream, the results in terms of red flags and operational indications were confirmed in the initial investigative cases when they were reread from a bottom-up perspective as generalizations of the financial characteristics detected in the first phase of the analysis.

4.4. Action at international level

The efforts to monitor the risks of terrorist financing have proceeded at global level with the aim of shaping effective strategies to prevent and combat the phenomenon. In 2019, the FATF again updated the Counter-Terrorist Financing Operational Plan that it adopted in 2016 in the framework of the Strategy on Combating Terrorist Financing, developed the same year.

The FATF identifies three priority lines of action: strengthening assessment and understanding of the risk of terrorist financing, improving transposition of the relevant standards into national legislation, and developing effective national systems for preventing and combating the financing of terrorism in the regions most exposed to that risk.

To assist national assessments of the risks of terrorist financing, the FATF has published its *TF Risk Assessment Guidance*, a handbook to which the UIF contributed, setting out good practices addressed especially to the most vulnerable countries. A new report, *Financing of Recruitment for Terrorist Purposes*, examines the ways in which financial support is provided to propaganda initiatives for radicalization and recruitment.

The FATF regularly updates its survey of financing of terrorism typologies (*ISIL, Al-Qaeda and Affiliates Financing*), drawing on the experience of national authorities. Recent developments show that, despite loss of control of the territory, the main sources of financing are basically unchanged, with recourse to kidnapping, extortion and other criminal activities; outside financial support also remains significant, and it is obtained chiefly through *hawala* and money transfer operations. Special attention is paid to reconstruction work in the conflict zones, in order to assess and guard against the risks of infiltration by terrorist components and the diversion of funds meant to be used for rebuilding infrastructures. The survey also underlines the tendency for the local cells established in different countries to be financially independent of the central organization.

The UIF contributes to the projects under way. In particular, an in-depth study has begun on the use of virtual assets for terrorist financing and on the difficulties of intercepting the related illegal flows ('The Criminal Exploitation of Virtual Assets for ML/TF Purposes: Addressing Challenges with Investigations and Confiscation'). The work to combat the financing of terrorism continued in Europe under the Action Plan that the European Commission adopted in 2016. The multiple lines of action set out include strengthening the cooperation between competent authorities (especially the FIUs) and eliminating forms of anonymity in financial transactions. As part of the work of the Egmont Group, the third phase of the ISIL Project[11] now under way focuses on the financing of individuals who act on their own or, at any rate, without the support of a structured organization. The analyses focus on the suspicious transaction reports referring to persons involved in terrorist attacks, whose information content is particularly important for reconstructing terrorist networks and identifying their facilitators.

4.5. International exchanges

As part of the Egmont Group's ISIL Project, which encompasses the study of financial support for foreign fighters, a group of FIUs, including the UIF, are continuing to engage in

[11] See UIF *Annual Report for 2017*, Section 5.4.

a multilateral exchange of information on persons and activities potentially of interest, based on broader indicators than actual elements of suspicion.

In 2019, the UIF received 101 requests and communications from foreign FIUs concerning terrorist financing. In 24 cases, these were cross-border reports sent by a European FIU, while 17 spontaneous communications concerned networks of remittances made by possible facilitators of terrorists, especially through online transactions; a handful of communications from abroad also concerned persons linked to subversive domestic terrorism. The UIF made 28 requests for information concerning terrorist financing, most of them addressed to FIUs in European countries.

In addition to information sharing, cooperation extends to joint in-depth analysis. As part of the EU FIUs Platform, the UIF, together with the Dutch FIU, coordinated a joint study by five European FIUs of transnational remittance networks held to be involved in the financing of terrorism. The project's final results were published by the competent national authorities and the initiative was cited in the *TF Risk Assessment Guidance* as an example of *best practice* in international cooperation whose results can be exploited in the assessment of terrorist financing risk.

5. CONTROLS

5.1. Inspections

The UIF's contribution to preventing and combating money laundering and the financing of terrorism includes on-site inspections of the entities subject to reporting requirements. Inspections are aimed at verifying compliance with the reporting requirements and acquiring data and information on specific transactions or financial phenomena that are deemed to be significant in terms of size and risk.

Inspection planning takes account of the degree of exposure to the risks of money laundering and terrorist financing of the different categories of obliged entity and of the control measures taken by the other authorities responsible for verifying compliance with the AML/CFT provisions. General inspections check the efficacy of active cooperation, in part by analysis of the procedures for reporting suspicious transactions; targeted inspections are directed at reconstructing specific financial movements, supplementing the information acquired in the analysis of STRs or from foreign FIUs, or at examining aspects that have emerged in the framework of cooperation with the judicial authorities, investigative bodies and sectoral supervisory authorities.

Through this direct interaction with the reporting entities, moreover, the UIF also pursues the objective of intensifying active cooperation, enhancing their ability to identify suspicious transactions and improving the quality of their reporting contribution.

In 2019 the UIF conducted 21 inspections, 11 general and 10 targeted; the latter were carried out in connection with specific transactions that were picked up in the course of off-site analysis, in some cases following information exchange with foreign FIUs, or during inquiries into virtual currency services and digital portfolios. One inspection was initiated at the request of the judicial authorities (Table 5.1).

Table 5.1

Inspections

	2015	2016	2017	2018	2019
Total	**24**	**23**	**20**	**20**	**21**
Banks	4	8	4	8	15
Trust companies	3	4	4	3	1
Payment institutions and other financial intermediaries	9	3	3	2	2
Asset mgt. cos. and securities investment firms	2	1	-	4	-
Insurance companies	2	-	6	-	-
Other entities (1)	4	7	3	3	3

(1) Comprises professionals, non-financial operators, gaming service providers and central securities depositories.

In selecting the obliged entities for inspection, the UIF takes account of several signs of possible shortcomings in active cooperation: the absence, small number or poor quality of suspicious transaction reports; problems or significant matters raised by reports from other

obliged entities; anomalies detected by analysis of the aggregated data or identified by econometric models; the existence of detrimental information on the obliged entity or on its customers; and specific information or requests for cooperation from other authorities.

The plan of inspections is drawn up in coordination with the sectoral supervisory authorities and with the Special Foreign Exchange Unit of the Finance Police with a view to enriching the body of knowledge on the obliged entities and avoiding overlapping or duplicate interventions.

Cooperation with the sectoral supervisory authorities also takes the form of joint inspections, to exploit synergies of institutional action and limit the burden on operators. In 14 inspections, the UIF inspection teams were supplemented with personnel from diverse organizational units of the Bank of Italy; in similar fashion, UIF staff took part in four anti-money laundering inspections carried out by the Directorate General for Financial Supervision and Regulation of the Bank of Italy. In one case, the Unit conducted a concurrent inspection with Consob in the exercise of their respective competences under Legislative Decree 231/2007.

Problems detected in the inspections

The inspections carried out by the UIF at banks of significant size found reporting deficiencies in some high-risk sectors. The main areas of weakness were the lack of monitoring of certain operating sectors (for example, transactions based on payment cards or on correspondent accounts), problems in information exchanges between entities belonging to cross-border banking groups, difficulties in capturing highly ramified and complex phenomena and in analysing them for purposes of active cooperation.

In 2019, the Unit proceeded with inspections of branches of EU intermediaries operating in various sectors, such as retail and private banking, documentary credit, the issue of electronic money and the provision of payment services. Weaknesses were found in the arrangements for reporting, which in some cases were not in conformity with national legislation. The assignment of important anti-money laundering functions to group structures, often located abroad, does not always ensure an adequate involvement of the branches' AML officers in the process of reporting suspicious transactions.

In the field of documentary credit, the financial flows and underlying commercial transactions confirm the presence of risks for which the safeguards are deficient, mainly linked to the countries of provenance of the counterparties involved. It was found that intermediaries' conformity assessment of letters of credit reflected a formal approach to the examination of a substantial body of documentation and information, impairing critical evaluation of the transactions observed. The weakness found in their ability to identify suspicious profiles is attributable to a failure to exploit all the information available and the lack of adequate anomaly indicators in internal control procedures.

The inspections of two branches of EU intermediaries, an electronic money institution and a payment institution, active in highly innovative sectors and operationally interconnected, brought out significant shortcomings of compliance with the anti-money laundering obligations. In particular, the provision of so-called white label services,[12] by means of the issue of IBAN numbers by one of the two institutions inspected, enabled a non-EU intermediary to make payment accounts available to Italian and EU customers without the necessary authorizations. The inspections showed that technological innovation has set off a

[12] This allows an intermediary to use under its own brand a payment infrastructure owned by another intermediary. By rebranding the services, the intermediary offering them can present them as if they were its own.

process of progressive segmentation of financial flows in the ever more complex field of payment services. In this context, important factors are both the large number of operators involved in executing money transfers, often working in different jurisdictions, and the online ordering of credit transfers, which does not require the intervention of on-the-spot safeguards. A consequence is the dispersion of information on the customer's profile and transactions among different entities, adversely affecting the clear division of tasks and the efficacy of controls on transactions. The rapid evolution of the market further enlarges the areas of vulnerability to money laundering risks.

Inspections were also carried out on two entities that provide virtual currency exchange services by means of credit transfers, credit cards and, in one case, also via ATMs located in Italy. The targeted inspection at the banks where the exchangers had accounts complemented the analysis of the underlying financial flows. The findings confirmed the risks associated with anomalous uses of virtual currencies for purposes of money laundering and terrorist financing, given the possibility of carrying out substantially anonymous and hard-to-trace transactions, which are de facto impediments to reconstructing the movement of funds. The risks that emerged during the inspections accentuate the need for further regulatory measures for the sector, at a minimum through a more stringent regime of enforcement, which would also give operators greater certainty and avoid possible distortions of competition.

In addition, the Unit conducted an inspection of a trust company entered on the list kept by the Ministry of Economic Development in relation to information on unwarranted tax offsets, including with credits of dubious existence, as part of the escrow agent service offered to customers.[13] The inspection revealed an underestimation of the risks of money laundering associated with this type of service.

At the behest of and in close coordination with the competent sectoral supervisory authority, the UIF also conducted an inspection of an auditing firm. The intervention confirmed that the auditors' contribution to identifying and evaluating potentially suspicious transactions was not always consistent with the considerable body of important accounting, corporate and financial documentation at their disposal. The exploitation of such information assets, which are particularly important for in-depth knowledge of the customer's subjective profile, would enable the members of this category to discharge their reporting obligations more effectively.

Following the inspections conducted during the year, the UIF informed the supervisory and control authorities on the aspects within their respective spheres of competence, and the judiciary authorities on matters of a possibly criminal nature. The parties inspected were informed of the shortcomings found and urged to take the necessary corrective measures. Steps were also taken for the application of sanctions for administrative violations in the matters within their competence.

[13] The parties to an escrow account contract entrust to a third party, the so-called escrow agent (in this case a trust company), as a guarantee, the good or the document that is the object of a transaction and its equivalent value in money. The escrow agent administers the assets on their behalf until, upon the occurrence of a stipulated condition, they are delivered to the contractual parties.

5.2. Sanction procedures

Anti-money laundering legislation envisages a complex system of administrative sanctions designed to punish violations of the obligations it imposes.

The UIF, in inspections and off-site analysis, ascertains and notifies violations of the suspicious transaction reporting and communication obligations established by Legislative Decree 231/2007; depending on the violation found, it transmits to the MEF the findings of violations it has notified to the parties concerned or submits them to the sectoral supervisory authorities for the matters within their respective competence, for the imposition of the sanctions provided for by law.

The sanction measures for which the UIF is responsible have an important enforcement and deterrence function, complementary to that deriving from the overall system of organizational safeguards required by legislation, from the controls performed by the various authorities and from criminal sanctions.

Pursuant to the legislation on gold transfers, the UIF also performs the inquiry for sanction proceedings begun by other authorities and transmits the related acts, accompanied by an explanatory report, to the MEF (see Section 6.3, 'Gold declarations').

The complex organization of sanctioning powers introduced by Legislative Decree 90/2017, substantially unaltered even after the entry into force of Legislative Decree 125/2019, has made it necessary to strengthen coordination and liaison with the sectoral supervisory authorities, particularly as regards violations in reporting suspicious transactions.

Accordingly, information exchanges have been intensified for the joint examination of possible violations of anti-money laundering legislation.

There are now well-established practices between the UIF and the Bank of Italy's Directorate General for Financial Supervision and Regulation for reciprocal participation in their respective collegial bodies responsible for assessing irregularities. On the basis of the inspection reports that the Unit transmitted in 2019, the Directorate General instituted sanction procedures for two cases of violations of the provisions of Legislative Decree 231/2007.

Cooperation with Consob proceeded, with information exchanges on possible failures to report suspicious transactions that were found during inspections and possible cases of market abuse.

In 2019 the UIF initiated 18 administrative sanction procedures for failure to report suspicious transactions, ascertained by inspections (Table 5.2); in one case, violations of the SARA aggregated data transmission obligations were notified. The findings of violations notified to the parties concerned were transmitted to the MEF for the possible levying of the sanction.

Table 5.2

Administrative irregularities

	2015	2016	2017	2018	2019
Failure to report a suspicious transaction	32	17	17	8	18
Failure to transmit aggregated data	-	1	-	1	1
Failure to declare a gold transaction	7	5	5	26	28
Failure to freeze funds and economic resources	10	8	5	-	-

The year saw an increase in the number of sanction procedures initiated by the UIF together with a significant rise in the total amount of the suspicious transactions that were found not to have been reported (€60.2 million, compared with €2.3 million in 2018).

Sanction proceedings on gold transfers

In 2019 the Unit sent the MEF documentation on 28 sanction proceedings concerning gold transfers. Of these cases, 21 referred to transactions relating to investment gold carried out by natural persons with a single German company active in several areas of Italy and brought to the UIF's attention by the Finance Police. The MEF agreed with the UIF's reading of these cases, according to which transactions of this kind, irrespective of the delivery of the gold to the purchaser, must be regarded as non-financial transactions subject to the declaration requirement under Law 7/2000, and imposed the consequent pecuniary administrative sanctions.

6. STRATEGIC ANALYSIS

International standards put strategic analysis among the official duties of the FIUs together with operational analysis. In line with those standards and with national legislation, the Unit is engaged in the identification and assessment of phenomena and trends, as well as of the weaknesses of the system.

Strategic analysis draws on the information and indications obtained from suspicious transaction reports, from analysis of aggregate reports (SARA), from operational activity, from collaboration with national and international authorities and from inspection reports. These sources are supplemented, where necessary, by additional data and information specifically requested from intermediaries.

The information is processed and combined in order to help guide the UIF's action, the planning of activities and the selection of priority objectives. Strategic analysis also uses quantitative methods, such as econometric techniques and data mining tools, to identify trends and anomalies on a statistical basis.

The purposes of strategic analysis include the assessment of the risk of involvement in money laundering and terrorist financing as it pertains to the economic and financial system as a whole or to specific geographical areas, means of payment and economic sectors, as well as the identification of situations and contexts for possible targeted examination.

6.1. Aggregated data

SARA reports are submitted monthly by financial intermediaries and derive from the aggregation of data on their transactions in accordance with criteria laid down by a UIF Measure. They cover all transactions carried out by customers for amounts (in a lump sum or split up) of €15,000 or more.

The data are anonymous and cover the full range of payment instruments and financial transactions. The aggregation criteria for SARA data mainly concern the means of payment used, the location of the reporting branch, the customer's sector of economic activity and residence, and the location of the counterparty and its intermediary (in the case of credit transfers). The data refer to both incoming and outgoing transactions, with the amount of cash transactions, if any, shown separately.

SARA data

There was an increase in the flows of SARA data received by the UIF in 2019 (Table 6.1), attributable to the phasing in of the amendments to Legislative Decree 90/2017 regarding simplified due diligence. Especially after the new supervisory Instructions on the matter were issued, some reporting entities began to include in their reports transactions with categories of customers, in particular financial intermediaries, that under the previous rules had been rated as low risk and therefore not within the compass of SARA reports. Among the entities that took this course of action were some banks of significant size. As a consequence, the total transaction amount reported more than doubled, rising from €30 trillion in 2018 to €62.2 trillion, while the number of records sent rose by 5.8 per cent to 108.8 million and that of the underlying transactions by 8 per cent to 359.5 million.

Following the recently issued Bank of Italy rules on record-keeping, the UIF is drafting a new Measure concerning the transmission of aggregate AML reports that will contain provisions for uniform treatment of the data on transactions put through by domestic and EU financial intermediaries.

The number of reporting entities decreased further by 2.1 per cent during the year, mainly owing to bank mergers. Banks continue to account for the preponderant share of the data sent (94.9 per cent measured by the number of records and 98.4 per cent by amount).

After banks, trust companies set up under Article 106 of the Consolidated Law on Banking were the category with the largest increase in reported transaction amount (+€27 billion), reflecting the high transaction volumes of some intermediaries active in securitization, factoring and leasing.

Table 6.1

Aggregate anti-money laundering reports (SARA reports)

TYPE OF INTERMEDIARY	**Number of reporting entities in the year**	**Number of records** (1)	**Total amount** (*billions of euros*)	**Number of underlying transactions**
Banks, Poste Italiane and CDP	520	103,290,212	61,277	328,421,287
Trust companies under Law 1966/1939	206	37,316	15	114,749
Asset management companies	207	1,434,734	230	6,499,042
Financial intermediaries under Article 106 of the TUB	209	1,467,987	341	5,025,254
Investment firms	131	177,140	97	3,372,448
Insurance companies	74	1,387,734	140	2,650,991
Payment institutions	59	739,751	40	11,832,164
Electronic money institutions	10	159,560	18	1,082,512
Trusts under Article 106 of the TUB	37	117,855	90	471,912
Total	**1,453**	**108,812,289**	**62,248**	**359,470,359**

(1) SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 6 March 2020.

Within the SARA database, cash transactions provide some of the most significant information from the point of view of preventing money laundering. The reports show, in addition to the amount of cash withdrawals and deposits on current accounts, the amount settled in cash in other types of transactions (such as securities trading and issues of certificates of deposit).

Cash transactions

In 2019 the total value of cash transactions continued the downward trend of recent years, decreasing by 2 per cent to about €200 billion. The decline involved deposits alone, which fell from €192 billion to €188 billion, while withdrawals held steady at €12 billion.

Cash withdrawals and deposits are distributed asymmetrically because of their respective characteristics: ordinarily, withdrawals are more fragmented and thus remain below the reporting threshold.

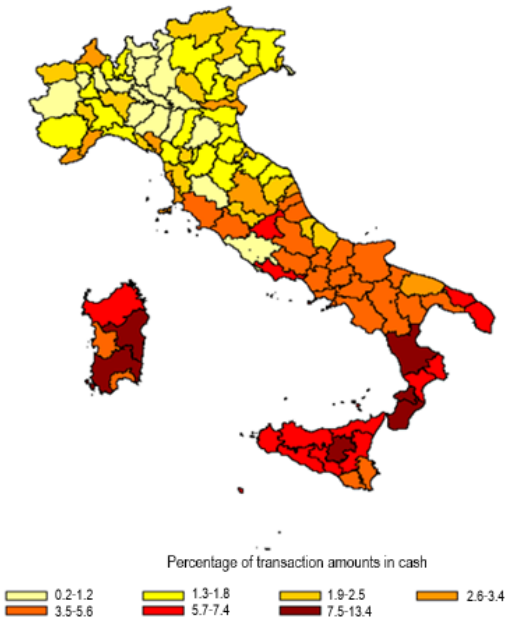
Anomalies in the use of cash

There are pronounced geographical differences in the intensity of the utilization of cash (Figure 6.1a). This may be due to differences in structural variables such as earning capacity, in spending habits and in local availability of financial services. In order to identify potentially anomalous cash transactions, for some time now the Unit has employed a statistical approach that it has developed: an econometric model based on the structural determinants of the use of cash is estimated; the unexplained share of cash transactions can then be considered potentially anomalous and symptomatic of illegal activities.[14] The geographical distribution of the incidence of such anomalies portrays the risk associated with the use of cash (Figure 6.1b).

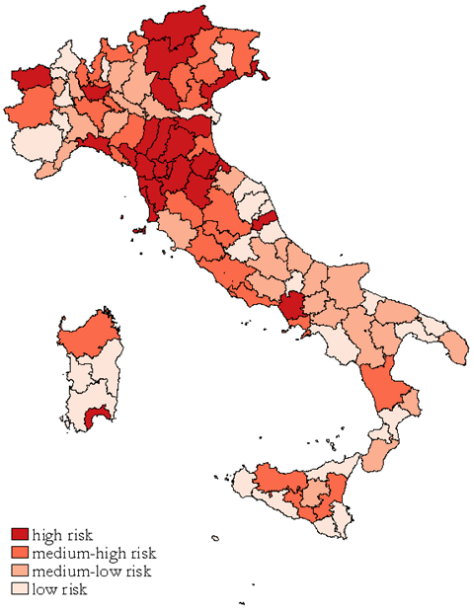
Figure 6.1

Use of cash and anomalies by province
2019

a) Use of cash (1) (2)



b) Anomalies in the use of cash (3)



(1) Share of cash transactions in total transactions. – (2) For uniformity with the preceding years, the SARA data used do not include the transactions of general government or of financial and banking intermediaries resident in Italy, in the European Union or in countries considered equivalent by the MEF Ministerial Decree of 10 April 2015. The SARA data are subject to correction by the reporting agents; the data used in this chapter are updated to 6 March 2020. – (3) Preliminary results. The variable of analysis (use of cash) is updated to 2019, some explanatory variables only to 2018 or 2017 (the last two years available as of March 2020). The shadow economy, at municipality level, is measured as a share of the underdeclaration of value added estimated by Istat.

[14] See the box 'Anomalous use of cash' in UIF *Annual Report for 2018*, p.73.

A comparison of the distribution of the incidence of the use of cash by province (Figure 6.1a) and the distribution of the share not consistent with economic and financial fundamentals (Figure 6.1b) reveals profound differences: recourse to cash increases gradually moving from North to South, while the anomalies are concentrated to a greater extent in the regions of the Centre and North, whose more dynamic economies attract illicit as well as lawful investments.

Credit transfers are another payment instrument recorded in the SARA data that are of particular importance in the effort to counter financial crime. The information content of credit transfer reports is ample and includes details of the residence (municipality or foreign country) of the counterparty and the intermediary. This wealth of information makes it possible to produce statistics and correlations based on the geographical provenance and destination of the funds.

Of particular interest are those cases in which the foreign intermediary involved in the transfer is located in a tax haven or a non-cooperative country: the transfer of funds to these jurisdictions may be for reasons that are not strictly economic, but, rather, relate to the opacity of their fiscal and financial systems.

Cross-border credit transfers

The total value of credit transfers to and from foreign countries grew by 3.7 per cent to €2,823 billion in 2019. The increase was due mainly to incoming transfers, which grew by 5.2 per cent, from €1,396 billion to €1,469 billion, while outgoing transfers increased by 2.2 per cent, from €1,325 billion to €1,354 billion (Table 6.2).

Table 6.2

Cross-border credit transfers by country of destination and origin (1)

Outgoing	Amount (*billions of euros*)	Incoming	Amount (*billions of euros*)
Total	**1,354**	**Total**	**1,469**
to EU countries	**1,089**	**from EU countries**	**1,169**
United Kingdom	293	United Kingdom	316
Germany	250	Germany	264
France	226	France	250
Belgium	81	Belgium	86
to non-EU countries	**265**	**from non-EU countries**	**300**
United States	93	United States	101
Turkey	21	Turkey	23
China	18	Russia	11
Russia	6	China	10
of which: tax havens	**85**	***of which: tax havens***	**94**
Switzerland	40	Switzerland	44
Serbia	18	Serbia	18
Hong Kong	10	Hong Kong	8
Singapore	4	Abu Dhabi	5

(1) See Figure 6.1, note 2.

The distribution of credit transfers by counterparty country reflects that of Italy's foreign trade, with an attendant concentration of flows involving Italy's main trading partners, especially the other members of the European Union: the flows to and from EU countries grew by 11 per cent on an annual basis. As for the main non-EU countries, the volume of flows with the United States and Turkey shrank sharply by respectively 27.1 and 55.1 per cent; Russia replaced Japan among the top four non-EU countries by volume of credit transfers with Italy.

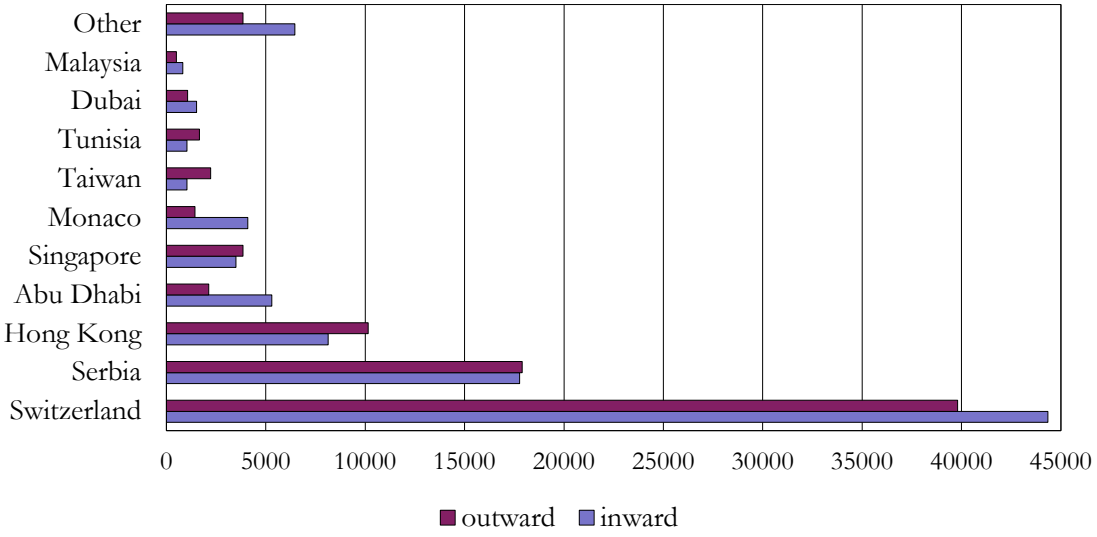
Flows with tax havens

The reference lists of tax havens and non-cooperative jurisdictions underwent further changes in 2019.[15] Overall, inflows and outflows in respect of such countries grew by respectively 9.3 and 4.9 per cent. The largest increments in absolute terms concerned Serbia and Switzerland. Compared with 2018, Malaysia replaced Iran among the top ten counterparty countries (Figure 6.2).

Figure 6.2

Credit transfers with tax havens or non-cooperative jurisdictions

(millions of euros)



(1) See Figure 6.1, note 2.

Anomalies in financial flows

Unlike the use of cash, the geographical distribution within Italy of the financial flows with non-cooperative jurisdictions or tax havens does not show the traditional North-South dualism. Instead, provinces with a high incidence of such flows are found both in the South and in the Centre and North, with a slight prevalence of the provinces of the Centre as regards inward credit transfers (Figure 6.3a)

[15] The list of non-cooperative countries and/or tax havens is taken from the ministerial decrees implementing the Consolidated Law on Income Tax (TUIR) in force at 31 August 2019, the list of high-risk and non-cooperative jurisdictions published by the FATF in February 2019, and the EU list of tax havens (update of 14 June 2019), in accordance with the publication of the statistics for 2019 in the UIF's *Quaderni dell'Antiriciclaggio*, *Dati statistici*. Compared with 2018, Pakistan, Botswana, Ghana, Cambodia, American Samoa, Guam, Fiji and the United States Virgin Islands were added, while Afghanistan, Iraq, Uganda, Laos, and Bosnia and Herzegovina were removed.

Applying a statistical methodology to the study of such transactions, it is possible to estimate, with an econometric model, the component of the flows with these jurisdictions that is explained by economic and financial fundamentals (in this case, those of the Italian provinces and of the foreign countries involved). The difference between the credit transfers observed and the value explained by structural factors is used as an anomaly indicator. [16]

As with cash, the money laundering risk profile associated with cross-border financial flows that emerges from this statistical approach deviates from the picture deriving from the simple analysis of observed flows (Figure 6.3b). The geographical distribution of the anomalies in outward transfers is not particularly uneven, with a high incidence in the North but also in provinces of the Centre and South not distinguished by a high level of observed flows, e.g. those of the regions of Lazio, Abruzzo, Campania and Calabria). As in the past, the anomalous inflows from abroad appear to be concentrated in the southern provinces. There is again a high incidence of anomalies in both inward and outward credit transfers in the provinces bordering on non-cooperative countries and/or tax havens.

[16] See UIF *Annual Report for 2017*, pp. 85-86.

Figure 6.3

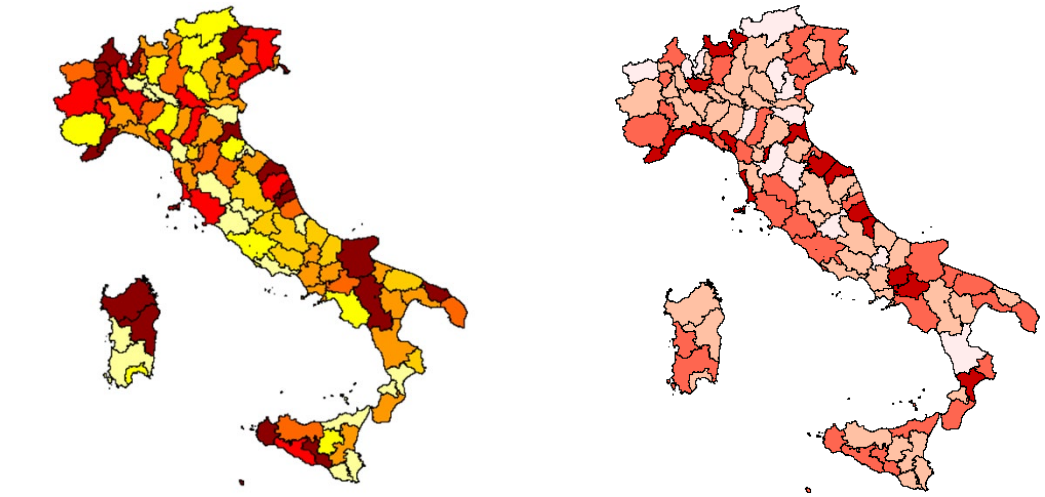
Credit transfers at risk

a) Credit transfers with non-cooperative jurisdictions or tax havens as a % of total cross-border credit transfers (1)

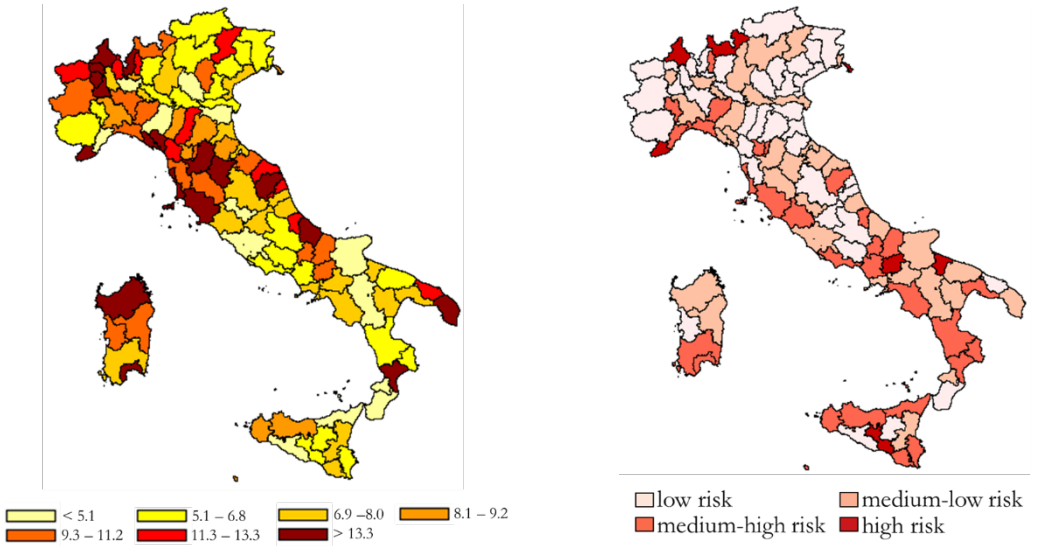
b) Anomalies in foreign credit transfers (2)

2019 **2018**

Outward credit transfers



Inward credit transfers



(1) See Figure 6.1, note 2. – (2) The maps refer to 2018, the latest month for which all the data needed to estimate the model are available.

6.2. Analysis of aggregated data and research activity

Good data quality is essential to reliable analyses and studies of financial flows. In order to identify potential reporting errors, aggregated data undergo automatic statistical checks based on quantitative methods as soon as they are received by the UIF. This control activity is instrumental in identifying not only possible errors in the data, but also possible anomalous flows requiring examination by the reporting entity. There are two types of checks: systemic checks, which compare the data of each reporting entity with those of the entire system for the same month, and non-systemic checks, which compare the conduct of individual financial intermediaries with their own reporting patterns over the previous 12 months.

Data identified as anomalous by the control algorithms are sent to the intermediaries, who verify their accuracy and correct any reporting errors.

The UIF is continuing to develop econometrics-based inquiry into phenomena and financial conduct of interest, with the twofold aim of increasing knowledge of specific phenomena and providing operational guidelines for preventing and combating money laundering. The results of these studies are used internally to identify sectors and geographical areas at risk and cases deserving closer scrutiny. The findings are also shared with other AML authorities according to their respective functions, including as part of the preparatory work for the National Risk Assessment. The methodology and the general findings are published in the 'Analisi e studi' series of *Quaderni Antiriciclaggio*.

Monitoring data quality

For years now, a system of statistical checks has been used to ensure the quality of SARA data and at the same time to identify possible anomalies not detected by intermediaries. In 2019 the system flagged more than 24,000 potentially anomalous aggregated data, against 25,000 the previous year. Consequently, 796 reporting entities (of which 477 banks) were asked to check the data they had sent. In 5.1 per cent of the cases questioned, the reporting entities found errors in the data transmitted. In 1.2 per cent (293 cases), the data checked were found to be related to STRs already sent to the UIF. In 0.8 per cent (194 cases), the reporting entities were prompted to review the underlying transactions with a view to submitting a suspicious transaction report.

The large number of reporting entities and the volume of data received necessitate constant administrative and technical support on the part of the UIF in order to ensure data quality. The Unit received some 1,600 requests for assistance in 2019. This was more than in 2018, partly because the legislative changes introduced during the year, while not affecting the SARA data aggregation procedures, raised some doubts among the obliged entities. [17]

In 2019 the Unit reaped important operational results deriving from the studies completed in previous years.

Businesses infiltrated by organized crime

The Unit's study of the financial accounts of firms infilrated by organized crime was applied concretely.[18] The results of the study enabled the UIF to define a set of financial

[17] The reference is to the amendments made by Legislative Decree 90/2017 to Legislative Decree 231/2007 concerning due-diligence and record-keeping obligations with regard to transactions in which the counterparty is a financial intermediary (see the preceding section, 'Aggregated data').

[18] See UIF *Annual Report for 2018*, p. 75.

statement indicators that distinguish the corporate management model of infiltrated firms. On the basis of these indicators, supplemented with others suggested in the specialized literature and taking account of some structural characteristics (province, size and sector of activity), a statistical similarity measure was calculated with which to identify the healthy companies most similar to the infilated firms.

Some statistical validations of this matching were performed using data from the Chamber of Commerce archive and the STR database. The preliminary results are especially encouraging as regards the ability of this approach to identify firms potentially controlled by organized crime.

Feedback from investigative bodies

The UIF has received valuable feedback from investigative bodies concerning its monitoring of the SARA data flows during the year and in previous years. The findings shared show that the most anomalous positions identified through the screening of flows with the countries of Eastern Europe, the Arab world and North Africa[19] were the object of subsequent investigation. The Unit's analysis of anomalous cash withdrawals with foreign credit cards at ATMs in Italy also had an investigative follow-up.[20]

Risk indicators for non-bank intermediaries

The UIF continued its work together with the Bank of Italy's supervisory directorates to develop composite money laundering risk indicators for non-bank financial intermediaries.[21] The indicators, which have already been prepared for banks,[22] are to be used in planning off-site AML controls and on-site inspections for these intermediaries as well, thereby increasing the number of obliged entities for which systematic evaluation of money laundering risk based on objective data will be possible. This will enhance the efficacy and efficiency of controls, which according to the latest international standards and national legislation must adopt a risk-based approach in planning control activities.

The indicators calculated for this group of operators are based on 'fuzzy logic', an approach taken from artificial intelligence, that can produce robust results even with limited data availability and translate qualitative assessments into quantitative indicators. As in the case of the banks, the new indicators are obtained from statistical elaboration of data from SARA reports, STRs and banks' automated prudential returns and are used to formulate an initial quantitative assessment of the risk exposure of each intermediary. In the subsequent phase of qualitative analysis, an evaluation is made of the adequacy of the risk-mitigation safeguards put in place by the intermediaries in observance of the rules established by legislation.

Credit transfers from abroad

As part of its research activity, the Unit developed a new model for the analysis of credit transfers coming from abroad. The methodology used makes it possible to obtain anomaly indicators at the level of the Italian municipality, the receiving bank and the foreign country of provenance. More precisely, the overall volume of inward credit transfers is compared with that which would be expected based on the economic, financial and demographic fundamentals. The selection of potentially anomalous cases for possible

---

[19] See UIF *Annual Report for 2016*, p. 84; UIF *Annual Report for 2017*, p. 87.

[20] See UIF *Annual Report for 2015*, p. 74; UIF *Annual Report for 2017*, p. 86.

[21] Investment firms, asset management companies, electronic money institutions, payment institutions and entities entered in the single register of financial intermediaries under Article 106 of the Consolidated Law on Banking. See also UIF *Annual Report for 2018*, p. 75.

[22] See UIF *Annual Report for 2016*, pp. 83-84.

further examination is performed by a statistical technique used in the literature to identify outliers on the basis of the distribution of a set of correlated factors.[23] Besides identifying specific anomalies in credit transfers coming from abroad, the methodology, by appropriately aggregating the elementary anomalies by destination municipality or bank, can generate more highly detailed quantitative money laundering risk indicators than the previous model. As in the past, aggregating the anomalies by country of provenance makes it possible to obtain a classification of countries at risk of money laundering based on 'objective criteria,' which could flank the evaluation based on the degree of compliance with international rules and standards. The preliminary results of the study show that the aggregate anomaly indicators based on the model are generally consistent with the indices of crime for the Italian provinces and the indices of money laundering risk for the foreign countries commonly included in comparable studies.

Screening of anomalous financial flows

The monitoring of financial flows with counterparties abroad proceeded. This massive analysis of the SARA data brought to light some anomalous flows relating to two countries of Eastern Europe that warranted operational examination. Data were requested from the intermediaries concerned and then crossed with the other databases available to the Unit (STR archives, commercial databanks, information provided by some foreign FIUs). The findings with regard to the most interesting positions were communicated directly to the investigative bodies for follow-up action according to their competence.

The anonymous STR database

The project to create an anonymous database containing most of the information regarding suspicious transaction reports was completed during the year. The project answers the need to access and process some contents of that database for purposes of strategic AML analysis (for example, statistical and econometric studies). The greater ease with which it will be possible to perform massive quantitative analysis on the STR data while still ensuring high standards of data security and confidentiality can enhance the efficacy of the UIF's institutional action through the development of advanced techniques applicable to operational analysis.

Other activities

Again in 2019, the UIF was an active participant in the national and international scholarly debate on topics concerning the economy, legality and law enforcement, collaborating with other financial and academic institutions, presenting the results of its analyses and research at major conferences, and publishing working papers and articles in international journals.

A UIF staff member had a three-month fellowship at the Financial Stability Institute and Bank for International Settlements, which concluded in June 2019. The collaboration produced a study that reviews the use by some anti-money laundering authorities of advanced data collection or advanced data analytics tools (so-called SupTech). [24]

SupTech applications for anti-money laundering

'SupTtech applications for anti-money laundering', a study of the advanced data collection and analytics tools used by the competent financial authorities for purposes of anti-money laundering supervision and financial intelligence, is the fruit of the collaboration between the Financial Stability Institute of the Bank for International Settlements and the UIF.

[23] More specifically, quantile regression techniques are used. See R. Koenker, 'Quantile regression', Econometric Society monographs no. 38, Cambridge University Press, 2005.

[24] R. Coelho, M. De Simoni and J. Prenio, *'SupTech applications for anti-money laundering'*, UIF, *Quaderni dell'antiriciclaggio*, *Analisi e studi*, no. 14 (2019).

The use of such techniques is already well advanced, given that these authorities need sophisticated tools to analyse the massive and heterogeneous body of data to which they have access (e.g. suspicious transaction reports, threshold-based communications, data provided by other governmental agencies, open sources). Such techniques increase their ability to detect networks of transactions, identify anomalous behaviours and, in general, transform enormous quantities of structured and unstructured data into useful information for operational purposes.

One of the chief motivations for adopting SupTech applications is the efficiency gain obtained through process automation. Less immediate, instead, is the assessment of their effectiveness for the identification of actual cases of money laundering, which can prove lengthy and laborious. To maintain the automatic learning capacity of SupTech systems (where they are based, for example, on machine learning), it is necessary to update the 'training data' regularly, given the speed with which criminal organizations alter their behaviour in order to avoid detection.

The main problems concern the computational capacity required and data confidentiality constraints, the latter particularly important if the development phase uses human resources external to the competent authorities. International cooperation in this field, which could help overcome many of the problems, is still embryonic. (In this regard, the FATF recently began discussing SupTech issues in the newly established Supervisors' Forum.)

The workshop organized in collaboration with Bocconi University on quantitative methods and the fight against economic crime reached its fourth edition.

Fourth UIF-Bocconi Workshop on quantitative methods and fighting economic crime

The fourth 'Quantitative Methods and Fighting Organized Crime' Workshop, organized by the UIF in collaboration with Bocconi University's Baffi-Carefin Center on International Markets, Money and Regulation, was held in Milan in March 2019.

The Workshop has become an important meeting-ground for research institutes, the banking sector and the authorities engaged in preventing and combating money laundering and economic crime. Sharing the results of the latest studies opens the way to exploring potential synergies to advance scientific knowledge and the capacity to counter criminal phenomena.

The first two works presented by the UIF, in part the result of collaboration with the Special Operations Group of the Carabinieri, concerned the effects of infiltration by organized crime on Italian firms' financial statements and the detection of anomalies in the use of cash at the level of individual banks and municipalities. A third presentation concerned the proposal for a new methodology for identifying anomalies in credit transfers to and from Italy (see the preceding section, 'Aggregated data').

Bocconi University researchers presented two studies: the first on the relations between anti-mafia certification and public subsides, the second on the possible links between public procurement procedures and corruption. Representatives of two of Italy's biggest banks discussed recent experiences in AML monitoring of financial transactions correlated with the use of virtual currencies and in the use of statistical and predictive models to identify suspicious transactions.

The study that the Unit carried out on the anomalies in credit transfers from abroad (see above) was also presented at the annual conference of the Italian Society of Law and Economics and at the fifth Banking Research Network Workshop organized by the Bank of Italy's Directorate General for Economics, Statistics and Research. In February, an overview of the UIF's activity of strategic analysis was presented at the periodic meeting of the FATF's Forum of FIU heads.

Publications

The Unit's research papers continue to be published in the 'Analisi e Studi' series of Quaderni dell'antiriciclaggio. A first paper examines the impact of AML inspections on banks' suspicious transaction reporting;[25] a second one, updating a previous work, develops an econometric model for detecting anomalies in transactions carried out in cash at banks.[26]

During the year, some of the Unit's research papers also appeared in outside publications. A working paper on trade-based money laundering that had already appeared in the Unit's '*Analisi e studi*' series was published in an international scholarly review.[27] A theoretical and empirical study of the determinants and characteristics of the FIUs' organizational structure was published in Bocconi University's Working Paper series.[28]

6.3. Gold declarations

The law governing the gold market in Italy provides that transactions involving investment gold or gold material for mainly industrial uses (other than jewellery) must be declared to the UIF. This requirement applies to gold sales and to physical transfers of gold out of or into Italy for amounts of €12,500 or more.[29]

Under the legislative provisions, the competent authorities may have access to the contents of gold declarations not only for AML purposes but also to combat tax evasion and for reasons of public order and public safety.

There are two types of declaration: ex-post declarations, made on a monthly basis for all the transactions carried out during the month; and advance declarations, required prior to a physical transfer of gold out of the country.

The number of gold transaction declarations rose sharply in 2019 (by 14.9 per cent to more than 40,000) and the amount declared grew even more markedly (by 30.9 per cent to nearly €19 billion). The increase was driven by the rise in the price of gold in the second half of the year. Gold sales again accounted for the lion's share (93.6 per cent) of the total amount (Table 6.3).

Table 6.3

[25] M. Gara, F. Manaresi., D.J. Marchetti and M. Marinucci, *'The impact of anti-money laundering oversight on banks' suspicious transaction reporting: evidence from Italy'*, UIF, *Quaderni dell'antiriciclaggio*, *Analisi e studi*, no. 12, 2019.

[26] M. Giammatteo, *'Cash use and money laundering: An application to Italian data at bank-municipality level'* UIF, *Quaderni dell'antiriciclaggio*, *Analisi e studi*, no. 13, 2019.

[27] M. Gara, M. Giammatteo and E. Tosti, *'Magic mirror in my hand … How trade mirror statistics can help us detect illegal financial flows'*, *The World Economy*, 42 (11), pp. 3120-3147, 2019.

[28] D. Bartolozzi, M. Gara, D.J. Marchetti and D Masciandaro, *'Designing the anti-money laundering supervisor: theory, institutions and empirics'*. Bocconi Working Paper no. 126, 2019

[29] Law 7/2000 and subsequent amendments.

Ex-post monthly declarations of gold transactions

TYPE OF TRANSACTION	**Number of declarations**	**Number of transactions**	**Declared value** *(millions of euros)*
Sales	38,542	101,807	17,706
Gold loan (concession)	1,304	2,582	751
Gold loan (restitution)	356	477	56
Other non-financial transactions	59	62	44
Personal imports of gold	128	163	240
Delivery services for investments in gold	439	441	122
Total	**40,828**	**105,532**	**18,919**

Physical transfers of gold grew by 32.6 per cent in value. Declarations (both advance and ex-post) submitted by non-residents were an important factor: compared with 2018, the number more than doubled, from 11 to 27, while the amount declared grew from €9.5 million to €15 million.

Categories of declarants

The number of entities registered with the system increased again in 2019, owing in particular to the addition of 19 professional dealers and 18 natural persons. Nevertheless, the number of reporting entities that were active during the year remained about the same (Table 6.4). The relative shares of gold traded by the different categories also remained unchanged, with professional gold dealers largely preponderant (82.6 per cent).

Table 6.4

Reporting entities engaged in gold transactions

TYPE OF REPORTING ENTITY	**Number of reporting entities registered**	**Number of reporting entities active in the year**	**Number of declarations**
Banks	81	31	6,855
Professional gold dealers	442	343	34,700
Other, natural persons	125	17	55
Other, legal persons	87	25	396
Total	**735**	**416**	**42,006**

Reversing the trend of the preceding years, the volume of industrial gold transactions almost matched that of investment gold transactions (44.3 against 46 per cent; for the remaining 9.7 per cent, the transaction purposes cannot be established with certainty). This was due in part to transactions in industrial gold with Latin America and Africa on the part of a number of operators.

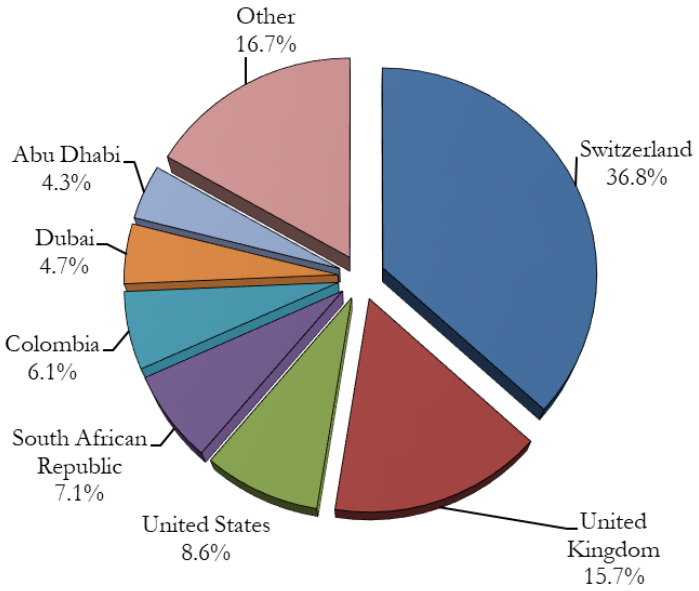
Counterparties

Geographically, the Italian counterparties are concentrated in the traditional goldsmiths' districts of Arezzo, Vicenza and Alessandria, which maintained a market share of about 60 per cent.

Gold transactions with foreign countries, which surged by 68.9 per cent compared with 2018, are even more highly concentrated: 74.3 per cent of the imports come from the first five countries (Switzerland, the United Kingdom, the United States, South Africa and Colombia). However, there were significant changes in the composition of foreign counterparties: Switzerland consolidated its lead, its share increasing from 29.8 to 36.9 per cent; among the first five counterparty countries, Colombia supplanted Dubai, whose share continues to contract (it was 15.4 per cent in 2017, compared with 4.7 per cent currently).

Figure 6.4

Transactions in gold with foreign counterparties



Statistics on advance gold declarations

The increase in advance declarations (Table 6.5) appears to reflect the generalized expansion of cross-border transactions discussed above. The significant growth in physical transfers of gold out of the country is being examined by the competent authorities as well.

Table 6.5

Advance declarations (transfers of gold abroad) (1)

TYPE OF TRANSACTION	**Number of declarations/ transactions**	**Declared value** *(millions of euros)*
Sales	1,013	1,990
No transaction (mere transfer)	162	258
Other non-financial transactions	2	0.4
Gold loan (restitution)	1	0.0(2)
Total	**1,178**	**2,249**

(1) Advance declarations are incorporated in ex-post declarations where the transfer underlies a commercial or financial transaction. - (2) The total amount declared was €40,000 in 2019.

Analyses of the ORO databank

Maintaining its proactive approach to managing the system for collecting gold declarations, the UIF continued to analyse the data so acquired with a view to identifying anomalous

operating practices and devising anomaly indicators.[30] Based on its findings, the Unit began a dialogue with some reporting entities in order to get a more precise picture of the transactions described in the declarations submitted.

In addition, in response to the communications concerning the analyses that the Unit carried out on specific anomalous transactions, the investigative bodies provided an important information feedback, from which one can infer the importance of the information the Unit had transmitted. More in particular, the Unit found that the transactions it had identified were under investigation for administrative or tax irregularities.

[30] See UIF *Annual Report for 2018*, pp. 78-79.

7. COOPERATION WITH OTHER AUTHORITIES

7.1. Cooperation with the judicial authorities

International and European principles and rules pursue the broadest possible cooperation between FIUs and the authorities responsible for preventing and combating money laundering and the financing of terrorism, having regard to their respective institutional powers and the principle of reciprocity in information exchanges. National legislation lays down as the key principle of the system coordination between prevention and enforcement, calling for various forms of cooperation and information exchange between the UIF, the investigative bodies and the judiciary, in compliance with the limits and the separation of roles provided for by law. Within this framework, the UIF has adopted ever more efficient and advanced forms of interaction and channels of information exchange.

Beyond fulfilling its reporting obligations pursuant to Article 331 of the Code of Criminal Procedure as regards offences that come to its attention in the performance of its duties, the UIF also provides, at the request of investigating magistrates, information in its possession for use in investigations related to money laundering, self-laundering, predicate crimes and the financing of terrorism. There are specific forms of cooperation between the Unit and the National Anti-Mafia and Anti-Terrorism Directorate (DNA).

In turn, the judiciary and the investigative bodies forward information to the UIF. The DNA makes regular reports to the Unit on the usefulness of the information received.

These information exchanges help the Unit to perform its functions more effectively, thanks to expanded knowledge of criminal patterns and practices, and to make a greater contribution to preventing and combating crime.

Information exchanges with the judicial authorities and investigative bodies increased sharply in 2019 by comparison with years past. The UIF received 395 requests from the judiciary and sent back 779 responses, including follow-up transmissions of further information regarding the same proceeding (Table 7.1).

Table 7.1

Cooperation with the judicial authorities

	2015	2016	2017	2018	2019
Information requests from the judicial authorities	259	241	226	265	**395**
Responses	432	473	429	488	**779**

Requests from the judicial authorities to the Unit are generally made to acquire STRs and the related financial analyses as well as information received from foreign FIUs. Last year the Unit also received the first requests from the judicial authorities for acquisition of the data transmitted to it with the threshold-based communications concerning persons under investigation.

With increasing frequency, judicial and investigative bodies avail themselves of the UIF's assistance in investigations on cross-border criminal activity, requiring the activation of foreign FIUs. A number of requests are for the purpose of in-depth financial analysis in relation to investigations under way.

International cooperation on behalf of the judicial authorities mainly involved the FIUs of the United Kingdom, Romania, Switzerland, Germany, Malta, Bulgaria and Spain. There were also significant exchanges of information with the FIUs of France, Poland and Luxembourg. The international channel allowed the acquisition, for investigative purposes, of information on the financial movements of the persons under investigation, the holders of foreign accounts used to channel the proceeds of illegal activities, and the subjective profile of the persons connected with the investigations, including any criminal proceedings against them in the foreign state involved.

The results of cooperation depend on the availability of all the elements required to initiate in-depth inquiries with the foreign FIUs, such as a description of the criminal context under investigation, indication of the alleged predicate offence, the elements linking the case to the foreign country involved (for instance, the persons or foreign accounts about which in-depth inquiries are requested).

Information from foreign FIUs is transmitted to the judicial authorities with the prior consent of the counterparts concerned and with special precautions to safeguard confidentiality and comply with the restrictions governing the use of the information.

For the most part, the requests for cooperation were made in the framework of investigations of organized crime, in some cases of foreign origin, of fraudulent transfers of values, fraud (in some cases online or via falsification or alteration of SWIFT messages), unauthorized financial activities, illegal online gaming, drug trafficking, tax offences and bankruptcy crimes.

Frequently the Unit was asked to cooperate in investigations on unauthorized financial intermediation by persons suspected of using web platforms for activities such as the provision of investment services or activities involving financial instruments, without the necessary authorization. There were also a good number of requests involving financial cyberfraud, such as the 'man in the middle' scam.[31]

The year registered the further effects of the decriminalization in 2016 of some offences formerly envisaged by the AML legislation,[32] which reduced the number of reports under Article 331 of the Code of Criminal Procedure (Table 7.2).

[31] The 'man in the middle' technique consists in interposing oneself between two parties who believe they are communicating directly with each other, impersonating one of the parties and instituting financial relations with the unaware interlocutor with a view to subsequent illegal gains (generally the acquisition of confidential financial data, the misappropriation of credit transfers and diverse payments). The most common method for carrying out this crime is illegal IT access to e-mail or other accounts of the victim's.

[32] Legislative Decree 8/2016.

Table 7.2

Reports to the judicial authorities	2015	2016	2017	2018	2019
Reports per Article 331 of the Code of Criminal Procedure	233	157	115	87	106
of which: submitted to judicial authorities	5	2	3	-	2
made in connection with technical reports sent to inv. bodies	228	155	112	87	104
Informative reports for investigative purposes	17	16	26	16	11

Cooperation with the DNA

Information exchange with the DNA under the protocols agreed to in 2017 and 2018 (see UIF *Annual Report for 2018*, p. 83) continued in 2019. The data transmitted by the Unit were of substantial help to the DNA's core function of promoting and coordinating investigations. In a number of cases the data led to further requests for cooperation to the Unit in order to acquire specific financial analyses to support criminal investigations.

The UIF again took part in the panel of technical experts set up at the DNA, which also involves the Customs and Monopolies Agency. The work concentrated on cases of underinvoicing of Chinese merchandise that have come to the Unit's attention in recent years. This practice consists in untruthful declarations of taxable values in the customs forms in order to evade the taxes due (VAT and duties); the Italian importers then rebate part of the difference between the real and declared value to the Chinese producer using hard-to-trace payment methods.

SAFE

A significant portion of the flow of information between the UIF and the investigative bodies was channeled through the SAFE portal, which permits fully computerized handling of the acquisition and processing of outside requests (see UIF *Annual Report for 2017*, Section 8.1).

Considerable use of the SAFE portal was made by the General Command of the Finance Police in the framework of investigations on behalf of the judicial authorities, which helped to enhance the speed and agility of the Unit's cooperation, especially on the international front. Public Prosecutors, by contrast, still tend to send most of their requests for cooperation by conventional channels. Only the Public Prosecutor's Office of Florence has begun information exchanges via SAFE.

7.2. Cooperation with the MEF and the FSC

The UIF cooperates with the Ministry of Economy and Finance (MEF), assisting in drawing up prevention policies, drafting regulations and liaising with international organizations as regards sanctions. The Unit participates in the work of the Financial Security Committee (FSC) set up at the Ministry, assigned to carry out analyses and coordination activities for preventing the use of the financial and economic system for purposes of money laundering and the financing of terrorism. All the authorities involved in the prevention and law enforcement system are represented on the Committee, which serves as a focal point for developing strategies and is responsible for applying international sanctions.

The UIF takes part in the work of the experts drawn on by the FSC; it provides support in drafting answers to the questions raised by commercial operators and financial intermediaries regarding the application of financial sanctions pursuant to European regulations and helps to consolidate guidelines for interpretation and draw up operational practices for sanctions.

The UIF was part of the working group that produced the document updating the National Risk Assessment, adopted by the FSC and released in March 2019. The updated assessment still rates money laundering risk in Italy as 'very significant' and raises the assessment of terrorist financing risk from 'fairly' to 'very' significant.

Italy's National Risk Assessment

The updated NRA uses the same methodology applied in 2014 to analyse the data and information on the period 2014-2018. However, there is a new classification of the supervised entities, based no longer on size but on the riskiness of their business operations, as determined by a set of statistical indicators developed in collaboration with the UIF. This approach is consistent with the revised supervisory model put in place by the authorities, which have strengthened the risk-based approach, in line with the recommendations of the FATF, the Basel Committee and other international bodies.

Despite a context of persistent problems (continuing substantial use of cash, a large shadow economy, and widespread illegal activity), the seriousness of the main actions that generate illicit proceeds (corruption, drug trafficking, tax evasion) and the recrudescence of terrorism (above all the actions of ISIS), Italy has been judged capable of responding to the risks of money laundering and terrorist financing thanks to adequate safeguards for prevention and suppression. These have been deemed sufficient also at international level and have been further reinforced thanks to legislative changes since the National Risk Assessment of 2014.

The new analysis also revised the judgment on the relative vulnerability of certain categories of operator. A distinction was made between Italian and foreign payment institutions and electronic money institutions (i.e. between those with a branch establishment in Italy and those doing business under the freedom to provide services), the new ratings reflecting the higher risk of the latter.

Trust companies under supervision (pursuant to Article 106 of the Consolidated Law on Banking) were deemed less vulnerable than others, owing to the stronger safeguards in place.

Among the providers of professional services, greater relative vulnerability was attached to accountants assigned to audit entities of public interest and entities subject to the intermediate supervisory regime. This judgment resulted, in part, from the findings of inspections conducted by the UIF and by Consob.

The risk assessment specifies the actions to be taken with respect to each operator and the various levels of priority. Apart from the desirable improvement in training and in dialogue with all operators, the high-priority interventions include strengthening the mechanisms of controls on agents, loan brokers and currency exchangers (confirmed as the weak link in the chain of financial service distribution), raising awareness among pro-

fessionals as part of active cooperation, and stricter monitoring of cash-for-gold operators, including via ad hoc guidelines. Lastly, with regard to problems detected in relation to the category of legal persons and trusts, the report sees the necessity of completing transposition of the EU measure providing for European interlinking of national registers (as envisaged by Legislative Decree 125/2019). The transposition will require finalizing the decree implementing the centralized register of beneficial owners.

7.2.1. List of designated persons and measures to freeze funds

The UIF monitors the implementation of asset freezing measures as part of the financial sanctions adopted at national or EU level in the framework of action to counter the financing of terrorism and the activities of countries that threaten international peace and security.

The UIF also collects financial information on the funds and economic resources that have been frozen and facilitates the dissemination of the lists of designated persons.

As regards countering the financing of proliferation of weapons of mass destruction, the overall framework of the sanctions adopted by the European Union against North Korea, also in accordance with UN Security Council resolutions, remained broadly unchanged. The European Union has adopted 16 amendments to the aforementioned regulation on North Korea (Regulation EU/2017/1509).

In particular, the new regulation extends the lists of persons subject to the freezing of funds and introduces new categories of goods (including oil) whose export is prohibited, as is the provision of related financial assistance by European financial intermediaries.

The requirement to send suspicious transaction reports to the FIUs in the event of suspected financing for proliferation (Article 23) and a specific authorization regime for transfers of funds for amounts that exceed certain thresholds were both confirmed.

In 2019 the UIF began a focused check on eight financial intermediaries, inquiring into compliance with the restrictions on funds transfers and provision of financial services to and from North Korea (Regulation EU/2017/1509, Article 21). The checks, on a sample of transactions carried out in 2018 and 2019, found that the intermediaries were in compliance with the restrictions.

The amounts of funds and economic resources frozen remained broadly at the same level as in 2018. Two accounts were closed owing to the delisting of a person on the consolidated UN list relating to ISIS and Al-Qaeda, and other changes in the amounts were due to account management costs and fees or transactions duly authorized by the Financial Security Committee or to the crediting of amounts to existing accounts, which EU rules expressly allow, provided that the new amounts too are frozen (Table 7.3).

Table 7.3

Measures to freeze funds at 31/12/2019

COUNTRY OR ENTITY	Accounts and transactions frozen	Persons subject to freezing	Amounts frozen		
			EUR	USD	CHF
ISIS / Al-Qaeda	30	25	38,518	114	
Iran	17	4	1,086,120	158,453	37,593
Libya	4	3	2,140,204	132,357	-
Syria	28	5	17,969,016	240,825	149,872
Ukraine/Russia	2	1	148,053	-	-
DPR of Korea	3	4	8,000	-	-
Total	**84**	**42**	**21,389,911**	**531,749**	**187,465**

As part of its participation in the work of the FSC, the UIF contributed to carrying out the assessments within its competence regarding compliance with the relevant legislation, specifically upon request of the UN panels of experts, tasked with verifying compliance with the requirements of the Security Council resolutions relating to the different sanction programmes in force. In the course of 2019, the UIF received four notices of fund freezes against entities included in the lists of those subject to financial sanctions. In most cases, these are updates regarding transactions on accounts held by designated Syrian banks.

7.3. Cooperation with supervisory authorities and other institutions

Italian legislation promotes cooperation between the various competent authorities and institutions at national level by providing that the Ministry of Economy and Finance (MEF), the supervisory authorities, the UIF, the Anti-Mafia Investigation Department (DIA), the Finance Police, government agencies and entities, the judiciary and law enforcement bodies work together to facilitate the discovery of circumstances that may point to facts and situations knowledge of which can be used to prevent the exploitation of the financial and economic system for money laundering or the financing of terrorism.

For the purposes of the AML decree, however, cooperation in derogation to official secrecy is provided for exclusively between MEF, the relevant supervisory authorities, the UIF, the DIA and the Finance Police.

Exchanges with the Bank of Italy's supervisory directorates

There was a constant exchange of information between the UIF and the Bank of Italy's supervisory directorates. The UIF helped to verify that there were no grounds for suspicion of money laundering or terrorist financing in certain acquisitions of significant holdings in banks.

The Supervisory Department submitted information to the UIF discovered during inspection activities, concerning possible shortcomings in active cooperation on the part of obliged entities. In turn, the UIF brought to the attention of the Department the anomalies found at intermediaries with regard to their organizational structure and compliance with the

Department's requirements (on evaluations for purposes of sanctions, see Section 5.2, 'Sanctions procedures'), as well as specific irregularities discovered in the course of financial analysis of suspicious transactions reported to the Unit.

... with Consob

Collaboration continued with Consob, with the usual exchanges of information on failures to submit STRs uncovered in the course of supervisory inspections and analyses of market abuse.

... with Ivass

In 2019, the continuing information exchanges with the insurance supervisor Ivass centred on the ascertainment of possible links of events relating to the ownership of insurance companies with money laundering or terrorist financing.

MED and Customs and Monopolies Agency

The UIF also cooperated with the Ministry for Economic Development and the Customs and Monopolies Agency in connection with transactions involving, respectively, trust companies and gaming operators. The Agency transmitted various information notes to the Unit, enabling it to conduct further inquiry into anomalous financial flows, some cross-border. The information exchanges with these two authorities could be impeded as a result of the new limits on national cooperation introduced by Legislative Decree 125/2019 (see Section 9.2, 'National legislation').

Investor Visa Committee for Italy

The UIF takes part in the inter-institutional Investor Visa Committee for Italy, which is mandated to assess whether applications comply with the legal requirements for issuing visas to foreigners intending to make investments in Italy, including via innovative entrepreneurial initiatives, or charitable donations for significant amounts (see UIF *Annual report for 2017,* p. 22). In the course of 2019, the UIF contributed to the evaluation of the investment visa applications submitted to the Committee, notifying it of any findings relating to the applicants, in all cases in full compliance with the secrecy rules governing the Unit's data, and responding, for its fields of competence, to any questions as to application of the rules.

Ministry of Justice

As provided for by Legislative Decree 231/2001, in 2019 the UIF continued to act as advisor to the Ministry of Justice concerning the codes of conduct drawn up by representative associations for purposes of crime prevention. In this context, guidelines are being drafted to assist the associations in drafting their codes, in order to facilitate examination by the competent authorities pursuant to the Decree. As far as the UIF's powers are concerned, the draft guidelines would differentiate the approach of the codes depending on whether the association members are subject to AML obligations or belong instead to other categories.

The UIF's representatives participate in the inter-institutional Coordinating Committee established by the Ministry of Foreign Affairs to develop an integrated approach to corruption, to foster dialogue and the sharing of information and proposals to ensure the active participation of the delegations representing Italy in international forums.

Anti-corruption Coordinating Committee

In addition to the Ministry of Foreign Affairs, which coordinates it, many other institutions are represented on the Committee, including the General Government Department, the National Anti-Corruption Authority (ANAC), the Ministry of Justice, the public procurement company CONSIP, the Ministry of the Economy (with representatives of the Treasury and Finance Departments), the Italian National Olympic Committee (CONI), the Ministry of the Interior (with representatives from the State Police Department), the Finance Police, the Customs and Monopolies Agency, the Italian National Statistics Institute (Istat) and the Italian Competition Authority (AGCM).

The UIF also takes part in a task force among the institutions belonging to the Committee in support of the Italian delegation to the G20's Anti-Corruption Working Group,

whose chairmanship passes from Saudi Arabia to Italy in 2021. The priorities for 2021 will include extending the corruption indexes, analysis of new forms of corruption, and the prevention of corruption in sports.

OECD evaluation of international corruption

The UIF is engaged in the fourth phase of the evaluation of Italy as regards implementation of the OECD Anti-Bribery Convention. The country monitoring exercise, begun in February 2020, is coordinated by the Ministry of Justice and also involves other public institutions. The final report, providing the conclusions of the analysis of the evaluation team and the on-site visit, may make recommendations and evaluations on the effectiveness of Italy's system for preventing and repressing crimes in connection with international bribery and corruption.

ANAC

On 11 September 2019, UIF and ANAC signed a new memorandum of understanding for the continuation of the cooperation instituted by the memorandum of 2014. The two bodies pledged, in the exercise of their respective institutional functions and in compliance with official secrecy obligations, to institute information exchanges with a view to identifying specific risk factors in connection with corruption or such as to jeopardize the proper functioning of corruption and AML safeguards in place in general government. Under the memorandum, ANAC is to assist the UIF in devising and updating indicators and patterns of anomaly, with special reference to the sectors most exposed to the risk of money laundering and corruption; and it may forward to the UIF information received from 'whistleblowers' (observing the principle of anonymity) or acquired within the framework of its own monitoring activity. The UIF contributes to devising risk factors and indicators for the prevention of corruption and stand ready to conduct joint analyses and studies as well as to share the general results of analyses and studies carried out as part of its own institutional functions. Both institutions will cooperate in promoting the proper application of the AML rules by general government entities.

Istat

In 2019 the UIF initiated a dialogue with Istat to work out forms of cooperation on AML-CFT. The initiatives planned will be directed first of all to providing Istat with methodological support in strengthening internal AML safeguards and mapping and analysis of money laundering risks in connection with certain activities (disbursement of grants to entities belonging to the National Statistics System, contracts for instrumental necessities and for institutional purposes, contracts with public and private entities to perform statistical analyses, etc.). An assessment is now being made of the possibility for the UIF to access statistical data that could be helpful in performing its function of strategic analysis and in developing anomaly indicators. The dialogue will also examine the possibility of the Unit's conducting training courses on money laundering risk as part of the programmes of the National Administration School.

8. INTERNATIONAL COOPERATION

8.1. Exchange of information with foreign FIUs

Within the system of international anti money laundering rules, the FIUs are given responsibility for the centralized reception and analysis of suspicious transaction reports and the related exchange of information with their foreign counterparts. These functions are essential for the analysis of financial flows that increasingly go beyond national borders and are therefore of interest to several jurisdictions.

Cooperation between FIUs is governed by the global standards of the FATF and the Egmont Group and by European Rules. The standards require FIUs to provide, either spontaneously or on request, and in a timely, constructive and effective manner, the utmost cooperation at international level on money laundering, associated predicate offences and the financing of terrorism.

The FIUs' power to exchange information is autonomous and direct, with no need for international treaties between governments. The UIF negotiates and concludes memorandums of understanding whenever they are required by the national law of the foreign FIU.

In accordance with the principle of multidisciplinarity, FIUs must have financial, investigative and administrative information for domestic analysis and reciprocal exchange. FIUs must also provide the information requested, exercising the same powers available to them for domestic analysis. The exchange of information between FIUs takes place using rapid and secure electronic communication systems. At international level, the Egmont Group manages and updates the encrypted platform called the Egmont Secure Web. At EU level, a decentralized communications infrastructure called FIU.NET is used for the structured exchange of information on a bilateral or multilateral basis and at the same time offers standardization, immediacy and a secure data exchange.

During 2019 the UIF exchanged information with the FIUs of all the EU Member States and with a total of 114 counterparts worldwide (compared with 125 in 2018). The suspicious transactions dealt with in these exchanges mainly concern the most common criminal phenomena in Italy: organized crime, corruption and tax offences, as well as cyber fraud. As part of the analysis of STRs, the UIF requests information from foreign FIUs where there are objective or subjective links to other countries.

Requests sent to foreign FIUs

Requests are generally aimed at reconstructing the origin or use of funds transferred from or to other jurisdictions, identifying movable or immovable assets abroad, verifying the formal ownership and the beneficial owners of companies and entities, and ascertaining whether there are ongoing inquiries or investigations.

Moreover, the exchange of information enables the UIF to provide Italian investigative bodies and judicial authorities with additional information to support their criminal investigations and proceedings (see Section 7.1, 'Cooperation with the judicial authorities').

In 2019, the UIF sent 963 requests for information to foreign FIUs. The number of requests held nearly stable after spiking at 1,082 in 2018. In detail, there was an increase of 19.3 per cent in information requests reflecting judicial needs and a 26.6 per cent decline in those concerning STRs with foreign connections (Table 8.1).

Table 8.1

Requests sent to FIUs in other countries					
	2015	**2016**	**2017**	**2018**	**2019**
Information required by the judicial authority	217	204	172	367	438
Information required for internal analysis	323	340	591	715	525
Total	**540**	**544**	**763**	**1.082**	**963**

The 'Ma3tch' function provided by FIU.NET for the anonymous matching of entire databases continues to be used. This makes it possible to identify recurring names in the archives of participating FIUs and links with other countries that otherwise would not be detected (see Section 8.2, 'Cooperation between FIUs').

The UIF received 1,350 information requests and spontaneous communications from foreign FIUs, an increase of 12.9 per cent for the year (Table 8.2).

Table 8.2

Requests/spontaneous communications received and responses provided					
	2015	**2016**	**2017**	**2018**	**2019**
Egmont network	1,078	1,259	668	594	621
Requests/spontaneous communications	*695*	*723*	*504*	*577*	*594*
Exchanges on ISIL	*383*	*536*	*164*	*17*	*27*
FIU.NET					
Requests/spontaneous communications	*518*	*580*	*524*	*602*	*729*
Total	**1,596**	**1,839**	**1,192**	**1,196**	**1,350**
Responses provided (1)	**1,223**	**1,568**	**1,232**	**1,681**	**1,862**
Communications to investigative bodies	**868**	**1,430**	**2,031**	**3,070**	**2,533**

(1) Refers to responses to requests for information and to feedback on communications, given when necessary.

Requests from foreign FIUs

The UIF responded to 1,862 of the information requests and communications received from foreign FIUs, 10.8 per cent more than in 2018. The figure comprises both responses to requests for cooperation and feedback on the use of the information acquired via spontaneous communications. In a good number of cases the feedback refers also to the quality

and usefulness of the assistance received. There was an increase (4.5 per cent) in the number of exchanges effected via the Egmont network, and in particular in the number of multilateral communications concerning financial networks and remittances traced to ISIL.

The UIF also exchanges information with FIUs that do not use the Egmont network, ensuring in any case the application of adequate security safeguards. This is particularly the case for counterparts that are not members of the organization.

A total of 11,017 cross-border STRs were received in 2019 from other European FIUs relating to cases with significant connections with Italy.

The most interesting cases involved the use of foreign accounts to transfer funds not reported to the tax authorities, the withdrawal and transfer of cash, and the layering of funds transfers to or from various countries. The use of trusts and trust companies to which to ascribe accounts or assets for purposes of interposition or dissimulation is common. A significant number of communications related to complex frauds or corruption, resulting in the transfer abroad of the proceeds; often the persons involved are under investigation in Italy.

Close attention continues to be paid to trade-based money laundering, which involves sophisticated import-export schemes of over- or under-invoiced goods. In the most significant cases, complex trading in goods and funds transfers through multiple countries were the work of criminal organizations re-investing large volumes of illicit proceeds.

The exchange of information with foreign FIUs has revealed that organized crime is especially active in transnational gaming operations.

Gaming has been growing rapidly in the European Union. It is estimated that the turnover on online gaming may reach €25 billion in 2020 (compared with €16.5 billion in 2015), while that on physical gaming is estimated at between €82 billion and €84 billion (€77.5 billion in 2015).[33]

The European Commission's updated Supranational Risk Assessment (see Section 9.1.2, 'Further European and international initiatives') identifies lotteries and gaming as a sector exposed to significant risks of money laundering and terrorist financing. Attention is focused both on traditional gaming (bookmaking and wagering, bingo parlors, casinos, slot machines, lotteries, poker) and online gaming.

The main threats are: i) the infiltration of organized crime into the ownership of gaming entities; ii) rigging of sports matches to determine results and alter bets; iii) acquisition of winning tickets or placing of safe bets by using various accounts and betting on every possible outcome so as to reduce or eliminate the risk of loss; iv) purchases of tokens or transfer of funds between gaming accounts; v) development of unauthorized online platforms by organized crime.

Cooperation among FIUs was especially important in inquiries into transactions and financial flows channeled by the European banks involved in recent cases of laundering of massive funds of Russian origin.[34]

---

[33] European Commission, *'Supranational Risk Assessment'*, 24 July 2019, p.190.

[34] European Commission, *'Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions'*, 24 July 2019. See also, below, Section 9.1, 'The evolution of European legislation'.

The UIF, along with other European FIUs, takes part in a task force to look into a vast activity of international money laundering involving one of the leading financial institutions of the Baltic countries. By sharing information, analyses and instruments, the task force detected an inflow of resources to Italy traceable to persons in Eastern Europe, often carried out by triangulation with corporate vehicles and foreign accounts. Often the funds served for transfers to third countries or investment in real or financial assets in Italy, in particular real estate and purchases of luxury goods. The UIF's contribution to the inquiry made it possible to identify and block some €20 million in foreign funds.

Again in 2019, there were numerous requests for cooperation regarding the suspension of transactions or the freezing of funds in Italy or abroad (a total of 50 cases, compared with 66 in 2018).

The application of suspension measures at the request of foreign FIUs is specifically provided for by the new European rules, transposed into Italian law by Legislative Decree 90/2017. The cases dealt with concern both the freezing of assets abroad, communicated as a matter of urgency by the FIUs of the countries concerned based on significant links with Italy and, conversely, requests by foreign FIUs to suspend transactions or block accounts in Italy where suspicious activities are detected or for precautionary purposes.

Cooperation for the suspension of transactions

In 2019 the UIF received 20 requests from foreign FIUs to block assets or resources in Italy, chiefly in connection with fraud, often cyber fraud, or identity theft, with the transfer to Italy of the proceeds for withdrawal or further transmission. In 30 cases, foreign FIUs alerted the UIF to the application of measures to block accounts or other assets traceable to persons with links to Italy who in most cases were under investigation. In these cases, the UIF promptly informed the Italian investigative bodies, and in the case of assets abroad intervened with the relevant counterpart FIU to prevent the assets from being released. This made it possible to identify, block and seize assets of persons under investigation that had not emerged during domestic investigations.

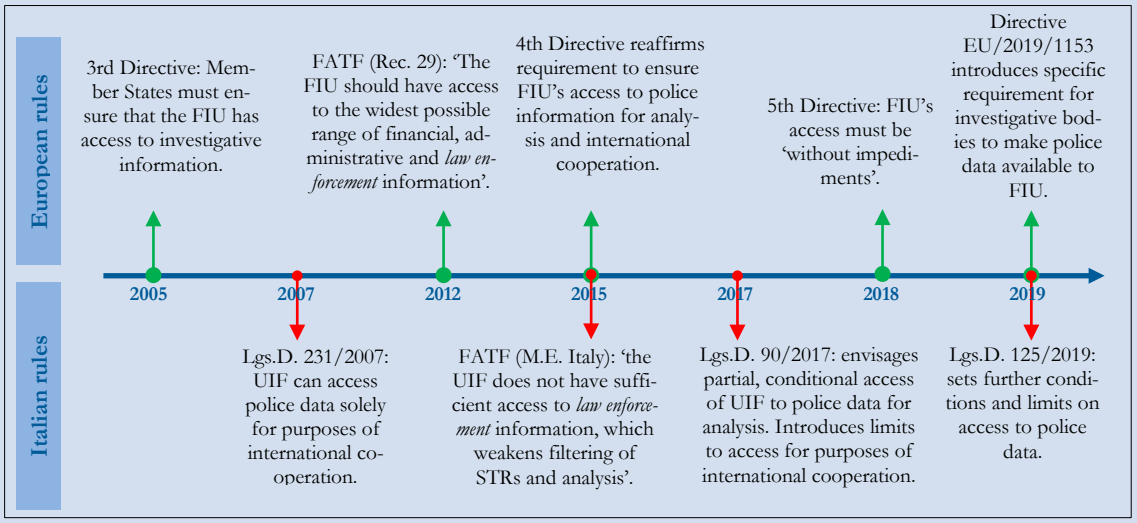
Specific provisions of the Fifth AML Directive enhance the information powers that must be granted to FIUs for domestic analysis and international cooperation.

FIUs must have the power to obtain information from any obliged entity, whether or not a prior suspicious transaction report has been filed. The information must be available in direct form upon simple request, and its acquisition may not be limited by national rules or procedures (e.g. conditions or authorizations). The new European rules prohibit the refusal of information exchange owing to connection with tax matters, national regimes of secrecy or confidentiality, or the existence of inquiries, investigations or proceedings under way. The directive further specifies that the information must be made available regardless of the existence or type of any predicate crime, in order to overcome a persistent problem that has prevented some FIUs from cooperating as asked.

Access to investigative information for international cooperation

The Fourth and Fifth AML Directives, in line with international standards, require the Member States to ensure that their FIUs have access to investigative information. This is necessary both for analysis and for cooperation with foreign FIUs.

Recent Italian legislation confirms the UIF's power to access investigative data for purposes of international cooperation, in derogation to confidentiality requirements (Legislative Decree 231/2007, Article 13-bis(3). However, de jure and de facto limits and conditions prevent prompt, full and fluid access.



The police data necessary for the UIF to perform its duties of mutual cooperation are transmitted with considerable delay and are significantly limited in substance, owing in part to systematic requests for judicial authorization even in cases where no investigative secrecy obtains. The flow of data to the UIF diminished steadily in the course of 2019, eventually almost ceasing. What is more, the data that were transmitted mainly referred to events that were not recent and hence of little use to the foreign FIUs making the requests for information.

Legislative Decree 125/2019 introduced significant amendments to Legislative Decree 231/2007 as it bore on international cooperation by the UIF (Article 13-bis). Some were in response to the objections raised by the Commission as part of the infringement procedure against Italy on the transposition of the Fourth AML Directive. Others, however, set new limitations on sharing, within Italy, of information acquired by the UIF through exchange with its counterparts abroad.

Until these recent amendments made it uncertain whether information could be made available to national authorities other than the Special Foreign Exchange Unit of the Finance Police or the Anti-Mafia Investigation Department, information on child pornography was also transmitted to the State Police's National Centre to Combat Online Child Pornography, while those relating to terrorist financing were forwarded to the Special Operations Group of the Carabinieri.

8.2. Cooperation between FIUs

Inter-FIU cooperation has been stepped up and extended to new forms. Despite growing difficulties in utilizing FIU.NET due to infrastructural obsolescence, the FIUs of the European Union have demonstrated greater capabilities for sharing information on cases of common interest, frequently availing themselves of a broader range of databases available in their own countries partly as a consequence of the Fourth Directive.

Exchanges have been sustained also by greater exploitation of the network's functions. The matching system serves to identify cases with otherwise unobservable connections with other countries, in particular exploiting the common criteria identified by the FIUs Platform (see Section 9.1.2, 'Further European and international initiatives'). The most significant cases with cross-border implications are considered for joint analysis; once activated by all the FIUs, the cross-border information flows will permit sharing a substantial store of information of mutual interest. However, an obstacle is posed by the significant differences in the single FIUs' methods of analysis, powers, and available information. Progress is possible by attaining greater harmonization of the rules and instituting forms of support and coordination through the specific European mechanism that the Commission is now weighing under the provisions of the Fifth Directive.

Work proceeded towards implementation of the automatic exchange of cross-border reports, instituted by the Fourth AML Directive, Article 53(1), to make sure that European FIUs transmit STRs with significant links to other Member States to the relevant counterpart FIUs.

The FIUs' Platform, as part of a project in which the UIF participates, approved an initial set of objective and subjective criteria designed to focus information exchange on cases of real interest for analysis.

Automatic exchange will involve, first of all, reports involving subjects operating under the freedom to provide services. Further subjective criteria refer, for instance, to the residence of the individuals or entities involved or the existence of investigations in other States. Objective factors concern the foreign origin or destination of financial flows or the holding of accounts or relationships abroad. The criteria also refer to links with illicit activities in another State and the importance of the case for other countries, based on elements drawn from specialized archives or discretional assessment.

Considering the wide range of STRs that may meet these criteria, a further selection is envisaged, based on matching via FIU.NET to bring out significant matches of cross-border connections.

The cross-border transmission of STRs by the FIUs of the European Union is still sporadic and highly uneven. Only a handful have instituted systematic exchanges of cross-border STRs, some still retain manual procedures and apply the agreed-on criteria only in part. Nevertheless, the volume of cross-border reports received is growing significantly, surpassing 14,000 in the last two years. Pending the application of the uniform criteria developed by the FIUs Platform, however, the reports exchanged by European FIUs are still markedly uneven in content and type. Since 2015 the UIF has been receiving cross-border reports on transactions by obliged entities operating under the freedom to provide services. For the most part, these reports come from FIUs in countries where online payment service platforms have been established. Since June 2017 the UIF has also been receiving, from some EU FIUs, cross-border reports identified according to the criteria laid down by the FIUs Platform.

However, the use of the IT tracks for these transmissions are highly uneven, which hampers fully automated handling.

Following Legislative Decree 125/2019, which provides that the UIF transmit to other European FIUs information on STRs regarding the Member States concerned, the Unit initiated the complicated process required for implementation of this new national rule. These are particularly costly obligations, whose complete fulfillment requires substantial investment in information technology and human resources, as well as appropriate selection criteria.

At the global level there remain limits to FIUs' ability to acquire and share financial data or information on the identity of the beneficial owners of corporations. In many cases these limits stem from forms of banking secrecy, privacy protections, and the relevance or equivalence of the alleged crimes in the country of the FIU to which the request is addressed. Further impediments derive from differences in the institutional nature of the FIUs, insufficient operational autonomy, or uncertain distinction between the tasks of analysis and those of investigation.

8.3. The EU FIUs Platform

The Platform, which has been active since 2006 and was formally recognized by the Fourth Directive, is the forum in which EU FIUs and the Commission discuss application of European rules, development of instruments of analysis and cooperation, and the conduct of joint operations.

Article 51 of the Fourth Directive gives the Platform a broad mandate focused on developing cooperation, both through the traditional instruments of information sharing and through innovative forms of automatic exchange and joint analysis. The exercise of this mandate is based on the results and proposals emerging from the Mapping Exercise regarding problems in the organization and activities of the European FIUs.

Standards and good practices have been defined, providing a common frame of reference for the more efficient utilization of the matching functionalities. The results of the project further the objective of making homogeneous, updated databases available for massive matching, while at the same time facilitating greater variety and extension of the types of underlying suspicious cases.

Within the Platform, the FIUs identify threats and vulnerabilities of common importance and subject them to in-depth analysis, comparing the patterns of behaviour that emerge from the transactions and contributing to the drafting of the Supranational Risk Assessment (see Section 9.1.2, 'Further European and international initiatives'). The Platform is also where the FIUs develop analyses and proposals on the European policies that concern their activity.

Activity centres on implementation of the Fourth and Fifth AML Directives, with special reference to the duties and characteristics of the European FIUs Coordination and Support Mechanism for inter-FIU cooperation. Special attention is paid to the transposition of Directive EU/2019/1153 (to be completed by August 2021), for uniform implementation of the measures instituting diversified channels of domestic and international cooperation between FIUs and investigative bodies. The Platform's priorities also include further study of new forms of cooperation and information exchange to institute between FIUs and the

customs authorities in implementation of Regulation EU/2018/1671, as well as with the supervisory authorities (CRD V, EBA Regulation).

The UIF has promoted the development of common analyses and positions on these issues in support of the European Commission and of European and national policymakers.

On the operational plane, the Platform imparts impulse to innovative forms of cooperation among FIUs through joint analysis of important cross-border cases.

Joint Analyses - Projects coordinated by the UIF

Joint analysis is an innovative form of cooperation among European FIUs envisaged by the Fourth Directive. Unlike ordinary information exchange in support of analyses conducted by each FIU, joint analysis involves the sharing of underlying cases that are of cross-border relevance and hard to deal with effectively on the strictly national plane, as well as further inquiry into them.

Through the Platform, the UIF has promoted a number of joint analytical exercises, some already concluded with the transmission of the results to the competent investigative bodies. Complicated mechanisms of financing of terrorism and international tax fraud have been reconstructed, and ideas have been developed towards a shared methodology for this new form of inter-FIU cooperation, compiled in a paper that will serve as support for further exercises but remains open to additions and modifications in the light of experience.

In 2019 the UIF sponsored two new joint analyses, still under way. Together with the FIUs of France, Germany, Spain and Hungary, an in-depth examination is being conducted on large-scale fraud and money laundering in connection with imports from China, settled for under-invoiced amounts.

The funds moved through this trade-based money laundering scheme are substantial, flanking and in good measure replacing the flows channelled in previous years through money transfer networks. The operational scheme reconstructed to date, in cooperation with the customs authorities of the countries concerned, involves the actual shipment of goods and is spread out in numerous EU countries, with arbitrage to exploit weaknesses in the various tax and customs regimes.

Together with the Croatian FIU, the UIF has initiated joint studies on widespread, repeated transfers by Italian firms, often newly formed, and active in particular merchandise sectors, of substantial funds to accounts in Croatia and other East European countries.

The modus operandi, followed systematically and often over long periods of time, consists in quick withdrawal in cash of the amounts transferred, or else retransfer abroad through accounts that are opened and immediately closed and companies that appear to have no real entrepreneurial purpose.

8.4. Developments in the FIU.NET

FIU.NET is the European IT infrastructure for cooperation and information exchange among FIUs for AML analysis.

Instituted in 2002, the network has grown steadily in sophistication and functionality, sustaining a constantly expanding volume of data and highly advanced forms of cooperation. It has been expressly recognized in European legislation (Directive EU/2018/843 – the Fifth

AML Directive – and Directive EU/2019/1153). Since 1 January 2016 FIU.NET has been hosted by Europol. In December 2019, following a special inquiry, the European Data Protection Supervisor delivered the opinion that the current operation of FIU.NET violates the data protection rules and ordered Europol to cease its management of the network, allowing 12 months to transfer the infrastructure to another entity.

The EDPS Opinion
The peculiar nature of the data and the tasks of the FIUs

The network's management procedures following its transfer to Europol were marked by problems in terms of the independence of the FIUs and the separation of financial analysis from investigative activity.

The importance and delicate nature of the data protection implications led the FIUs in 2018, at the prompting of the UIF, to request a check by the European Data Protection Supervisor of compliance with the guarantees of confidentiality and inaccessibility of the data exchanged among the FIUs for purposes of analysis and financial intelligence. In the opinion delivered in December 2019, the EDPS ruled that the legal basis for Europol's management of FIU.NET was lacking, insofar as the suspicious transactions in whose regard the FIUs cooperate have administrative relevance, in support of financial analysis, and do not relate to crimes and criminal investigations, to which Europol's competence is limited.

The EDPS consequently used its injunctive power to order Europol to cease all processing of data connected with FIU.NET and hence stop managing the network. The FIUs Platform began complex studies to devise, within the narrow time frame allowed, alternative solutions to permit the network's continued functioning and its consistent inclusion, in the future, in the developing European system, considering among other things the possible tasks to be assigned to the FIU Mechanism.

The EDPS opinion clearly states the principle of specialization, which under international standards and European AML rules characterizes the activity of FIUs and the use of their data.

The opinion is based on a series of principles, namely:

- financial analysis is an administrative task, distinct from criminal investigation;
- this task is reserved to FIUs, ad hoc authorities distinct from investigative bodies;
- the particular organizational nature of FIUs (whether they be administrative, police or mixed entities) does not affect the nature of their function or the way it is performed;
- the data underlying their analyses, first and foremost suspicious transaction reports, cannot be directly drawn on or used for investigative purposes;
- what makes possible the investigative utilization of the information processed by FIUs is the dissemination by the latter of the results of their analyses to support or trigger criminal investigations or penal proceedings.

8.5. Relations with foreign counterparties and technical assistance

The UIF maintained its commitment to international technical assistance in its areas of competence through bilateral initiatives and participation in multilateral projects. Activities in 2019 included the organization of a study visit to the Unit by members of the Ukrainian anti-corruption bureau, within the framework of an EU-funded programme of technical assistance. The visit focused on the UIF's experience of analysis to combat money laundering and corruption as well as on cooperation with other authorities, and specifically investigative bodies.

Knowledge of the legislative and organizational measures taken in Italy and the positive assessment of the FATF on the quality of the Italian AML arrangements have led foreign FIUs to request the UIF to provide assistance and to share experiences. The Unit's contribution relates to Italian regulations, characteristics, organization and activities.

The UIF also participates in technical assistance and support activities within the Egmont Group, and in particular the Training and Technical Assistance Working Group and the Membership, Support and Compliance Working Group. This involves assistance to FIUs in the formation or consolidation stages and development of training programmes. Assistance plans are also directed to overcoming operational difficulties and restrictions and to devising efficient procedures.

International technical assistance, through the dissemination and installation of effective systems and practices for the organization and activity of FIUs, fosters the formation of new FIUs, the reinforcement of existing ones, and their membership of the Egmont Group. This serves to extend the reach and enhance the efficacy of the global network for the prevention of money laundering and terrorist financing.

8.6. Participation in the FATF

Given the importance of international cooperation for combating money laundering and terrorism effectively, various governmental and technical bodies have been set up over time, their scope ranging from regional to global. The work of these bodies is particularly intense with regard to the different risk areas that are emerging at global level and the need to adapt and harmonize prevention and law enforcement measures.

The UIF participates in the activity of these international and EU bodies, either on its own or as part of delegations composed of members of multiple national authorities.

In 2019 the Unit again took part in the work of the FATF within the Italian delegation coordinated by the Ministry of Economy and Finance. The commitment in the working groups and in plenary meetings focused in particular on the Mutual Evaluation of Member Countries carried out under the fourth round and on the related follow-up checks. The UIF also cooperates directly, its experts participating in evaluations of the AML systems of individual countries to facilitate proper implementation of the standards and the effectiveness of the measures.

This contribution covers all the various stages of the evaluation procedure: recognition of the risks posed by each country involved and the quality of the collaboration with the local

authorities, analysis in drawing up the reports and participation in the discussion on their approval.

UIF experts took part in the assessment activities of the fourth round of Mutual Evaluation of Belgium, Canada, Austria and Switzerland, the follow-up on Spain headed by the FATF, and the Mutual Evaluation of Malta carried out by Moneyval; one expert is involved in the evaluation of France. The UIF's reviewers intervened in the checks on China and on the Czech Republic (as part of Moneyval).

Engagement in the evaluation activities makes it possible to detect shortcomings in individual countries' AML regimes with respect to international standards and weaknesses in their effectiveness, with a particular focus on the characteristics, activities and international cooperation of the FIUs. As well as contributing to ongoing in-depth analyses of the risks in connection with technological innovation and to the possible specific compliance measures for innovative operators and instruments (such as FinTech/RegTech), the UIF participated directly in reconnaissance and analysis of the peculiar risks inherent in the use of virtual currencies and the consequent extension of AML safeguards, achieved by focused amendments of the standards.

The UIF also took part in identifying and further analysing the updated typologies of money laundering and financing of terrorism, sharing the cases and the experience gained from its operational analysis (see Section 4.4, 'Interventions by international bodies').

FATF initiatives on virtual assets and stablecoins

Following the updating of the standards on virtual assets, in June 2019 the FATF released its guidelines on the safeguards required to deal with the risks of money laundering and terrorist financing inherent in the use of these instruments.

A contact group was formed in order for members to: i) share their experiences in this field; ii) devise solutions for the implementation of the standards, including by means of dialogue with the private sector; iii) increase communication and dissemination of knowledge; and iv) monitor emerging trends and weigh possible lines of intervention. Further study was begun on so-called stablecoins, transferable instruments based on blockchain technology; they differ from ordinary virtual assets in the stability of the value represented in digital form, thanks to the type of asset selected as reference for their issuance (for example, currencies that are legal tender or guaranteed securities, including government-guaranteed assets). Multiple kinds of stablecoin can exist, differing according to the characteristics of the scheme devised by the issuer and usually described in a white paper associated with each stablecoin. The FATF made it clear that the AML standards apply to all stablecoins, irrespective of their legal status.

Further study is under way on peer-to-peer transactions, by which digital instruments such as virtual assets and stablecoins can be transferred without the intermediation of an entity subject to AML obligations. These raise risk-prevention requirements analogous to those for cash transfers, but more severe in that thanks to information technology even very substantial financial resources can be transferred or distributed – practically instantaneously – between persons in different places or jurisdictions.

FATF Forum of FIU heads

The FATF Forum of FIU heads offers an authoritative venue for studying and producing proposals for the detection of risks and for policy action. The activity of the Forum, which

is not part of the formal organization of the FATF, depends on the impulse imparted by the rotating Chair.

The current Chair has not called any new meetings. The member FIUs have nevertheless continued to share experiences at meetings organized on the occasion of FATF working sessions, so as to ensure connection with the activities of the Egmont Group and share ideas emerging from their operational experience.

In 2019 the UIF contributed, within the Forum, to the finalization of three especially important projects.

The project 'Countering Proliferation Finance: FIUs' Roles,' initiated together with in-depth studies towards extending the standards on AML and combating the proliferation of weapons of mass destruction, has conducted a survey of national experiences in detecting risks of proliferation finance, in identifying and reporting suspicious transactions, and in applying adequate countermeasures via financial sanctions and targeted investigations.

The survey revealed significant differences in national approach as regards the role of the FIU, depending in part on the highly generic nature of the international standards, which focus principally on the application of UN-ordered fund freezes.

The project 'Enhancing FIU Strategic Analysis' has further analysed the main characteristics of this function, which differs significantly from FIU to FIU in its methods, information sources and output. The exercise identifies problems and factors of effectiveness; the compilation of a collection of good practices can favour convergence towards shared methods and objectives, enhancing the quality of strategic analysis.

The UIF contributed actively to the project, providing both the expertise developed through specific studies and the scientific knowledge acquired in the design and application of methods of quantitative analysis for the detection of AML-related anomalies.

A third project is dedicated to the role of intermediaries and FIUs in detection, reporting and analysis of criminal activities involving virtual assets. Study has highlighted the inherent limitations of traditional AML safeguards in their regard.

8.7. Participation in other international organizations

The UIF contributes to the activities of the Egmont Group by promoting its policies and lines of action. Of particular importance in the Group's activities are the Support and Compliance procedures activated when insufficient ratings are assigned in the Mutual Evaluation on issues relating to FIUs' activities and competences. The assessments conducted by the Egmont Group focus on problems in international cooperation and promote the adoption of appropriate corrective action, including through targeted technical assistance initiatives. Where necessary, action plans are drawn up to overcome the limits to FIUs' ability to cooperate, for example through the acquisition of additional information from obliged entities.

Six new FIUs were admitted to the Group in 2019, bringing total membership to 164. The Group concluded the preliminary analysis of reported shortcomings of the FIUs in seven countries. The UIF actively contributed, in particular by drafting the review of the Latvian FIU and monitoring implementation of the Group's action plan for the Swiss FIU

(with the objective of enabling that FIU to acquire information from obliged entities in line with the standards).

The Support and Compliance procedure, currently limited to technical compliance alone, will be extended to review the effectiveness of the activities of the FIUs, with particular regard to analytical work (Immediate Outcome 6 as per the FATF methodology) and international cooperation (Immediate Outcome 2). It is important to avoid duplication with FATF assessments, concentrating on the shortcomings most important to the work of the FIUs.

Further study was initiated on the various models of cooperation between FIUs and other public authorities (public-public cooperation), considering a broad spectrum of authorities as called for by international standards (investigative and judicial bodies, supervisory and control authorities, customs and other authorities involved in countering money laundering and terrorist financing).

The participating FIUs shared innovative experiences in cooperation, highlighting the positive results achieved in four key areas: asset recovery, money laundering in connection with tax offences, combating organized crime, and financing of terrorism. However, it is necessary to eliminate the many barriers (legislative restrictions, technological barriers, and cultural resistance) that still impede the ability of FIUs to cooperate effectively with the competent authorities, thereby maintaining the harmful segmentation of information between the various players.

The work of the Egmont Group continued with the identification and analysis of the typologies of money laundering and financing of terrorism. The Report on the Laundering of the Proceeds of Corruption was approved, setting forth 72 anomaly indicators (red flags), divided into four categories drawn from the operational experiences of FIUs in the analysis of STRs. A new homogeneous, structured format was developed for exchanging information via the Egmont network, which will allow greater automation and efficiency in international cooperation.

Further ongoing projects deal with the laundering of the proceeds from human trafficking and the drafting of operational guidelines for the analysis of virtual assets.

As a member of the Italian delegation, the UIF follows the activities of Moneyval. In this context, one of its experts participated in the Mutual Evaluation of Malta. In addition, a UIF expert provides support for the activities of the Conference of the Parties under the 2005 Warsaw Convention on Money Laundering and Financing of Terrorism of the Council of Europe.

Within the new system of thematic assessment adopted by the Conference to check implementation of the Convention in specific spheres, in 2019 attention went to the characteristics of the crime of money laundering and to the power of FIUs to suspend suspicious transactions reported. In this regard, the assessment confirms the completeness of the Italian system and the efficacy of the UIF in blocking potentially illicit transactions and liaison with the investigative bodies in this regard.

9. THE LEGISLATIVE FRAMEWORK

9.1. The international and European context

9.1.1. European regulatory developments

The European AML system, after being reinforced in 2018, evolved further in the year under review.

The main lines of development consisted in: making the most of financial intelligence, both to generate more information for FIUs themselves and to facilitate its use by a more extensive network of law enforcement agencies; strengthening cooperation, both national and international, among the competent authorities; reinforcing the safeguards for compliance checks and for the analysis of suspicious cases, with the possible centralization of certain tasks at European level.

Cooperation between FIUs, law enforcement authorities and Europol

This is the sense of Directive EU/2019/1153 of 20 June, published on 11 July 2019, which enhances cooperation among authorities, based on the observation that the efficacy of investigation and penal action may be compromised by the lack of mechanisms for prompt access to bank account information and financial data and analyses. The Directive lays down that 'bank account information',[35] financial information and the results of FIU analyses must be available for use by all the authorities assigned to prosecution of 'serious criminal offences';[36] while FIUs must have access to law enforcement information[37] in order to prevent money laundering, the related predicate offences and the financing of terrorism, as well as to facilitate cooperation among FIUs. The FIUs' access to such information, in addition to that provided for in Directive EU/2015/8493, Article 32(4), must be subject to national procedural safeguards.[38]

In implementing the Directive, each Member State must designate the authorities competent for the prevention, detection, investigation or prosecution of 'serious criminal offences'.[39] The list of authorities is set out broadly in order to avoid lacunae in information exchange; as the Directive specifies, the list must include 'at least asset recovery offices',[40] plus tax and anti-corruption authorities insofar as they are responsible for the prevention, detection, investigation or prosecution of criminal offences under national law.

---

[35] Directive EU/2019/1153, Article 2(1.7).

[36] The notion of 'serious criminal offences' refers to Annex I of Regulation EU/2016/794. It covers a very wide range of offences, not all strictly economic or financial in nature, including, for instance, in addition to terrorism, organized crime, trafficking in migrants, kidnapping, illegal trafficking in cultural goods and works of art, and sundry environmental crimes, also racism and xenophobia as well as homicide and grievous bodily injury.

[37] To ensure uniform application, Article 2(6) of the Directive defines 'law enforcement information' to include criminal records, information on investigations, on the freezing or seizure of assets, on other investigative or provisional measures and information on convictions and on confiscations.

[38] Article 8.

[39] Article 3. 'Each Member State shall notify the Commission of its competent authorities [so] designated … and shall notify the Commission of any amendment thereto.'

[40] Article 3(1).

The Directive does not interfere with provisions that define the purposes, actors and obligations of the AML system laid down in the distinct European rules to ensure compliance with the international standards. As far as FIUs are concerned, the Directive is intended to capitalize on their contribution of analysis also to benefit the prosecution of crimes other than money laundering and the authorities competent therefor, but with no implications as regards their own internal framework. Accordingly, the requirements of independence and operational autonomy are preserved, and the role and organizational status accorded to them in each Member State are not altered.

Specific provisions relate to cooperation between FIUs and Europol by means of information exchange, either direct or via the latter's national units.

FIUs must be able to obtain information from Europol in support of their own analyses, in keeping with the cooperative mechanisms envisaged in the national plan (see below). This requirement of reciprocity is found in the 'Europol' regulation',[41] which contemplates forms of cooperation between Europol and the competent authorities of the Member States, necessarily including the FIUs.[42]

The deadline for transposition of the Directive is 1 August 2021. By 2 August 2024, and every three years thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.[43]

The four reports of the Commission

New developments in AML rules were prompted by the recent episodes of crisis at some European banks, which were involved in transnational money laundering owing to serious deficiencies of governance and risk management and in the controls carried out by the competent national authorities.

The Commission's examination of the risks and possible policy action led to the publication, on 24 July 2019, of four reports, accompanied by a communication to the Council and the Parliament setting forth the main conclusions.[44]

Supranational Risk Assessment

The set of reports includes the update of the Supranational Risk Assessment (*Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*).[45] The Report updates the exercise completed in 2017, analyses threats and vulnerabilities in specific sectors, estimates the residual risks and sets out consequent recommendations to Member States. European FIUs participated directly in the studies, contributing with reports on the results of their own operations.

The Supranational Risk Assessment

The new Report analyses risks according to sectors of activity, the most common methods of money laundering and terrorist financing, and the various vulnerabilities of the financial and non-financial sectors.

---

[41] Regulation EU/2016/794.

[42] Regulation EU/2016/794, Article 7(8).

[43] Article 21(1).

[44] European Commission, *'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework'*, 24 July 2019.

[45] European Commission, *'Report from the Commission to the EU Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities'*, 24 July 2019. See below, Section 9.1.2, 'Further European and international initiatives.'

Cash is confirmed as the instrument most widely used by money launderers to transfer funds quickly. It is also the principal grounds for suspicious transaction reports. There continues to be a significant level of risk in connection with 'liquid' instruments equivalent to cash.

In the financial sector, the main risks arise in connection with innovative instruments (FinTech). The features of the products and the speed of transactions heighten risk in the absence of adequate due diligence and monitoring.

In the non-financial sector, the risks relate to the difficulty of identifying beneficial owners and the limitations imposed by professional confidentiality. In the gaming sector, risk exposure continues to be high for online products (significant volumes, remote operations) and low for bingo halls.

The risk exposure of non-profit organizations varies with their structure and activities. Organizations engaged in expressive activities (art, sports, culture) are especially vulnerable, and vulnerability increases with proximity to war zones and with establishment in countries whose systems for countering the financing of terrorism have deficiencies.

Emerging risks cited in the Report include: professional football, whose lack of transparency has created fertile ground for the use of illegal resources; free ports, owing to the possibility of counterfeiting, violation of intellectual property rights, VAT fraud and corruption; and 'investor visa' regimes, above all for the possibility of tax evasion and corruption.

The Report underscores vulnerabilities in connection with the spread of anonymous or unregulated products, such as virtual currencies, and the difficulty of identifying their beneficial owners. It also mentions the tardiness of many Member States in transposing the European AML rules.

The assessment, finally, cites a series of updated mitigating measures that the Union as a whole and the single Member States should adopt. As provided by the Fifth AML Directive, anti-laundering safeguards need to be extended to virtual currency service providers, while the content of registries of beneficial ownership of entities and companies must be broadened and their availability increased.

Cooperation between FIUs and the role of the mechanism

The Commission's report on recent cases of money laundering and serious deficiencies in organization and compliance involving some European banks,[46] considers the lacunae that were found in the relevant national control systems. The Report develops proposals for greater harmonization of the rules (for instance, by converting the Directive into a Regulation), the institution of a European supervisory authority (taking account of the new duties and powers now assigned to the EBA and the ECB), and strengthened cooperation among supervisors and between supervisors and FIUs.

One of these Reports is devoted to the interconnection of national bank account registers,[47] with the aim of granting integrated access to information on bank accounts throughout the Union.

---

[46] European Commission, *'Report from the Commission to the European Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions'*, 24 July 2019.

[47] European Commission, *'Report from the Commission to the European Parliament and the Council on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts'*, 24 July 2019.

Another Report examines the characteristics of FIU activities and cooperation[48] and the possible role of the European support and coordination mechanism under the Fifth AML Directive[49] and Regulation EU/2018/1672 on the physical transfer of cash.[50]

The Report stresses the central role of FIUs within the AML system and their independent status. It recognizes the key role of the FIUs' Platform in facilitating their activities and cooperation among them.

The Report notes the great variety, among Member States, of the formats and procedures for submitting suspicious transaction reports, and the consequent disparities and deficiencies of IT support tools. It considers the possibility of introducing uniform formats in order to make things easier both for the reporting entities and for the FIUs themselves. Every proposal for central reporting within the European mechanism has been met by reasoned opposing arguments by the FIUs and supervisory authorities.

The Commission criticizes the persistently inadequate application of the obligation to transmit cross-border STRs, affirming that this requirement is imperative for proper functioning of the AML system.

The Report underscores the weaknesses in the FIUs' ability to provide information, specifically noting the effects of restricted access to certain types of data and excessive slowness of response times (in the absence of enforced deadlines). Better exploitation of matching on the part of the FIUs is seen as essential.

In highlighting the positive results of the joint analyses carried out between 2016 and 2018, the Report mentions the difficulties encountered in reconciling the different national approaches and IT capacities, as well as the lack of a common methodology. It refers to the need to centralize the tasks of promoting and facilitating joint analysis within the European mechanism.

The paper recalls the technical shortcomings that, under Europol's management, impede the utilization of FIU.NET, the legal problems concerning data protection, and the persistent inaction on the indispensable development of the network.

The weaknesses in information exchange between FIUs and supervisory authorities are cited as one of the main causes of the recent crises involving some European banks. The Commission notes the need for greater information-sharing, recalling both the provisions of the Fourth and Fifth AML directives and the new measures introduced by CRD V.

The Commission expresses concern over the lack of data protection guarantees in third countries whose FIUs receive information for European FIUs, given that these countries lack equivalent rules.

The conclusions of the Report observe that FIUs, in addition to receiving higher-quality STRs, also need to be able to cooperate more extensively among themselves and with other national authorities, such as customs and tax agencies. Standard forms and efficient IT instruments for STRs would be useful. FIUs should ensure direct linkage of their systems with

---

[48] European Commission, *'Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units'*, 24 July 2019. The Report explicitly draws information and observations from the FIU Platform's Mapping Exercise on the features, powers, and cooperation of financial intelligence units.

[49] Article 65(2) of the Fourth Directive as amended by the Fifth Directive.

[50] Regulation EU/2018/1672, recital 26.

FIU.NET, as well as to produce more effective analysis. The FIUs' Platform has been essential for mapping problems, drawing up proposals, and developing operational activities at European level. However, it lacks the power to take binding measures or issue binding instructions. A more incisive mechanism is needed to develop methods, cooperation, and joint analysis. Developments along these lines could be promoted by the European mechanism.

The European FIU mechanism: tasks

In European fora the UIF has taken the initiative in fostering shared reflection on the tasks that should be assigned to the European mechanism and how they should be configured.

On the basis of this examination, also carried out within the European Platform, in the future framework of more harmonized rules the mechanism should draw up detailed provisions on compliance by the obliged entities, on the powers and functions of the FIUs, and on inter-FIU cooperation. These tasks may include issuing instructions on the grounds for filing suspicious transaction reports and on their contents, common instruments and methods of analysis and effective procedures for information exchange.

The proper functioning of international cooperation requires standards for full and effective communication of information and data, via motivated requests and rapid responses, based on adequate investigation. It is important to define a certain, shared framework governing the possibilities and limits of any utilization of the information exchanged, especially for criminal investigations or proceedings.

The mechanism could foster joint analyses among the European FIUs on phenomena of cross-border relevance, instituting appropriate methods and tools on the basis of in-depth study and the experience already gained in the Platform.

The essential functions of STR reception, financial analysis and dissemination in support of investigations (new or already under way) must still be entrusted to national FIUs; any other solution, apart from the difficulty of realization, would jeopardize the system's efficiency.

The mechanism's action should be conducted according to the principle of subsidiarity, flanking and supporting the action of the national FIUs without substituting for or overlapping with them. Interventions should concentrate on matters and cases that cannot be handled effectively on the national plane or without close operational relations between the member country FIUs.

In its Conclusions issued on 5 December 2019,[51] the Ecofin Council confirmed the reflections and proposals of the Commission in the reports cited above. On this basis, the Council determined a set of priorities: greater harmonization of European AML rules (possibly through a Regulation); resolution of the structural problems that have arisen in the activity of national AML supervisory authorities, including by means of centralization of tasks in a European body; increasing FIUs' capacity for effective analysis and cooperation, strengthening the impetus for joint analysis and instituting a mechanism for support and coordination.

[51] Council of the European Union, '*Conclusions on strategic priorities on Anti-Money Laundering and Countering the Financing of Terrorism*', 5 December 2019.

The Commission has planned the steps ahead and initiated the necessary studies. The FIUs have been involved directly, especially as regards the role and characteristics of the European mechanism.

On 7 May 2020 the Commission issued an Action Plan setting forth options and policy indications for a thorough revision of the European AML framework, on which it initiated a public consultation to conclude on 29 July 2020.[52] On the basis of its studies, the Commission will draw up legislative proposals for the Council and the Parliament, whose adoption is expected in 2023. Areas for action consist in six pillars, namely those identified in the Commission's four reports released at the end of July 2019. In particular, it reaffirms the necessity to: ensure effective transposition by Member States of Community rules; produce a more harmonized AML 'rulebook'; foster more efficacious supervisory arrangements based on a single European body; reinforce cooperation and integration among FIUs through the institution of a European support and coordination mechanism; improve criminal law enforcement; consolidate the EU's role as single global player within the FATF and in engagement with third countries.

9.1.2. Further European and international initiatives

Ma3tch

The Fourth Directive refers expressly to the need for more extensive and efficacious use of Ma3tch.[53] This FIU.NET function, which allows the anonymous matching of entire databases, makes it possible to identify names that recur in the archives of the participating FIUs and connections with other countries that do not emerge from the context analysed.

Work continued in 2019 to facilitate the more extensive and systematic utilization of the function. In this framework the FIUs' Platform finalized a report, to which the UIF contributed actively, making recommendations in order to attain more uniform exchanges among FIUs and integrate this instrument into the individual units' procedures for analysis and cooperation.

The report carries out reconnaissance on the approaches and procedures used by the various FIUs for the connection between Ma3tch and their own processes of analysis, selection of relevant cases, and exploitation of the outturn. While most of the units are aware of the positive effects of this matching, the report finds that for purposes of effective support to analysis the tool is still employed only episodically and in the absence of specific procedures.

The report further observes the need for extension and frequent updating of the datasets provided for matching. It invites the FIUs to earmark resources for the exploitation of Ma3tch, noting that this expense would be amply repaid by the efficiency gains from the increased capacity to assess the importance of single cases and their level of priority, including for activation of international cooperation.

High-risk third countries

In 2019 the Commission continued its work to finalize the methodology for identifying third countries which – by reason of strategic deficiencies in their systems of prevention – present high risks for the Union of money laundering or terrorist financing.[54]

---

[52] European Commission, 'Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing', 7 May 2020.

[53] Fourth AML Directive, Article 56.

[54] Article 9 of the Fourth Directive, as amended by the Fifth, assigns the Commission to prepare a list of high-risk third countries.

In order to support an independent assessment on the part of the Commission in identifying these jurisdictions, in lieu of simple reference to the list prepared by the FATF (a method criticized by the European Parliament), the Fifth Directive refers to additional factors to consider in determining strategic deficiencies, which now include not only the adequacy of the third country's legislative and regulatory framework but also the effectiveness of anti-money laundering measures and the action of the competent authorities. At the same time, the Fifth Directive strengthens the set of countermeasures vis-à-vis third countries at risk, instituting better-harmonized enhanced due diligence for obliged entities.

On the basis of the previous methodology the Commission, by a delegated regulation issued on 13 February 2019[55] and taking a more rigorous approach than the FATF, produced a list of 23 high-risk jurisdictions (as against just 12 on the FATF blacklist). The Regulation, approved by the Parliament, was rejected by the Council (see UIF *Annual Report for 2018*, pp. 107-108), which found that the blacklisting process was untransparent and did not offer the relevant countries the possibility of presenting arguments in their defence.

The new methodology was published by the Commission on 7 May 2020.[56] It acknowledges the need for dialogue with the third countries involved and guarantees coordination with the FATF's assessments, while specifying in greater detail the criteria and procedure for removal from the blacklist. In particular, it provides that inclusion on the FATF blacklist certainly means a presumption of risk also for the single market, and hence European blacklisting. The scope of the latter extends to additional countries where specific risks or threats originate, to be identified by independent assessment based on an ample set of factors and on the contributions of the FIUs and the Platform.[57]

The assessment takes account both of the type and intensity of the threats posed by third countries and of the vulnerability of their respective AML systems. The evaluation of the residual risk follows from this comparative consideration. The relevant areas for the assessment, according to this methodology, comprise: criminalization of money laundering and terrorist financing; customer due diligence requirements, record keeping and reporting of suspicious transactions; the powers and procedures of competent authorities; the sanction regime; the country's practice in international cooperation; transparency as to beneficial ownership; and implementation of international financial sanctions.

9.2. The national legislative framework

Closely following the 2017 reform,[58] in 2019 Italian AML rules were amended by the transposition of the Fifth Directive[59] into national law. On this occasion, some changes to the existing rules to dispel doubts of interpretation and new provisions were introduced on

[55] Issued pursuant to Article 64 of the Fourth Directive as amended by the Fifth.

[56] European Commission, *'Revised EU methodology for the identification of high-risk third Countries'*, 7 May 2020.

[57] FATF delisting, therefore, does not mean automatic European delisting.

[58] Legislative Decree 90/2017.

[59] Directive EU/2018/843.

such important matters as cooperation and information exchange between the authorities belonging to the AML system.[60]

The UIF made its own technical-institutional contribution to the legislative work coordinated by the Ministry of Economy and Finance. It produced a series of proposals and observations, some critical, on some of the measures (see the testimony of the Unit's Director to the relevant committees of the Senate and the Chamber of Deputies).[61]

Work continued on the drafting of secondary legislation, chiefly for implementation of the 2017 reform. The Bank of Italy and Ivass issued new provisions on organization, internal procedures and controls, and customer due diligence. The Bank also adopted a new measure for record-keeping and data accessibility, plus specific rules for the supervised entities referred to in Article 134 of the Consolidated Law on Public Security. The UIF, in addition to taking part in the work of the Bank and Ivass, also adopted its own Instructions on threshold-based communications and published new communications alerting obliged entities to particular risk sectors, in view among other things of the health crisis.[62]

9.2.1. Legislative measures

Legs. Decree 125/2019

The transposition into Italian law of the Fifth Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and the introduction of measures amending Legislative Decree 231/2007 were accomplished by Legislative Decree 125 of 4 October 2019, which went into effect on 10 November 2019.[63]

Cooperation between authorities at national and international level

The main changes relate to the rules for domestic and international cooperation among authorities and to some provisions concerning obliged entities, supervision of groups, due diligence and anonymous electronic money products. There were also some limited intrventions on sanctions.

On the domestic front, legislation retains the firm principle of cooperation among the administrative, judicial and investigative authorities to identify any circumstance that can serve in any way to prevent the use of the financial system for the purposes of money laundering or terrorist financing.[64] The new rules did establish, however, that for the purposes of Legislative Decree 231/2007 information exchanges in derogation to official secrecy shall be allowed only: *i)* between UIF, MEF, sectoral supervisory authorities, DIA and NSPV;[65] *ii)* in relations between all of the above authorities and the judicial authorities or police forces delegated by the latter, when the information is necessary to a penal proceeding.[66]

---

[60] See below.

[61] '*Hearing of the Director of the UIF of 18 September 2019*'.

[62] See below.

[63] The government was delegated to transpose the Fifth Directive on the prevention of money laundering or terrorist financing by Law 117/2019, the 'European delegation law' for 2018.

[64] Legislative Decree 231/2007, Article 12(1).

[65] Legislative Decree 231/2007, Article 12(1-bis).

[66] Legislative Decree 231/2007, Article 12(8).

As to international cooperation, three new provisions concern relations between the authorities involved in the AML apparatus,[67] international exchanges between the UIF and foreign FIUs,[68] and cooperation among the sectoral supervisory authorities.[69]

The first provision lays down a general requirement for cooperation with the competent authorities of other EU Member States, permitting a refusal only if justified by impediments to ongoing inquiries, investigations or penal proceedings.

The second provision furnishes significant clarifications of the rules for cooperation between FIUs, in order among other things to respond to the objections raised by the European Commission in the infringement procedure against Italy's transposition of the Fourth AML Directive. Specifically, it describes in greater detail the forms and procedures for cooperation between the UIF and other countries' FIUs, consistent with the specific provisions of the directive.[70] The general capacity of the UIF to 'exchange information and cooperate with the FIUs' in accordance with the usual requirements of confidentiality and reciprocity is now flanked by provisions specifying the minimum necessary content of information requests between FIUs (pertinent facts, context, motivation) and the modalities for use of the information exchanged.

The set of measures relating to the most recent reform correspond, moreover, to the modalities the Unit has constantly followed in its practice of international cooperation. There is also reference to the new indications for the use of the information acquired from other FIUs, which must be circumscribed to the purposes of analysis, in compliance with the limits set by the foreign counterparts, and any further sharing of which requires the latter's consent. The same safeguards apply to information supplied by the UIF.

Further, the same provision refers to the use of FIU.NET and adequate technology for the anonymous matching of data in support of information exchange and endorses the principle that in its international cooperation the UIF shall make use of all its powers as Financial Intelligence Unit for Italy.

It also expressly refers to the Unit's participation in joint analyses in accordance with the new modalities instituted by the FIUs' Platform and lays down the requirement to transmit to other countries' FIUs the information on relevant STRs, identified taking account of the indications formulated by the Platform itself ('cross-border reports').

The provision concerning sectoral supervisory authorities provides for information exchange between AML authorities, prudential and resolution supervisors, and the European Central Bank.

As regards another area, the reform modifies the rules on the UIF's access to investigative information. European rules and FATF standards envisage such access in order to enhance FIUs' capacity for financial analysis and compliance with the obligations of international cooperation. On this point, in addition to the limit already laid down in 2017, which subordinates access to any information covered by investigative secrecy to the approval of the judicial authority responsible for the proceeding, the 2019 reform further limits the UIF's

[67] Legislative Decree 231/2007, Article 13.

[68] Legislative Decree 231/2007, Article 13-bis.

[69] Legislative Decree 231/2007, Article 13-ter.

[70] Legislative Decree 231/2007, Article 13-bis.

ability to acquire investigative information: in fact, the Unit cannot be informed of cases in which a police investigation is under way and a notification has already been transmitted to the judicial authority, if the latter has not yet determined whether or not to take penal action.[71]

Problems with the new provisions on institutional cooperation by the UIF

Cooperation and information exchange between authorities is an essential prerequisite for the proper functioning of the anti-money laundering system. The changes made in 2019, however, threaten to be a backward step for these rules, significantly narrowing the spectrum of the Unit's permissible exchanges as part of its AML prevention.

As noted, the rules on official secrecy limit the set of Italian authorities with which the UIF is allowed to exchange information. In particular, exchange is not allowed with any police force except the NSPV and the DIA, or with other authorities whose control duties are inter-related with action against money laundering (such as the Revenue Agency, the Customs and Monopolies Agency, or the National Anti-Corruption Authority), in violation of the principle of broad cooperation affirmed in the decree. This approach is inconsistent with the anti-money laundering directives, which envisage the broadest cooperation with the AML authorities,[72] and in contrast with the indications of the FATF on the occasion of the Mutual Evaluation of the Italian AML system, and also, lastly, with the European Commission's report of 24 July 2019.[73] In practice, the restrictions introduced by this reform threaten to have an adverse impact on the UIF's institutional activities of cooperation, which – without prejudice to the special position of the NSPV and the DIA as recipients of suspicious transaction reports – should be conducted broadly and promptly with all the other authorities of the AML system, to the benefit of full efficacy of the preventive apparatus.

The new provisions authorizing the UIF to share the information acquired from the FIU network with the competent Italian authorities also raise questions of interpretation, in connection with the restrictions in force with regard to official secrecy, and they risk reducing the positive effects of international cooperation, with repercussions on the UIF's response capability and on other FIUs' judgment of its reliability in respecting international principles.

Finally, as a complementary aspect of information exchange among authorities, the restrictions on the UIF's access to investigative data do not appear to take account of the fact that the Unit's access to pre-trial information is perfectly consistent with the Unit's typical intelligence functions for the prevention of money laundering and terrorist financing. Such knowledge would enable it to corroborate, through financial analysis, those very inquiries. Similarly, the reference to the protection of investigative secrecy as regards international cooperation among authorities would not appear to be in line with the European rules.

[71] Legislative Decree 231/2007, Article 12(4).

[72] Article 49 of Directives EU/2018/843 and EU/2019/1153.

[73] See Section 9.1.1, 'European regulatory developments.'

Additional amendments to the AML decree exclude financial consultants from the scope of the obligation to transmit aggregate data to the UIF[74] and extend to general government communications the rules on analysis and development of STRs.[75]

Aggregate data, general government and threshold-based communications

The amended legislation specifies that communications from general government entities shall be subjected to financial analysis by the UIF and then transmitted to the competent investigative bodies as is provided for with regard to the analysis and development of suspicious transaction reports.

It clarifies the perimeter for utilization of the information obtained from threshold-based communications, i.e. the data relating to transactions held to be at risk, identified on the basis of the objective criteria (thresholds) defined by the UIF in its Instructions and transmitted periodically to the Unit. In particular, Legislative Decree 231/2007 now specifies that apart from their use for the analysis of phenomena or typologies of money laundering and financing of terrorism and for the financial analysis of suspicious transactions, such communicatons shall be utilized also for further investigative analyses.[76]

Obliged entities

An important change consists in the broadening of the scope of the anti-money laundering obligations to new entities, in particular persons engaged in trade in antiquities and works of art, provision of virtual currency services and real estate intermediation.

The AML rules now apply to all those who buy or sell works of art or serve as intermediaries in such purchases or sales, and to those who store, trade in or intermediate sales of works of art within free ports. The obligations apply only where the value of the transaction is at least €10,000.[77]

In the virtual currency sector, obliged entities now include 'providers of digital portfolio services',[78] for prevention of risks in connection with the safeguarding of private cryptographic keys on behalf of clients for purposes of holding, memorizing and transferring virtual currencies.[79] The notion of 'digital currency service providers' is significantly modified in accordance with the FATF's indications on the occasion of the revision of the international standards on virtual assets and virtual asset service providers.[80] The definition of virtual currency itself has been significantly revised to specify that it comprises the digital representation of value, not only not issued by but also not guaranteed by any central bank or public authority and not necessarily linked to a currency that is legal tender. It is further specified that virtual currencies comprise not only those used as means of exchange for the purchase of

[74] Legislative Decree 231/2007, Article 33.

[75] Legislative Decree 231/2007, Article 40(1.d).

[76] Legislative Decree 231/2007, Article 47(2).

[77] Legislative Decree 231/2007, Article 3(5.b) and 3(5.c).

[78] Legislative Decree 231/2007, Article 3(5.i-bis).

[79] Legislative Decree 231/2007, Article 1(2.ff-bis).

[80] Legislative Decree 231/2007, Article 1(2.ff). According to FATF, the activities covered include not only exchange between virtual assets and legal tender but also i) exchanges between one or more forms of virtual asset; ii) transfers of virtual assets; iii) custody and/or administration of virtual assets or instruments that allow control of virtual assets; iv) participation in or provision of financial services in relation to the offer and/or sale of an issuer's virtual asset.

goods and services and transferred, stored and negotiated electronically but also those used 'for investment purposes'.[81]

For business agents engaging in real estate intermediation, it is specified that the obligations of Legislative Decree 231/2007 apply also to instances in which they act as intermediary for the rental of a property, providing that the monthly rental is at least €10,000.[82]

The new text of the measure also clarifies that in credit securitizations, the banking or financial intermediaries charged with collecting the transferred credits, performing cashier and payment services and verifying conformity, shall comply with the AML obligations also in respect of the debtors transferred to the credit securitization vehicles and the subscribers of the securities issued by these companies.[83]

Group supervision

The amendments to the law affect the duties of the sectoral supervisory authorities, which were given new powers for more effective supervision of banking and financial groups.[84] The same logic applies to the new provision requiring parent companies to adopt a comprehensive approach in preparing safeguards and procedures to mitigate the risks of money laundering and the financing of terrorism, according to the modalities laid down by the sectoral supervisory authorities.[85]

Beneficial owner and due diligence

Some changes were also made to the rules on beneficial ownership[86] and accessibility of the information to be contained in the nascent Register of Beneficial Owners.[87]

On 23 December 2019 the MEF, in concert with the Ministry for Economic Development, initiated a public consultation on the Register of Beneficial Owners introduced by Legislative Decree 90/2017. The information on beneficial ownership of companies with legal personality, of private legal persons, of trusts producing legal effects relevant for fiscal purposes, and of legal regimes similar to the latter must be communicated and conserved in a special section of the Company Register, access to which is open to the authorities specified in the anti-money laundering decree, to the obliged entities and to the public, under the terms and conditions laid down by Legislative Decree 231/2007. The draft ministerial decree, the consultation on which was concluded on 28 February 2020, lays down the modalities for item entries, access to and conservation of the Register. The data and information must be made available for a period of 10 years. The initial communication must be transmitted by the entities involved to the Chamber of Commerce by 15 March 2021 or, for entities established after that date, within 30 days of their establishment. Any variations must also be communicated within 30 days. The Chamber of Commerce is also assigned competence for ascertainment and prosecution of violations of the obligation to communicate data and information on beneficial ownership and for levying sanctions.

---

[81] Legislative Decree 231/2007, Article 1(2.qq).

[82] Legislative Decree 231/2007, Article 3(5.e).

[83] Legislative Decree 231/2007, Article 3(2-bis). This regulatory change is intended to overcome the problems that have arisen for the analyses and supervision performed by the Bank of Italy and the UIF, both on- and off-site.

[84] Legislative Decree 231/2007, Article 7.

[85] Legislative Decree 231/2007, Article 16(1).

[86] Legislative Decree 231/2007, Article 20.

[87] Legislative Decree 231/2007, Article 21.

Some aspects of customer due diligence were revised, in particular enhanced due diligence.[88]

Other changes

The decree adds a series of items that the obliged entities must now consider in carrying out enhanced customer due diligence: transactions involving oil, arms, precious metals, tobacco products, cultural artifacts and other mobile goods of archeological, historical, cultural or religious interest or of rare scientific value, ivory, and protected species. It is specified that in the case of relationships, services and transactions involving high-risk third countries, enhanced due diligence must always be implemented, as in respect of customers or beneficial owners who are politically exposed persons, save when they are acting in the capacity of a general government body. In the latter case the obliged entities shall adopt customer due diligence measures commensurate with the concrete risk discovered.

Parliament intervened on the text of the decree also for purposes of coordination with the personal data protection rules.[89]

In implementation of the Fifth Directive, the decree introduces a ban on the issuance of anonymous electronic money products and on the use of such products issued in foreign countries as from 10 June 2020.[90]

Sanctions

Several specific correctives were made to the rules on sanctions in order to remedy problems that had arisen in application.

The measures: i) clarify the applicability of sanctions for failure to submit an STR also to the natural person who is responsible for carrying out an audit assignment;[91] ii) provide expressly for the sanction power of the MEF in the case of infringement of the information obligations vis-à-vis the UIF;[92] iii) clearly establish that sanctions can be imposed for infringement of provisions issued by the sectoral supervisory authorities on matters of organization, procedures and internal controls and also expressly assign to those authorities the powers of sanction for infractions committed by the persons responsible for the direction and control functions of intermediaries;[93] and iv) introduce new sanction provisions addressed to cash handling operators under the supervision of the Bank of Italy.[94]

---

[88] Legislative Decree 231/2007, Articles 24 and 25.

[89] Legislative Decree 231/2007, Article 2 (*Purposes and principles*) and Article 39 (*Prohibition of communications regarding suspicious transaction reports*). The latter article has been amended further in order to clarify the exact scope of the derogation to the prohibition on communication to customers or third parties of the fact of a report's having been made, of information exchanges with the UIF, or of the existence (or probable existence) of investigations or analyses, as provided by Article 39(3). Specifically, the clause now provides that the prohibition shall not apply to communications between banking and financial intermediaries, on condition that they belong to the same group (or to communications between intermediaries and their branches or subsidiaries in which they have a majority interest situated in third countries, providing that said branches or subsidiaries are in compliance with group policies and procedures).

[90] Legislative Decree 231/2007, Article 50.

[91] Legislative Decree 231/2007, Article 58(3).

[92] Legislative Decree 231/2007, Article 65.

[93] Legislative Decree 231/2007, Article 62. The State Council had already so ruled (Opinion 2017 of 3 August 2018).

[94] Legislative Decree 231/2007, Article 62.

Tax decree

The so-called 'tax decree', lastly, provides for the gradual lowering of the limit on transfers between different persons of cash and bearer securities (not made via banks or other authorized intermediaries), as provided by the AML rules.[95]

The decree provides that the current limit of €3,000 be lowered to €2,000 as of 1 July 2020 and then to €1,000 as of 1 January 2022. The sanctions for infractions are proportionate to the new limits: hence the minimum will be €2,000 from July 2021 to the end of the year and €1,000 from then on.

Decree Law 34/2019 converted into Law 58/2019

One legislative change in 2019 worthy of mention was the insertion into the Consolidated Law on Finance of a new type of corporate entity, the *Società di Investimento Semplice* (SIS), or simple investment firm, whose configuration as a fixed-capital investment firm (SICAF) makes it subject to the AML regulations.[96] There are also provisions to foster innovation and competition in the capital market by means of the creation of a temporary, experimental technical-legislative space for firms in the FinTech sector, with simplified regulation, while guaranteeing adequate investor protection.

The measure determines that the Ministry of Economy and Finance, after consulting the Bank of Italy, Consob and Ivass, shall adopt one or more regulations defining the conditions and procedures for experimentation with FinTech activities to pursue, by means of new technologies such as artificial intelligence and distributed registry, product and service innovation in the areas of finance, credit, insurance and regulated markets. A FinTech Committee is to be formed under the MEF, assigned to determine the objectives, define the programmes and take actions to foster the development of FinTech, and also to formulate legislative proposals and facilitate contacts between the operators in this area and governmental institutions and authorities.[97] On 19 February 2020 the MEF published its draft of the FinTech regulation; the draft, subjected to public consultation ending on 19 March, further specifies the competences of the FinTech Committee, the scope of the experimentation and the requirements for admission to it.

9.2.2. Secondary legislation and self-regulation

Instructions on threshold-based communications

The procedure for approval of the UIF's Instructions on threshold-based communications (*'UIF instructions on threshold-based communications'*) was completed on 28 March 2019 after the Financial Security Committee handed down its favourable opinion on 20 March. The Instructions were published in the *Gazzetta Ufficiale* on 15 Aplril 2019 (see Section 1.4, 'Threshold-based communications').

The Instructions, implementing the provisions of primary legislation and consistent with national and international risk analyses, specify the types of transactions to communicate and the categories of obliged entities, as well as the cases in which the

[95] Article 18 of Decree Law 124/2019, converted with amendments into Law 157/2019, amending Articles 49 and 63 of Legislative Decree 231/2007.

[96] The SIS – whose exclusive corporate purpose is direct investment of the capital raised in SMEs not listed on regulated markets, during the phase of testing, formation, and start-up of business – is defined by the law as an Italian Alternative Investment Fund. In fact, the Consolidated Law on Finance, Article 1(1.m-ter), defines as 'Italian alternative UCITS' all investment funds, SICAVs and SICAFs within the scope of Directive EU 2011/61.

[97] Decree Law 34/2019, Article 36. The Bank of Italy, Consob, and Ivass are also assigned, each for its own area of competence, to draft an annual analytical report on the FinTech sector, showing the results of application of the experimental regime and suggesting legislative or regulatory modifications that may be necessary to the development of this industry, the protection of savings and financial stability.

transmisstion of a threshold-based communication excludes the obligation to report the transaction as suspicious. In particular the Instructions require banks, Poste Italiane, payment institutions and electronic money institutions (including branches and central contact points) to transmit to the UIF, every month, the data on cash transactions totalling €10,000 or more in the month, even where they consist in several transactions of at least €1,000. The communication excludes the need for the STR when the transactions: a) are not connected with other transactions, different in type, that suggest total transactions that are suspicious; and b) are not carried out by customers at high risk of money laundering and financing of terrorism (for more details, see Section 1.4, 'Threshold-based communications' as well as UIF *Annual Report for 2018*, Section 9.2.2 and box 'Instructions for sending threshold-based communications').

Communication on anomalous use of virtual currencies

On 28 May 2019 the UIF issued a *'Communication on the anomalous use of virtual currencies'*. Apart from referring to the previous *'Communication of 30 January 2015'*, the new communication describes additional risky behaviours, drawn from the Unit's analysis of the STRs received, and gives supplementary indications for compiling the reports, with a view to better description of the suspicions and fuller transmission of information relevant to the UIF's financial analysis.

The new Communication draws attention to the possibility of anomalous origin of the funds used to purchase virtual assets and in particular to the collectors who gather funds from multiple persons by reloading prepaid cards, credit transfers, and repeated cash deposits. Special attention must be paid to possible links with criminal activity denoted by the use of information technology, in particular scams via websites, as well as cases in which the use of the virtual assets appears directed simply to increase the opacity of speculative, real estate or corporate transactions. Reporting entities must also consider the possible utilization of virtual assets in connection with suspected unauthorized financial intermediation and infringement of the rules governing the offer to the public of financial products or the provision of investment services. In any event, the proper appreciation of these situations demands careful assessment of the characteristics of the various entities involved, even where they are specialized, in the transactions under examination. To channel reports on anomalous use of virtual currencies to the appropriate method of analysis, the UIF has also made available to reporting entities a dedicated field in the reporting form.

Faced with the COVID-19 pandemic, on 27 March 2020 the UIF issued a Statement under the title *'Temporary measures and instructions to mitigate the impact on entities obliged to transmit data and information to the UIF'*.

Considering the operational difficulties in connection with the health emergency, entities required to transmit data and information to the UIF were allowed an extension of 30 days with respect to the ordinary deadlines for the transmission of aggregated data, threshold-based communications, and declarations on gold transactions. The statement further specified that in administrative proceedings for infringement of the legal obligations ascertained by the Unit and those proceedings in which the Unit has powers of inquiry, the suspension of time limits envisaged by Decree Law 18/2020, Article 103 (from 23 February to 15 April 2020), later further extended (to 15 May) by Decree Law 23/2020, and the modalities for notification by mail laid down in Decree Law 18/2020, Artricle 108, would apply.

Communication on prevention of financial crimes in the COVID-19 emergency

On 16 April 2020 the UIF issued a *Communication* for the prevention of financial crimes in connection with the COVID-19 emergency. Within the framework of public measures to

support persons and firms in difficulty, the Communication appeals for cohesive action to prevent any distortions and preserve the integrity of the legal economy. The entities obliged to detect suspicious situations are thus called on to pay attention to certain risk profiles in order to keep the level and quality of active cooperation high.

The Communication stressed the risks that could arise in handling the COVID-19 health emergency, and in particular those relating to possible fraud in the supplies and services directly involved in dealing with the emergency. It highlighted the risk of supply and marketing of products, such as personal protective equipment, sanitizing solutions and electro-medical equipment, that is actually non-existent, counterfeit or of quality inferior to the requisite standards, as well as of speculative manoeuvres on these products. It noted some possible cases of corruption, especially in contract assignments to provide supplies or services for assistance and research, and also mentioned fraudulent mechanisms in connection with fund-raising, including online crowdfunding, for the benefit of fictitious non-profit organizations. The communication further noted that the prolonged lockdown had produced situations of financial difficulty, with a high risk of criminal infiltration by organizations which, thanks to local roots, recruitment of members among the most vulnerable groups, and abundant illicit capital, can exploit new opportunities for usury and for acquisition or infiltration of troubled firms with a view to money laundering. Given public programmes for the distribution of fresh financial resources to firms in difficulty, very careful attention has to be paid to possibly criminal abuses that may occur in the accessing of credit guaranteed by various forms of government intervention, as in the use of the resources so made available. Lastly, the communication recalls the importance of monitoring the new electronic payment instruments and remote activities, in particular online activities, whose increased use heightens exposure to the risk of cyber crimes against individual users or firms or entities (e.g. phishing, business e-mail compromises, CEO frauds, and ransomware attacks, sometimes requesting ransom to be paid in virtual currencies).

Instructions on SARA

The Bank of Italy's changes to the rules on record-keeping[98] necessitate the updating of the UIF's instructions on aggregate AML reports (Segnalazioni AntiRiciclaggio Aggregate, SARA), to terminate the transitional period of continuing application of the provisions of 23 December 2013. The UIF's measure will not only delete references to the Single Electronic Archive and set the threshold for reporting transactions at €5,000 but also clarify the relationship between the current rules, the new secondary regulations on customer due diligence and the instructions on threshold-based communications, as well as update the Infostat-UIF registration form as regards the entities subject to the obligation to transmit aggregate data pursuant to the reforms of 2017 and 2019.

Bank of Italy

On 26 March 2019 the Bank of Italy issued a *'Measure containing provisions on organization, procedures and internal controls for purposes of preventing money laundering and the financing of terrorism'* and on 30 July a *'Measure on customer due diligence'* (see UIF *Annual Report for 2018*, Section 9.2.2).

The deadline for compliance with the new provisions on AML organization, procedures and internal controls was set at 1 June 2019, but an extension (to 1 January 2020) was granted for certain obligations, such as description of the policy on choices concerning organizational arrangements and the obligation to conduct the risk self-assessment (whose results for 2019 must be transmitted to the Bank of Italy by 30 April 2020).

[98] See below.

As to due diligence, reporting entities are required to comply with the new instructions by 1 January 2020; and for customers acquired prior to the entry into force of the Measure, for whom the previous regime allowed some exemptions from the due diligence requirements, any missing data and identification documents must be procured by the first possible contact, and in any case no later than 30 June 2020.

On 23 April 2019 the Bank of Italy issued rules applicable to the supervised entities referred to in Article 134 of the Consolidated Law on Public Security that handle euro banknotes and are required to be entered in the register kept by the Bank. The *Measure* specifies the requirements and procedure for entry in the register and the organizational safeguards and international controls that these operators must institute for AML purposes.

Pursuant to the proportionality principle, operators are required to institute the AML function and formally assign responsibility for transmitting suspicious transaction reports to the UIF; for smaller operators with less complex operations, simplified diligence requirements are provided for. In addition, the Measure requires the transmission to the Bank of Italy of regular AML-CFT reports and indicates the powers of control, intervention and sanction assigned to the supervisory authority. These provisions supplement those concerning cash handling , last amended on 5 June 2019.

On 19 September the Bank initiated a public consultation on its draft Measure containing *'Provisions on customer due diligence and the conservation of data and information for non-financial agents entered in the register referred to in Decree Law 350 of 25 September 2001, Article 8'*, addressed to agents engaged in the handling of euro banknotes. The consultation terminated on 18 November 2019 and the final text was approved on 4 February 2020.

The Measure lays down the general criteria of the AML decree on whose basis agents must determine the risk profile to assign to each customer. For the application of simplified diligence, an additional factor of potential low risk is having the legal status of banking or financial intermediary. For enhanced due diligence, in addition to providing examples of some high-risk factors specified by the AML decree, the Measure also indicates others, calibrated in relation to the agent's typical business, and further specifies the content of enhanced due diligence.

Cash handling is often performed as part of trilateral relations, involving the agents to whom the measures are addressed, their customers (mainly banking and financial intermediaries that have outsourced their cash handling operations), and the person to whom the agent concretely provides the service (the 'subject served', for instance mass retailers, money transfer agents, etc.), which are usually customers of the intermediary. The provisions are intended to ensure that agents carry out due diligence on their own customers and at the same time, for the efficacy of the AML system, require them to monitor the transactions of the 'subjects served' so as to detect any anomalies or incongruencies to consider for purposes of submitting an STR.

On 24 March 2020 the Bank of Italy issued its new *Measure on conservation and accessibility of documents, data and information for countering money laundering and the financing of terrorism*, replacing the Bank's measure of 11 April 2013 on the Single Electronic Archive; supervised intermediaries must comply with the new measure by 31 December 2020.

The new measure governs the procedures whereby the data and information stored pursuant to AML legislation must be made accessible to the Bank of Italy and the UIF in order to guarantee the reconstructability of customers' transactions and facilitate the control

functions, including inspections. Intermediaries may, alternatively: i) use computerized record-keeping systems that meet the technical standards and principles laid down by the measure in terms of accessibility, timeliness, integrity, non-alterability, transparency, completeness and clarity of the data and information; or ii) opt for dedicated archives that meet the standards of the measure ('standardized archives'). The latter include the archives already instituted when Legislative Decree 90/2017 went into effect (in particular Single Electronic Archive).

The measure specifies certain data that intermediaries must make available to the competent authorities; to be noted, in particular, are the provisions concerning transactions of €5,000 or more; the indication of the cases referred to in Legislative Decree 231/2007, Article 17(6) (provision of payment services and issue and distribution of electronic money by means of agents engaged in financial activitiy or authorized persons and agents), for which the data and information must be made available regardless of amount; the abrogation of the requirement to record split transactions; accessibility of information on accounts and other transactions with general government entities. In addition, with regard to the requirement to make the relevant data available to the authorities, exemptions are provided for accounts and transactions with certain types of customer. The data and information must be accessible to the authorities for ten years after the closing of the account or conclusion of the transaction.

Ivass

On 12 February 2019 the insurance supervisor Ivass issued the Regulation implementing Legislative Decree 231/2007 as regards organization, procedure and internal controls, and customer due diligence,[99] and on 11 December it released for public consultation the draft *Measure* laying down the requirements for identifying secondary establishments in Italy and insurance intermediaries subject to the requirements of instituting AML and internal audit functions, as well as firms doing business in Italy without branches that are required to designate an STR officer. The Measure will amend the aforementioned Ivass Regulation of 12 February 2019 to include the methodology for the self-assessment of money laundering risk. The consultation was concluded on 25 January 2020.

Council of Accountants

On 16 January 2019 the National Council of Accountants, in keeping with the Financial Security Committee's opinion of 6 December 2018, adopted the technical rules envisaged by the AML decree[100] for risk assessment, customer due diligence and record-keeping.

Following the approval of the technical rules, on 22 May 2019 the Council issued interpretative guidelines to assist accountants in applyling the AML regime.

The guidelines clarify that the operational solutions suggested are the fruit of interpretative orientations developed in the absence of specific indications from the competent authorities. Thus, should the authorities issue official interpretations on specific points, the guidelines will be adapted accordingly. As a self-regulatory organization, the Council has produced a form, annexed to the guidelines, to facilitate performance of the obligations of risk assessment and customer due diligence.

Lawyers' Council

On 20 September 2019 the National Lawyers' Council too issued technical rules on procedures and methodology for assessment of the risk of money laundering and financing of terrorism, internal controls, customer due diligence, including simplified due diligence,

[99] For greater detail, see UIF *Annual Report for 2018*, Section 9.2.2.

[100] Legislative Decree 231/2007, Article 11(2).

and record-keeping, after obtaining the favourable opinion of the Financial Security Committee (see UIF *Annual Report for 2018*, Section 9.2.2.*)*.

10. RESOURCES AND ORGANIZATION

10.1. Organization

The UIF is headed by the Director, who is assisted by the Deputy Director and by a number of staff managers. It is organized into two Directorates: the Suspicious Transactions Directorate, for the financial analysis of suspicious transaction reports, and the Analysis and Institutional Relations Directorate, for legislation, analysis of financial flows and cooperation with the judiciary and other domestic and foreign authorities.

The Director is also assisted by the Advisory Committee for the Review of Irregularities, an internal collegial body charged with making proposals with regard to the initiation of sanction procedures, the transmission of reports to sectoral supervisory authorities, judicial authorities and investigative bodies, and any other action deemed necessary in respect of the irregularities detected.

A Committee of Experts has been established, composed of the Director of the UIF and four experts appointed for three years by decree of the Minister for Economy and Finance, after hearing the Governor of the Bank of Italy. The Committee is an invaluable forum for discussion, providing constant support for the Unit's activities and insights into the most important issues.

The reorganization of the UIF decided in 2019 was implemented in January 2020. The top management of each directorate has been strengthened by the creation of a Deputy Head; three new divisions have been created and two operating sectors eliminated.

Within the Suspicious Transactions Directorate, an additional Report Analysis Division was formed in order to improve supervision and better distribute the increased workload, and a Special Sectors and Anti-Terrorist Financing Division was created, specialized in analysis of STRs relating to virtual currency transactions, money transfer services, payment cards and gaming services. These types of operation are all characterized by the high number and marked fragmentation of transactions and by the interaction of numerous parties, necessitating special analytical methodologies and tools.

The Information Management Division was assigned three sets of tasks. The first comprises collection and analysis of the new threshold-based communications, data processing on STRs and threshold-based communications in support of the other divisions and the Director, extraction and transmission of data on the persons reported to the DNA, design of data quality controls, and, in liaison with the other divisions, formulation of standards and methodologies for risk assessment on suspicious transactions. The second set of tasks involves development and implementation of IT resources, with the support of the IT Department of the Bank of Italy. Lastly, the Division handles contacts with reporting entities, technical support and the management of the database of reporting entities.

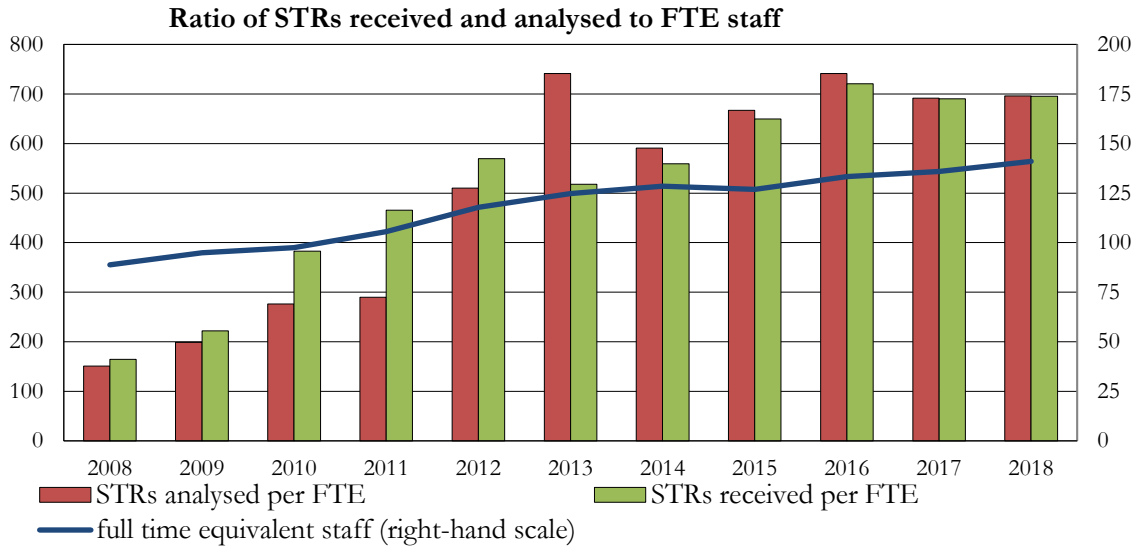
Within the Analysis and Institutional Relations Directorate, the two main activities of the Legislation and Institutional Relations Division (legislative-institutional and inspective-sanction) were separated with the creation of a Division for Inspection Coordination and Analysis of Irregularities.

10.2. Performance indicators and strategic plan

In 2019, the Unit analysed 709 STRs per full-time equivalent employee (FTE), with a significant further improvement of 1.9 per cent in this indicator compared with 2018 (Figure 10.1).

The indicator tends to underestimate the real increase in productivity because it does not take into account the activities carried out by the UIF other than the processing of STRs, which have increased significantly over the years. Counting only the FTE employees assigned to STR analysis, we find a rise of 7.2 per cent in STRs analysed per FTE. Again in 2019, the variation in the indicator reflected an increase in analysed reports that was greater than that in the human resources assigned (8.4 and 1 per cent respectively), which further reduced the backlog: at the end of the year, the number of reports still being processed was down to 46.3 per cent of the average monthly flow.

Figure 10.1



Definition of strategic guidelines

The UIF draws up its strategic action plan every three years. The 2017-19 Strategic Plan focused on three chief axes of action: 1) improving skills, technical equipment, processes and organization to refine the capability for analysis and selection and better contribute to identifying methods of money laundering; 2) increasing information exchange with foreign FIUs and more firmly establishing the UIF's role of initiative in international fora; 3) enhancing the sharing of results also with the broader public of non-specialists in order to increase trust in the preventive apparatus and in intermediaries and other agents as well, helping to foster the perception and sharing of the value of legality in economic activity. The objectives set were all attained (Figure 10.2).

Figure 10.2

Strategic objectives of the UIF and results achieved

	2017 - 2019	References in UIF Annual Report
Effectiveness	✓ Monitoring of efficiency levels ✓ Improvement of techniques and instruments for operational analysis ✓ Proactive analytical approach ✓ Development of a more risk-based operational and strategic analysis	Par. 1.2 - 2.1 - 2.2 - 10.2 Par. 2.2 - 2.4 - 3.1.3 Par. 3.1.2 - 3.2 - 3.3 Par. 1.4 - 2.3 - 2.4 - 2.5 – 3.1.1 - 4.3 – 6.1 – 6.2 - 8.1
Collaboration	✓Promotion of greater involvement of the reporting entities ✓ Launch of an integrated system for exchanging information with the authorities (SAFE) ✓ Cooperation with DNA (National Anti-Mafia and Anti-Terrorism Directorate) ✓ Pursuit of additional forms of co-operation with LEAs and authorities ✓ Greater sharing of information with the other FIUs ✓ Impetus to FIU Platform activity	Par. 1.1 - 1.3 - 2.2 - 3.1.2 Par. 7.1 Par. 2.3 - 2.4 - 2.5 - 3.1.3 - 7.1 - 10.4 Par. 5.1 – 7.1 - 7.3 – 8.7 Par. 4.5 - 8.1- 8.2 Par. 4.5 - 8.1 - 8.3 – 8.4
Organization	✓ Continue with organizational review ✓ Creation of specialist centers of competence ✓ Creation of safety and confidentiality safeguards ✓ Development of advanced IT analytical tools	Par. 10.1 Par. 1.1 - 1.3 - 2.4 - 4.3 - 10.1 Par. 10.4 Par. 6.2 - 10.4
Communication	✓ Increased transparency and accountability ✓ More opportunities to talk with the authorities, operators and members of the civil society	Par. 10.5 Par. 1.1 – 1.3 - 4.4 - 10.5

The strategic guidelines for the Unit were further developed in the course of 2019 to take account of the changing operational environment, with a view among other things to planning the strategy objectives for 2020-2022. The introduction during the year of threshold-based communications on the use of cash requires new tools of analysis to exploit the information and the specific sensitization of reporting entities to the need to improve data quality. In addition, there is the need to expand and systematize the databases available to allow their effective utilization by analysts.

The objective of IT upgrading, which is necessary to adapt analytical capability to rapidly changing criminal contexts, was further refined to shorten implementation times.

The Unit also found it necessary to encourage an improvement in the quality of the STRs submitted by the reporting entities – not only the most recent additions to the system but also certain large entities which, consequent to the reorganization of their AML activity, displayed a deterioration in reporting capacity.

To facilitate the application of the new European rules designed to reinforce information exchange among FIUs, suitable automated procedures for the exchange of cross-border STRs, the matching of massive data, and joint analysis need to be developed.

With a view among other things to complying with international provisions, and notwithstanding heightened regulatory impediments, a priority objective continues to be reinforcing synergy and information exchange with a broad range of domestic authorities and bodies. Strategic analysis must be further developed.

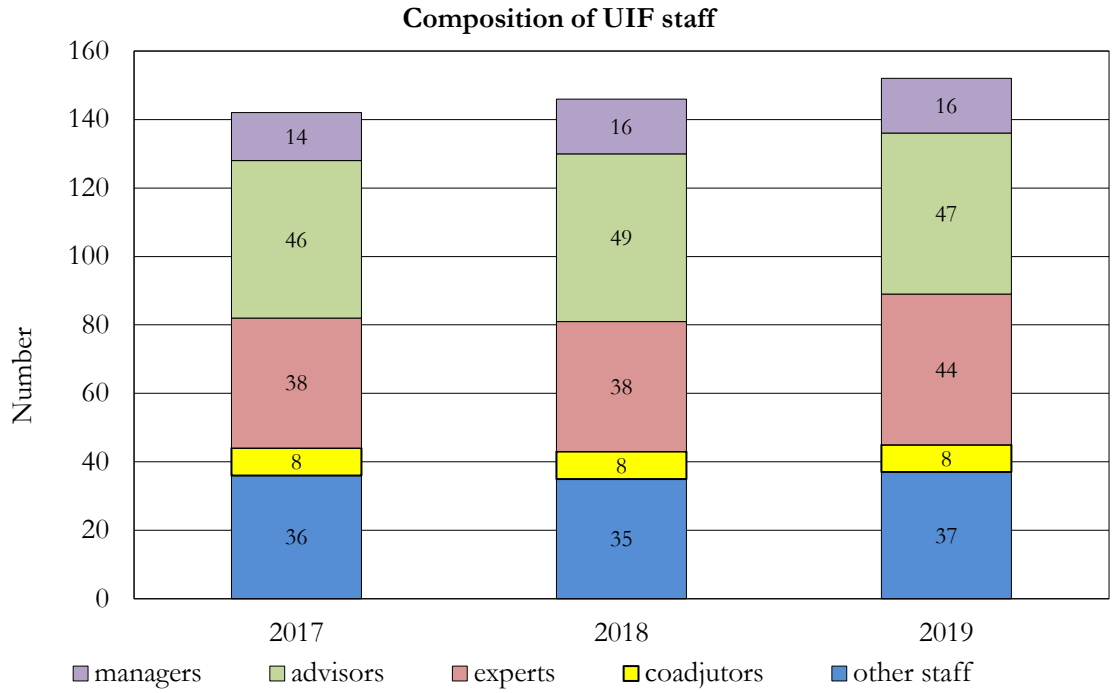
10.3. Human resources

In 2019, the number of staff increased from 146 to 152, following the exit of 12 and the addition of 18 members, of whom 14 new hires and four from other Bank of Italy areas through internal mobility procedures (Figure 10.3). As at 31 December, 88 members of staff were assigned to the Suspicious Transactions Directorate and 61 to the Analysis and Institutional Relations Directorate.

The planned further expansion of human resources by 20 employees in the three years from 2020 through 2022 is intended to make up for the staffing shortfall in 2019 and meet the additional requirement due to the sharply increasing number of STRs and the new duties of the Unit consequent to the AML reforms of the past two years (threshold-based communications, cooperation with the DNA, cross-border STRs, virtual currency operators).

The year saw a considerable increase in staff training, both through in-house seminars (21 in 2019), which involved the entire staff, and through external training events on specific topics of interest to the Unit (17 courses attended by 41 UIF staff members), such as cryptocurrency intelligence, dark web analysis, and forensic analysis of virtual currencies and blockchain technology, with a specific focus on the changing relationship between organized crime and money laundering. Participation in in-house training activities at the Bank of Italy (83 courses for 104 participants) and the ESCB (2 courses for 2 UIF participants) also contributed to the professional growth of the staff in fields of special interest to the Unit.

Figure 10.3



The UIF has adopted a Plan for the prevention of corruption, to assign independent weight to the risk of internal corruption stemming from the performance of its institutional functions. The Plan relates closely, with specific references, to the Bank of Italy's Three-year Corruption Prevention Plan.

The Unit's anti-corruption Plan describes the mechanisms for detecting and mitigating risks, based on prompt and secure management of information, the adaptation of the organizational model, action on IT systems, and the selection and training of human resources.

The UIF designated its corruption prevention officer in 2019.

Starting in mid-March 2020, given the necessity of avoiding the physical presence of employees owing to the risks of the COVID-19 epidemic, work was continued on a remote basis, with no repercussions on productivity. Indeed, productivity improved, enabling the Unit to handle the further increase in STRs thanks to the remote working instruments that the UIF has had in place for several years now, with the invaluable cooperation of the IT directorates of the Bank of Italy.

10.4. IT resources

Major objectives for the advancement and development of the UIF's technological assets were attained, in line with the Unit's strategic directives for information technology, solidly based on three pillars: security, extension of the information base, and automation of analytical processes.

New version of Infostat-UIF portal

In July the new version of the Infostat-UIF portal was installed, revamping the portal in HTML5 technology, replacing the old Flex framework. The change, intended to improve security on inward and outward information flows, complements the earlier release (at the

end of 2018) of a new two-factor user authentication system ("strong" authentication).[101] The new release also installed a functionality whereby reporting entities can independently download from the Infostat-UIF portal the official print-out of the STRs transmitted in data entry mode.

Feedback flows

Work on the 'Feedback to reporting entities' project continued in 2019. In the spirit of Legislative Decree 90/2017, which emphasized the importance of feedback to the obliged entities on their STRs, the focus was on automating the mode of transmission of information and enhancing the efficiency of the Unit's work processes, while at the same time guaranteeing confidentiality.[102] The first functionality, installed in 2018, involved the automatic transmission of negative outcomes, i.e. the list of STRS requiring no further action.[103] In 2019 alone the procedure produced feedback responses on over 15,800 STRs submitted by more than 450 entities.

Another area for action within the project is the automatic transmission of new types of communications, such as the UIF's feedback forms for the entities submitting the largest volumes of STRs. This feedback offers summary indicators of their activity (the function for automatic generation and transmission of these forms was completed in early 2020).

Threshold-based communications

The reform of 2017 assigned the Unit important new functions, including receiving communications on transactions at risk of money laundering and financing of terrorism identified by obliged reporting entities on the basis of objective criteria defined by the UIF in ad hoc instructions (see Section 1.4, 'Threshold-based communications').

In 2019 the dedicated IT infrastructure for receiving these communications was installed. After a trial phase with selected intermediaries, the new data collection procedure was launched in September. For ready use of the information contained in the threshold-based communications during financial analysis of STRs, the Unit's RADAR platform was adapted to support the process of analysis. Studies were also begun to develop processes for the dissemination of threshold-based communications data and information to the competent investigative bodies.

Exchange of confidential information

The first phase of the project for the exchange of confidential information via the Infostat-UIF portal was completed in the second half of 2019, and the function was released for production on 17 February 2020. This phase made it possible to concentrate all the information exchanges for purposes of further inquiry into STRs and acquisition of supplementary documentation on the Infostat-UIF portal, with its particularly high security safeguards (further strengthened by recent modifications).

The second phase, begun in November 2019, has the objective of standardizing the exchange formats and allowing transmission of structured data. This will ensure a high degree of automation of the exchange processes, with appreciable efficiency gains, lower costs for the obliged reporting entities and improvements in the quality and usability of the information for the UIF. Precisely to enable intermediaries to curb costs and shorten the time

---

[101] For access to the portal, the user must supply, in addition to username and password, a one-time password (OTP) received via SMS on a specially notified cellphone number.

[102] The project envisages that data can be transmitted not only by certified email but also through the platform used by the reporters to send their STRs, thus taking advantage of an existing IT channel with its attendant security safeguards.

[103] These are STRs which, considering the inquiry conducted by the Unit and feedback from the investigative bodies, lack sufficient supporting evidence of the suspected money laundering or terrorist financing.

required for developing IT procedures, the Unit has long been collaborating with the Revenue Agency, with which it has agreed to extend the data scheme envisaged for the 'Financial investigations' project, to be used as a vehicle also for information exchange with the UIF.

Improved personal data matching

The revision of the algorithms used by the procedures for matching names among the various UIF databases was completed in February 2019, so as to offer analysts a unified picture of all the activities of each person.

To adapt to technological advances in this field, the Unit also completed its study of a new, improved system for matching names. The new system will also improve the processing of names of non-Western persons (which require special techniques of analysis) and more generally enhance the Unit's ability to link different operational contexts by identifying recurrent names and identities.

Managing partner database

Research and development has begun on a project for a new IT procedure to manage the database of the entities which for various reasons are required to transmit information to the UIF. The objectives include instituting a simpler process for registering name changes of reporters, automating various procedures for verification and updating that are now handled manually, and improving the way the system handles connections among different reporters (e.g. membership of the same group, mergers and acquisitions).

New process for sending STRs for some types of reporting entities

In August 2019 the UIF' completed its project to develop new reporting modalities for operators in the payment card and gaming sectors. The objective, following a similar project directed to the money transfer sector in 2016, is to ease the reporting burden for these operators, whose business requires them to report on a large number of persons, transactions and accounts. The project should make it easier to fill out the STRs in data entry mode through acquisition of a file conforming to a standardized layout. In light of the amendments introduced by Legislative Decrees 90/2017 and 125/2019, which added virtual currency and digital wallets service providers to the list of obliged entities, and considering the specific characteristics of this sector, the project has been extended so as to facilitate reporting by these operators as well.

In October and November 2019 the new data layout was presented to the entities in these sectors making the most reports. A fruitful dialogue with these operators (who displayed considerable interest in the initiative) made it possible to refine and optimize the layout and the upload function, which were made available on 30 January 2020

New controls on STRs

In January 2020 changes were released for the Infostat-UIF portal to yield a more accurate representation of the transactions described in the STRs and improve the quality of the data transmitted. Unlike the previous controls, which in case of divergences always blocked the acquisition of the report, in the case of minor reporting incongruities the new procedure acquires the data transmitted and notifies the incongruity to the reporter, which, where appropriate, may send a replacement report.

Information exchanges with the DNA

Under a memorandum of understanding signed in 2018, the project for the progressive automation of information exchange with the DNA and for the gradual integration of the return flows with the Unit's analysis platform proceeded. The project employs cryptographic techniques which, as is required by law, guarantee the confidentiality of the personal data exchanged.

Automatic classification of reports

The trial stage has begun on a joint project with the IT Department of the Bank of Italy for implementation of machine learning and deep learning algorithms directed to construc-

tion of forecasting models capable of automatic classification of suspicious transaction reports. The project forms part of the broader search for technological solutions to support the UIF in the analysis of STRs.

The project is based on supervised algorithms.[104] The training of the algorithms is effected in a 'secure' IT environment (called a 'Blind Learning Environment') which thanks to ad hoc technological solutions allows the specialized staff of the IT Department to test the classification techniques without directly accessing the confidential contents of the reports.

SAFE Evolution

The steady increase in information exchanges with foreign FIUs requires reducing the residual areas of manual data processing to the minimum, which will also result in quicker dissemination to the competent Italian investigative bodies. Further enhancement of the efficiency of the UIF's work processes can come from completion of the 'SAFE Evolution' project, in course of realization. This will allow automatic interaction between the Unit's internal SAFE system for managing information exchanges with investigative bodies, judicial authorities and foreign FIUs and the secure communication infrastructures used by foreign FIUs for international information exchange (Egmont Secure Web and FIU.NET). However, there are still problems that can only be resolved in the competent international fora, such as the incomplete standardization of the information flows sent by partner FIUs.

10.5. External communication

The UIF is increasingly engaged in a dialogue with the public at large and all other entities and institutions involved in preventing and combating money laundering and the financing of terrorism.

The content of the *Annual Report*, in which the UIF gives an account of its activities to the Government, to Parliament and to the general public, is officially presented every year to representatives of the institutions, financial intermediaries, operators and the professions at a public meeting. The Annual Report is available in English and Italian on the UIF website.

The *Hearing of the Director of the UIF* at the joint session of the Justice Committee, the Finance Committee, and the European Policies Committee of the Chamber of Deputies and the Justice, Finance and Treasury and EU Policies Committees of the Senate of the Republic of the 18th legislature, held in September 2019, focused on certain provisions of the government's draft revision of the AML decree with respect to the principles of the Fourth and Fifth Directives and the vulnerabilities of the system due to the spread of new technologies. The *Hearing of the Director of the UIF* before the Committee on 'Criminal influence and control of activities connected with various forms of gaming', as part of the Parliamentary committee of inquiry into mafias and other criminal organizations, foreign as well as Italian, was held in December 2019. The Director described the UIF's activity in combating economic crime and money laundering, especially in the gaming sector, and offered some remarks on the recent modifications of the legislative framework for the system of prevention and on some provisions that could be improved.

[104] These are algorithms which for proper use must undergo preliminary 'training' to analyse a given domain of interest through observation of a large number of 'examples' (that is, expected inputs and outputs of the algorithm itself). The training thus serves to teach the algorithm how to process the data of interest automatically and in the manner desired (synthesized from the examples used in training).

The *UIF's website* reports the changes that have taken place; alongside a description of the work carried out, it gives an overview of the Italian and international AML-CFT system, with comprehensive and up-to-date information on regulatory and institutional aspects, initiatives and further research. The *UIF Newsletter* began publication in 2019, offering brief updates on the Unit's activity and on anti-money laundering issues in general.

The UIF continues in its compilation of *Quaderni dell'antiriciclaggio*, a series of notebooks on AML topics divided into the series 'Statistics' and 'Analysis and studies', published on the Unit's website. The first series, published every six months, contains statistics on STRs, SARA aggregated data and gold declarations, plus a summary of the UIF's activities. The second, launched in March 2014, gathers contributions on the subject of money laundering and the financing of terrorism. Three studies were published in 2019: on the impact of AML inspections on the banks' reporting of suspicious transactions (*Quaderno No. 12)*; on the use of cash in Italy (*Quaderno No. 13*); and on SupTech applications for anti-money laundering (*Quaderno No. 14*).

In 2019, the UIF took part in conferences, seminars and meetings to increase awareness and understanding among the public and various classes of operators, and to work further with other authorities on the issues involved in money laundering and the financing of terrorism. In particular, the UIF sent speakers to 66 education and training initiatives for the benefit of other authorities and trade associations, at both national and international level. The most important events include the courses organized by the Magistracy School in Caltanisetta, the school for training officials at the Presidency of the Council of Ministers, the Central Operational Service of the State Police and the Anti-Drug Services Directorate of the Ministry of the Interior. The Unit also collaborated on a series of lessons and workshops at the Superior Institute of Investigative Techniques of the Carabinieri and the Ancona Public Prosecutor's Office; cooperation continued with a number of universities as well, in particular with Bocconi University in Milan and the University of Siena. New training initiatives involving associations of professionals and representatives of local authorities (municipalities and regions) were also launched.

GLOSSARY

Accredited entities and agents

Pursuant to Article 1(2)(nn) of Legislative Decree 231/2007, they are accredited operators or agents, of any kind, other than the financial agents listed on the register under Article 128-quater, paragraphs 2 and 6 of the TUB, used by payment service providers and electronic money institutions, including those with their registered office and head office in another Member State, to carry out their activities on Italian national territory.

Administrations and bodies concerned

Pursuant to Article 1(2)(a) of Legislative Decree 231/2007, they are the bodies responsible for supervising obliged entities not supervised by the relevant authorities, namely government departments, including tax offices, those with powers of inspection or authorized to grant concessions, authorizations, licenses or other permits, of any kind, vis-à-vis obliged entities, and the bodies responsible for verifying the possession of the requisites of professionalism and integrity, under the relevant sectoral rules. For the exclusive purposes set out in this Decree, the definition of administrations concerned includes: the Ministry of Economy and Finance as the authority responsible for supervising auditors and audit firms with no mandate to audit public-interest bodies or bodies under an intermediate regime, and the Ministry of Economic Development as the authority responsible for the supervision of trust companies not listed in the register under Article 106 of the TUB.

Anti-Mafia Investigation Department (Direzione Investigativa Antimafia - DIA)

A specialized interforce investigation bureau drawn from various police forces and having jurisdiction over the entire national territory. Set up within the Ministry of the Interior's Department of Public Security by Law 410/1991 this Department has the exclusive task of ensuring coordinated preventive investigations into organized crime, in all of its forms and connections, and of carrying out police enquiries into crimes of mafia-style association or crimes related thereto.

Beneficial owner

Pursuant to Article 1(2)(pp) of Legislative Decree 231/2007, the beneficial owner (or owners) is the natural person, other than the customer, who is the ultimate beneficiary on whose behalf the ongoing relationship is established, the professional service is provided or the transaction is carried out.

Central contact point

Pursuant to Article 1(2)(ii) of Legislative Decree 231/2007, this is a person or department, established in Italy, designated by the electronic money institutions, as defined in Article 2(1)(3) of Directive 2009/110/EC, and by payment service providers, as defined by Article 4(11), of Directive 2015/2366/EC, with their registered office and head office in another Member State, and that operates without a branch office on national territory via accredited entities and agents.

Countries with strategic deficiencies in the fight against money laundering and financing of terrorism identified by the FATF

This group includes countries with weak safeguards against money laundering, as identified by the FATF in public statements that are issued three times a year. Based on these assessments (see *FATF High-Risk Jurisdictions subject to a Call for Action – 21 February 2020* and *Jurisdictions under Increased Monitoring February 2020*), the following countries are not aligned with the legislation for combating anti-money laundering and terrorist financing: Albania, Barbados Bahamas, Botswana, Cambodia, Democratic Republic of Korea, Ghana, Iceland, Iran, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen and Zimbabwe.

Cross-border report

This term refers to suspicious transaction reports received from an EU FIU that concern another Member State and which, pursuant to Article 53 (1) of the Fourth Directive, must be forwarded promptly to the relevant counterparties. These reports are identified based on a methodology developed within the EU FIUs Platform.

Designated entities

Pursuant to Article 1 (1) (l) of Legislative Decree 109/2007 designated entities means natural persons, legal persons, groups and entities designated as being subject to fund freezing based on EU regulations and national legislation.

Digital portfolio service providers

Pursuant to Article 1(2)(ff-bis) of Legislative Decree 231/2007, these are defined as natural or legal persons that provide to third parties, on a professional basis, including online, private cryptographic key safeguarding services on behalf of their own customers, for the purpose of holding, memorizing and transferring virtual currencies.

Egmont Group

An informal body set up in 1995 by a group of FIUs to further international cooperation and increase its benefits. The number of participating FIUs has grown steadily over time and it became an international organization in 2010, with its Secretariat in Toronto, Canada.

European FIU Platform

An EU body chaired by the European Commission and composed of the EU FIUs. Article 51 of the Fourth AML Directive formally recognized the role of the platform, in operation since 2006, and described its mandate in terms of developing stronger cooperation, exchanging opinions, and providing assistance in matters relating to the implementation of EU rules that apply to FIUs and reporting entities.

Financial Action Task Force (FATF)

An intergovernmental body set up within the OECD to devise and promote strategies to combat money laundering and the financing of terrorism at national and international level. In 1989, it issued 40 recommendations on monitoring money laundering, to which nine special recommendations were subsequently added on the financial fight against international terrorism. This area was fully reviewed in 2012, with the issuance of 40 new recommendations. The FATF also promotes the extension of anti-money laundering and counter-terrorism measures beyond the OECD's membership by cooperating with other international organizations and conducting inquiries into emerging trends and money laundering typologies.

Financial Intelligence Unit (FIU)

A central, national unit tasked, for the purpose of combating money laundering and the financing of terrorism, with receiving and analysing suspicious transaction reports and other information relevant to money laundering, the financing of terrorism and their predicate crimes, and disseminating the results of such analyses. Depending on the choices of national legislatures, the FIU may be an administrative authority, a specialized structure within a police force, or part of the judicial authority. In some countries, a mix of these models has been adopted.

Financial Security Committee (FSC)

Pursuant to Article 3 of Legislative Decree 109/2007, this is a committee established at the Ministry of Economy and Finance (MEF), chaired by the Director General of the Treasury, composed of 15 members and their respective delegates, appointed by MEF decree, upon designation by the Minister of the Interior, the Minister of Justice, the Minister of Foreign Affairs and International Cooperation, the Minister of Economic Development, the Bank of Italy, Consob, Isvap (now Ivass) and the Financial Intelligence Unit. The Committee also includes an official in the service of the Ministry of Economy and Finance, an officer from the Guardia di Finanza (Finance Police), a manager or police officer of an equivalent rank under Article 16 of Law 121/1981, in the service of the Anti-Mafia Investigation Department, an officer of the Carabinieri, a manager of the Cus-toms and Monopolies Agency and a magistrate from the National Anti-Mafia Directorate. For asset freezes, the Committee shall be supplemented by a representative of the State Property Agency. The entities represented on the FSC shall communicate to the Committee, even derogating from official secrecy, the information in their possession relevant to matters within the Committee's remit. In addition, the judicial authorities shall forward any information deemed useful for combating the financing of terrorism and the proliferation of weap-ons of mass destruction. The entry into force of Legislative Decree 231/2007 extended the Committee's remit,

initially limited to coordinating action against the financing of terrorism, and to the fight against money laundering (See Article 5(3) of Legislative Decree 231/2007 previously in force, which now corresponds to Article 5, paragraphs 5, 6 and 7).

Financing of terrorism

Under Article 1(1)(d) of Legislative Decree 109/2007, the financing of terrorism is any activity directed, by whatever means, to the supply, intermediation, deposit, custody or disbursement of funds or economic resources, however effected, which are destined, in whole or in part, to be used for the commission of one or more crimes for the purposes of terrorism as specified in the Penal Code, regardless of the actual utilization of the funds or economic resources for the commission of such crimes.

Financing of weapons of mass destruction proliferation programmes

Under Article 1(1)(e) of Legislative Decree 109/2007, the financing of weapons of mass destruction proliferation programmes means the provision or collection of funds and economic resources, by any means, directly or indirectly instrumental in supporting or promoting all activities linked to the creation or carrying out of programmes to develop nuclear, chemical or biological weapons.

FIU.NET

A decentralized communication infrastructure for the Financial Intelligence Units of the European Union, permitting a structured, multilateral exchange of information, with standardized applications and immediate and secure information exchanges.

Freezing of funds

Pursuant to Article 1(1)(b) of Legislative Decree 109/2007, and in accordance with EU regulations and national legislation, this is a prohibition of the movement, transfer, modification, use or management of or access to funds, in such a way as to modify their volume, amount, collocation, ownership, possession, nature, purpose or any other change allowing for the use of the funds, including portfolio management.

General government entities

Pursuant to Article 1(2)(hh) of Legislative Decree 2007 these are general government entities under Article 1(2) of Legislative Decree 165/2001 and subsequent amendments, national public bodies, and companies owned by general government entities and their subsidiaries, pursuant to Article 2359 of the Italian Civil Code, limited to their activities of public interest governed by national law or by the European Union, as well as subjects responsible for tax collection at national or local level, regardless of the legal form.

High-risk third countries

Pursuant to Article 1(2)(bb) of Legislative Decree 231/2007, these are non-EU countries with strategic deficiencies in their national AML/CFT systems, as identified by the European Commission through its delegated Regulation (EU) 2016/1675 and subsequent amendments, in the exercise of its powers under Articles 9 and 64 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 as amended by Directive (EU) 2018/843.

Means of payment

Pursuant to Article 1(2)(s) of Legislative Decree 231/2007, means of payment are cash, bank and postal cheques, bankers' drafts and the like, postal money orders, credit transfers and payment orders, credit cards and other payment cards, transferable insurance policies, pawn tickets and every other instrument available making it possible to transfer, move or acquire, including by electronic means, funds, valuables or financial balances.

Money laundering

Article 648-bis of the Penal Code makes punishable for the crime of money laundering anyone who, aside from cases of complicity in the predicate crime, 'substitutes or transfers money, assets or other benefits deriving from

a crime other than negligence, or who carries out other transactions in relation to them in such a way as to hamper the detection of their criminal provenance.' Article 648-ter makes punishable for illegal investment anyone who, aside from the cases of complicity in the predicate crime and the cases specified in Article 648 and 648-bis, 'invests in economic or financial assets moneys, goods or other assets deriving from crime.'
Pursuant to Article 2(4) of Legislative Decree 231/2007, the following actions, if performed intentionally, constitute money laundering: (a) the conversion or transfer of property, carried out knowing that it constitutes the proceeds of criminal activity or of participation therein with the aim of hiding or dissimulating the illicit origin of the property or of helping any individual involved in such activity to avoid the legal consequences of his or her actions; (b) hiding or dissimulating the real nature, origin, location, arrangement, transfer or ownership of property or rights thereto, carried out in the knowledge that they constitute the proceeds of criminal activity or of participation therein; (c) the acquisition, detention or use of property, knowing at the time of receiving it that it constitutes the proceeds of criminal activity or of participation therein; and (d) participation in one of the actions referred to in the preceding subparagraphs, association with others to perform such actions, attempts to perform them, the act of helping, instigating or advising someone to perform them or the fact of facilitating their performance.

Moneyval (Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism)

Moneyval is a subcommittee of the European Committee on Crime Problems (CDPC) of the Council of Europe, established in September 1997. It serves as the Council's unit on money laundering, also taking account of FATF measures and making specific recommendations to the member states. It evaluates the anti-money laundering measures adopted by Council of Europe member countries that are not FATF members. As a regional group, it has the status of Associate Member of the FATF. Under a thoroughly revised statute, Moneyval has served since January 2011 as an independent monitoring body of the Council of Europe in the fight against money laundering and the financing of terrorism; it reports directly to the Committee of Ministers, to which it submits an annual report.

National Anti-Corruption Authority (Autorità Nazionale Anticorruzione - ANAC)

Under Article 19 of Decree Law 90/2014, converted with amendments into Law 114/2014, this authority took over the functions and resources of the former authority for the supervision of public works, service and supply contracts (AVCP). The Authority is responsible for preventing corruption within general government, in state-owned, controlled and participated companies, also by implementing transparency in all management aspects, as well as through supervision activities for public contracts, appointments in any sector of public administration that could potentially be subject to corruption, while avoiding the aggravation of proceedings with negative consequences for citizens and businesses, by guiding the behaviour and activities of public employees, with interventions in advisory and regulatory settings, as well as through fact-finding activities.

National Anti-Mafia Directorate (Direzione Nazionale Antimafia - DNA)

The DNA, established as part of the General Prosecutor's Office at the Court of Cassation by Legislative Decree 367/1991, converted with amendments into Law 8/1992, has the task of coordinating the investigation of organized crime at national level. The jurisdiction of the DNA was extended to cover terrorism proceedings, including international ones, with Legislative Decree 7/2015, converted with amendments into Law 43/2015. Pursuant to Article 103 of Legislative Decree 159/2011, the DNA is managed by one magistrate with the functions of a national Public Prosecutor and two magistrates with functions of deputy prosecutors, together with magistrates that can substitute them, chosen from among those who have performed, also not continuously, the functions of a public prosecutor for at least ten years and that have specific aptitudes, organizational skills and experience in handling proceedings involving organized and terrorism-related crime.

Non-cooperative countries for tax purposes identified by the European Union

The following are on the EU list of non-cooperative jurisdictions for tax purposes: American Samoa, Cayman Islands, Fiji, Guam, Oman, Palau, Panama, Samoa, Seychelles, Trinidad and Tobago, US Virgin Islands, Vanuatu (*Council Conclusions 2020(C64/03, 27 February 2020).*

Office of Foreign Assets Control (OFAC)

This is an Office of the US Treasury Department, set up under the auspices of the State Secretary for the

Treasury for terrorism and financial intelligence. The OFAC administers and enforces economic and trade sanctions, based on US foreign and security policy, against foreign nations, organizations and individuals.

Organization of Agents and Mediators (OAM)

Pursuant to Article 1(1)(q) of Legislative Decree 231/2007, this Organization is responsible for managing the lists of financial agents and loan brokers, pursuant to Article 128-undecies of the TUB (Consolidated Law on Banking). The OAM also holds: i) the currency exchange register, which has a special section for providers of virtual currency services (Article 17-bis, paragraph 8-bis, Legislative Decree 141/2010, added by Legislative Decree 90/2017 and amended by Article 5(1)(a) of Legislative Decree 125/2019; ii) the register of entities and agents under Article 45 of Legislative Decree 231/2007; and iii) the register of cash-for-gold traders under Article 1(1)(q) of Legislative Decree 92/2017.

Politically exposed persons

Pursuant to Article 1(2)(dd) of Legislative Decree 231/2007, these are natural persons that currently hold, or held important public offices up until less than one year ago, together with their immediate family members or persons known to be their close associates, and are listed as follows: 1) natural persons that hold or have held important public offices and are or have been: 1.1 President of the Italian Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, Regional President, Mayor of a provincial capital or metropolitan city, Mayor of a town with a population of at least 15,000, and similar positions in foreign countries; 1.2 a Member, Senator, Member of the European Parliament, regional councillor and similar posts in foreign states; 1.3 a member of the central governing bodies of political parties; 1.4 a Constitutional Court judge, a magistrate of the Court of Cassation or the Court of Auditors, a State Councillor or other component of the Administrative Justice Council for the region of Sicily, and similar positions in foreign countries; 1.5 a member of the decision-making bodies of central banks and independent authorities; 1.6 an ambassador, chargé d'affaires or equivalent positions in foreign states, high-ranking officers in the armed forces or similar ranks in foreign countries; 1.7 a member of the administrative, management or supervisory bodies of enterprises owned, also indirectly, by the Italian State or by a foreign State or owned, mainly or totally, by the regions, provincial capitals and metropolitan cities and by towns with a total population of not less than 15,000 inhabitants; 1.8 a general manager of an ASL (Local Health Authority) or a hospital or university hospital or other national health service entities; and 1.9 a director, deputy director, member of a management board or a person with an equivalent role in international organizations; 2) family members of PEPs include: the parents, the spouse or any person considered by national law as equivalent to the spouse, the children and their spouses or partners considered by national law as equivalent to the spouse; 3) persons who are known to be close associates of politically exposed persons include: 3.1 natural persons linked to PEPs because they have joint beneficial ownership of legal entities or other close business relationships; and 3.2 natural persons that only formally hold total control of an entity known to have been set up for the de facto benefit of a PEP.

Sectoral supervisory authorities

Pursuant to Article 1(2)(c) of Legislative Decree 231/2007, the Bank of Italy, Consob and Ivass are the authorities responsible for supervising and checking banking and financial intermediaries, auditors and audit firms with mandates to audit public-interest entities and entities under an intermediate regime. The Bank of Italy supervises and checks non-financial operators with cash-in-transit and valuable items transport companies that employ private security guards, and that have a licence under Article 134 of the TULPS (Consolidated Law on Public Security), limited to the handling of euro banknotes, and included on the list under Article 8 of Decree Law 350/2001, converted with amendments into Law 409/2001.

Self-laundering

Pursuant to Article 648-ter.1 of the Penal Code, 'whoever, having committed or attempted to commit a crime with criminal intent, uses, replaces or transfers money, assets or other utilities deriving from the commission of such a crime to economic, financial, entrepreneurial or speculative activities, in such a way as to actively hinder detection of their criminal origin' shall be punished for the crime of self-laundering. This rule was introduced by Article 3(3) of Law 186/2014.

Self-regulatory body

Pursuant to Article 1(2)(aa) of Legislative Decree 231/2007, this is a body that represents a professional category, including its various branches and the disciplinary boards on which the current legislation confers regulatory powers, supervisory powers, including checking compliance with the rules governing the exercise of the profession and the powers to impose, via the mechanisms in place for this purpose, the sanctions applicable for the violation of such rules.

Special Foreign Exchange Unit (Nucleo Speciale di Polizia Valutaria - NSPV)

Established within the Finance Police (Guardia di Finanza), this unit combats money laundering, both as an investigative police body and as the administrative body responsible, together with the Bank of Italy and the Anti-Mafia Investigation Department, for controls on the financial intermediation sector. It has special powers conferred by the law relating to foreign exchange regulations on the Unit's members, as well as those concerning fiscal powers.

Standardized archives

The files that make available the data and information envisaged in the provisions issued by the competent sectoral supervisory authorities pursuant to Article 34(3) of Legislative Decree 231/2007, in accordance with the technical standards and the analytical details referred to therein. They include the Single Electronic Archives (AUIs) already set up on the date of the entry into force of Legislative Decree 90/2017.

Tax havens and/or non-cooperative countries and territories

The blacklist of jurisdictions included in the decree of the Minister of Finance of 4 May 1999 (most recently amended by the ministerial decree of 12 February 2014) is as follows: Andorra, Anguilla, Antigua and Barbuda, Aruba, the Bahamas, Bahrein, Barbados, Belize, Bermuda, Bonaire, the British Virgin Islands, Brunei, the Cayman Islands, the Cook Islands, Costa Rica, Curaçao, Djibouti, Dominica, Ecuador, French Polynesia, Gibraltar, Grenada, Guernsey (including Alderney and Sark), Hong Kong, the Isle of Man, Jersey, Lebanon, Liberia, Liechtenstein, Macao, the Maldives, Malaysia, the Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Niue, Oman, Panama, the Philippines, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, the Seychelles, Singapore, Sint Eustatius and Saba, Sint Maarten (the Dutch part only), Switzerland, Taiwan, Tonga, the Turks and Caicos Islands, Tuvalu, the United Arab Emirates(Abu Dhabi, Ajman, Dubai, Fuijayrah, Ras El Khaimah, Sharjah and Umm Al Qaiwain), Uruguay and Vanuatu.

Trade-based money laundering

The term refers to the process of concealing the proceeds of crime and of transferring value through commercial transactions to seek to legitimize the illicit origin of such transactions.

Virtual asset service providers

Pursuant to Article 1(2)(ff) of Legislative Decree 231/2007, they are natural or legal persons that, as a business, provide third parties with services which are functional to the use, exchange and safekeeping of virtual currencies and their conversion from or into legal tender currencies or digital representations of value, including those convertible into other virtual currencies, as well as issuance, offering, transfer and clearing services and every other service functional to acquisition, trading or intermediation in the exchange of such currencies.

Virtual currency

Pursuant to Article 1(2)(qq) of Legislative Decree 231/2007, a virtual currency is a digital representation of value, not issued by a central bank or a public authority, not necessarily linked to a currency that is legal tender, and used as a medium of exchange for purchasing goods and services or for investment purposes, and transferred, stored and traded electronically.

ACRONYMS AND ABBREVIATIONS

ANAC	National Anti-Corruption Authority (Autorità Nazionale Anticorruzione)
ATM	Automated Teller Machine
AUI	Single Electronic Database (Autorità Unico Informatico)
CASA	Anti-Terrorism Strategic Analysis Committee (Comitato di Analisi Strategica Antiterrorismo)
CDP	Cassa Depositi e Prestiti spa.
CIFG	Counter-ISIL Finance Group
CNDCEC	National Council of Accountants and Bookkeepers (Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili)
CNF	National Lawyers' Council (Consiglio Nazionale Forense)
CNN	National Council of Notaries (Consiglio Nazionale del Notariato)
CONSOB	Companies and Stock Exchange Commission (Commissione Nazionale per le Società e la Borsa)
DDA	Anti-Mafia District Directorate (Direzione Distrettuale Antimafia)
DIA	Anti-Mafia Investigation Department (Direzione Investigativa Antimafia - DIA)
DNA	National Anti-Mafia Directorate (Direzione Nazionale Antimafia e Antiterrorismo)
ECB	European Central Bank
EMI	Electronic Money Institution
EU	European Union
FATF	Financial Action Task Force
FSC	Financial Security Committee
FIU	Financial Intelligence Unit
IRPEF	Personal income tax
ISIL	Islamic State of Iraq and the Levant
IVASS	Insurance Supervisory Authority (Istituto per la Vigilanza sulle Assicurazioni)
MEF	Ministry of Economy and Finance
NRA	National Risk Assessment
NSPV	Special Foreign Exchange Unit of the Finance Police (Nucleo Speciale di Polizia Valutaria della Guardia di Finanza)
OAM	Organization of Agents and Mediators (Organismo degli Agenti e dei Mediatori)
OECD	Organization for Economic Cooperation and Development

PI	Payment Institution
PEP	Politically Exposed Person
RADAR	Collection and Analysis of AML Data (Raccolta e Analisi Dati AntiRiciclaggio)
SARA	Aggregate AML Reports (Segnalazioni AntiRiciclaggio Aggregate)
SGR	Asset management company
SICAF	Fixed capital investment company
SICAV	Open-ended investment company
SIM	Securities investment firm
STR	Suspicious Transaction Report
TUB	Consolidated Law on Banking (Testo Unico Bancario – Legislative Decree 385/1993).
TUF	Consolidated Law on Finance (Testo Unico della Finanza – Legislative Decree 58/1998).
TUIR	Consolidated Law on Income Tax (Presidential Decree 917/1986)
TULPS	Consolidated Law on Public Security (Royal Decree 773/1931).
UIF	Italy's Financial Intelligence Unit (Unità di Informazione Finanziaria)
UNCAC	United Nations Convention against Corruption
VAT	Value Added Tax
VD	Voluntary Disclosure