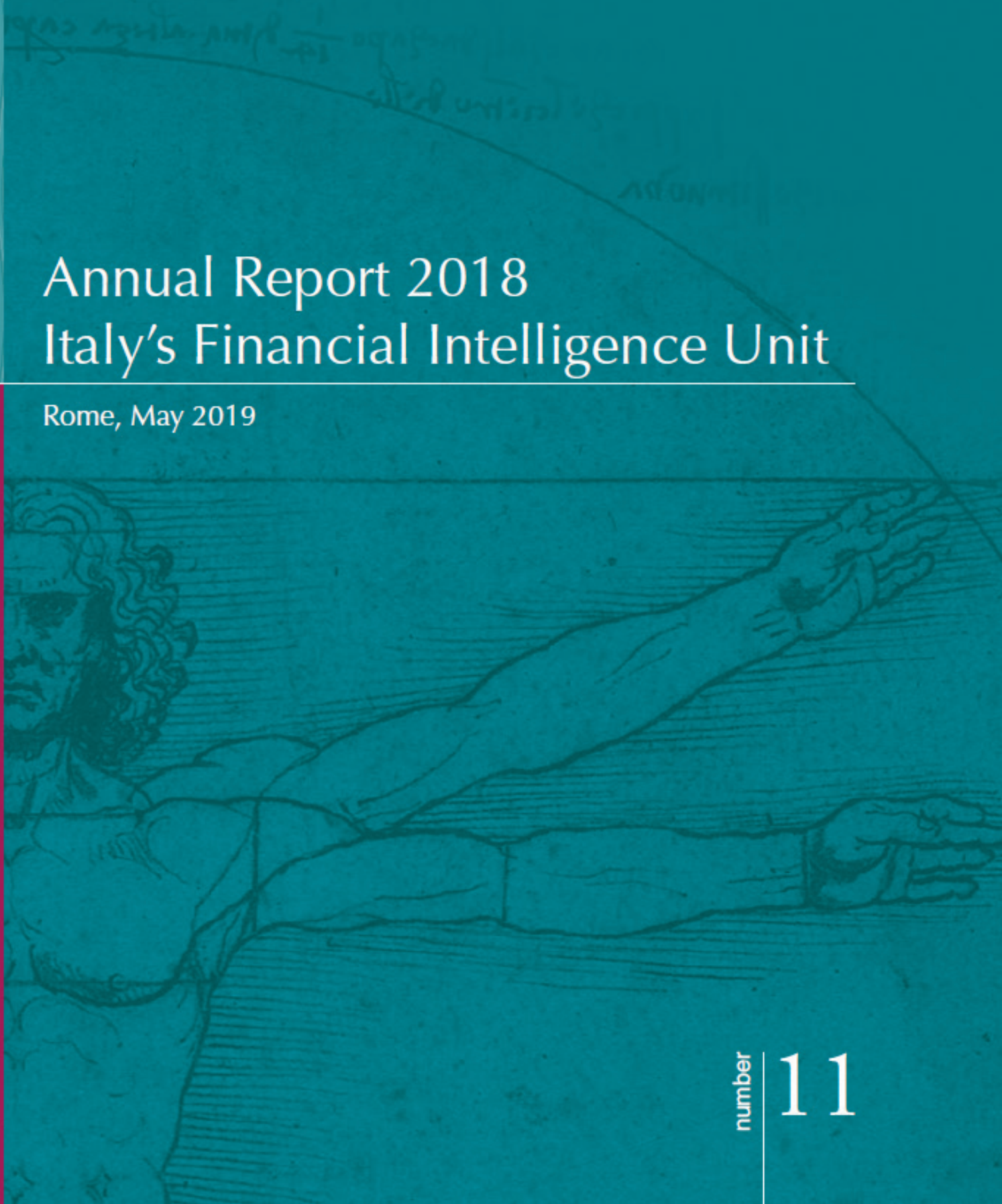
BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2018
Italy's Financial Intelligence Unit

Rome, May 2019



year 2018

number 11

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2018
Italy's Financial Intelligence Unit

Rome, May 2019

The Unità di Informazione Finanziaria per l'Italia (UIF) is the central national body charged with combating money laundering and the financing of terrorism. It was set up at the Bank of Italy pursuant to Legislative Decree 231/2007, in compliance with international rules and standards requiring each country to institute its own financial intelligence unit, independently run and operating autonomously.

The UIF 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 these data with the sources and 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 the supervisory authorities, government departments and professional bodies. The Unit works 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 tackle cross-border money laundering and the financing of terrorism.

Bank of Italy, 2019

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

Active collaboration continued to grow in 2018. The increase in reports of suspicious transactions (more than 98,000, of which more than 1,000 on suspicion of financing of terrorism) has required the continuous refinement of processes and approaches to ensure timeliness and accurate analyses.

The progressive diversification in types of reporting entities and the increase in their numbers (currently over 6,200) has led the UIF to seek methodologies for differentiated analysis in order to make the best possible use of contributions from active cooperation, including from non-banking sources. The use of behavioural models and aggregate analyses has increased further, especially in areas such as money transfers, where the individual transactions reported are small in amount but, given their number and frequency, may represent highly risky activities.

The STRs analysed and transmitted to the investigative bodies have exceeded those received, with a further decrease in the already very limited backlog. The results of investigations confirm the usefulness of the analyses carried out, which often led to the launch of particularly important investigations, including on corruption and organized crime. The Unit has taken a more proactive approach in exercising its power to suspend suspicious transactions, which has been initiated ex officio in a number of cases.

Relations with the Public Prosecutors' Offices and the investigative bodies have been strengthened with reference to a wide range of criminal offences. The full commencement of exchanges with the National Anti-Mafia and Counter-Terrorism Directorate, introduced by the reform of the anti-money laundering legislation, allows the National Public Prosecutor's Office to obtain useful information quickly to fully exploit its power to take the initiative and to coordinate, and the UIF to acquire significant data on the names reported, which is of great importance to the analysis setting.

Information exchanges with foreign FIUs have increased significantly and are becoming more and more important for further investigation of STRs and for domestic cooperation. At European level, the UIF has promoted and actively participated in carrying out joint analyses with other FIUs on money laundering and the financing of transnational terrorism activities.

The Unit contributed to the international bodies' projects focused on the sharing of experience and best practices, in the belief that this is a prerequisite for effective cooperation between FIUs. The European Commission is currently looking at the establishment of a European FIU Coordination and Support Mechanism, which should consolidate and extend the competences of the current EU FIUs Platform.

The use of the SARA and ORO databases has been even more intensive and systematic in order to develop background analyses and studies, to define risk indicators to support supervisory authorities and to intercept new significant issues.

The UIF worked on and carried out a public consultation of the legislation on the new threshold-based communications, which was enacted in March 2019, after consultation with the Financial Security Committee. These communications will cover cash withdrawals and cash deposits, in view of the widespread use of these instruments in Italy and their importance for the analysis of suspicious transaction reports and of financial flows.

The Unit believes that the public administration's contribution, which is still too low, can be a valuable resource to deepen the analysis of suspicious transactions reports and to identify others that are difficult for the obliged entities to detect. It has therefore updated the specific anomaly indicators and strengthened the training and awareness of public operators, taking advantage of the needs and sensitivities of some regional and municipal authorities as regards protection against criminal infiltration of the local economic fabric

The Unit has worked on understanding and investigating changes in financial markets and their new vulnerabilities. This has meant refining its specialist knowledge of products, tools and threats in order to adequately address the new complexities; discussion spaces have been opened with operators to find out more about the characteristics of emerging sectors and to share methodologies for more effective measures to combat money laundering and the financing of terrorism.

The initial evidence on the risks of virtual currencies in terms of potential uses for criminal purposes has led the UIF to focus on the characteristics of suspicious transactions in crypto-currencies, which have also been reported given the current and future extension of the reporting requirements to the various market players in this sector.

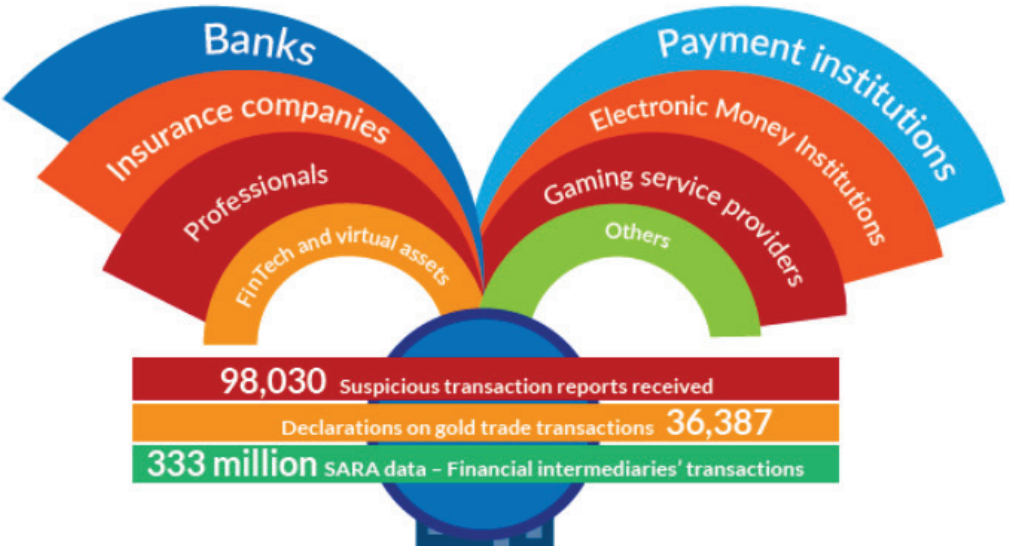
The new morphology of the payment services market, driven by FinTech and the PSD2 Directive, requires further updating of the safeguards and increased awareness. The UIF's strategy focuses on a closer partnership with payment services' operators in order to raise awareness of the associated money laundering risks.

The Unit's strategic choices must keep pace with an increasingly dynamic and innovative reality. Acquiring more human and technological resources and strengthening the available information sources are essential steps. The Unit's organizational reform, to be implemented over the coming months, aims at further enhancing the professional skills of the UIF's staff and stepping up the commitment to combating money laundering and the financing of terrorism.

The Director

Claudio Clemente

Financial analysis



98,030 Suspicious transaction reports received

Declarations on gold trade transactions 36,387

333 million SARA data – Financial intermediaries' transactions

Intelligence, dissemination and controls

UIF

98,117 Suspicious transaction reports analysed

11,881 Money transfer operations reassessed using aggregate analysis

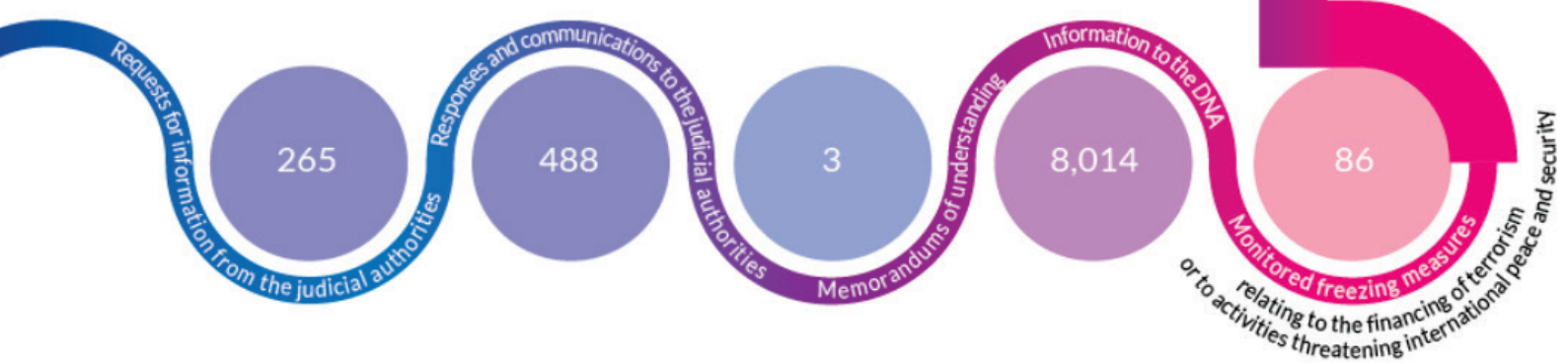
329 Suspicious transactions evaluated for suspension purposes

47 Suspension orders

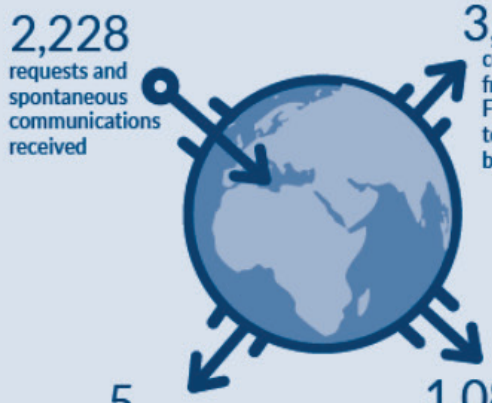
20 Inspections

35 Sanctions procedures

Cooperation with investigative bodies and national authorities



Foreign FIUs



2,228 requests and spontaneous communications received

3,070 communications from foreign FIUs sent to investigative bodies

5 technical assistance activitie

1,082 requests sent to other FIUs

Contributions

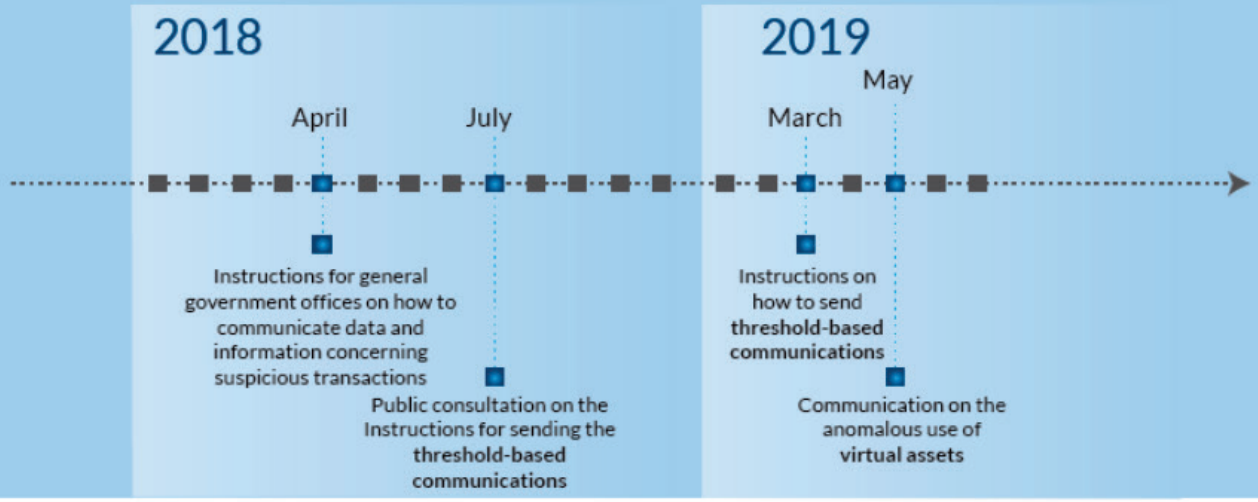
to awareness of money laundering

60 speakers at conferences and workshops on money laundering at universities and other institutions

4 training training interventions at regional bodies and other general government offices

6 publications in the *Quaderni dell'antiriciclaggio* and in scientific reviews

Legislation



IT Infrastructure

- Automation of the feedback flow to reporting entities
- IT system for collecting and using threshold-based communications
- Exchange of confidential information in the Infostat UIF platform
- New ways to send STRs for operators in the payment card, gaming and virtual currency sectors
- Automation of data exchanges with the National Anti-Mafia Directorate

1. ACTIVE COOPERATION

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

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 the foreign FIUs, reconstruct innovative ways to launder money and select those cases with a higher level of risk. The UIF sends data and information to the DNA (the National Anti-Mafia Directorate) in order to detect possible links to criminal contexts and allow for prompt action.

The Unit sends the results of its analyses to the competent law enforcement bodies (the NSPV - Special Foreign Exchange Unit of the Finance Police and the DIA - the Anti-Mafia Investigation Department) 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 Unit uses this body of information to develop anomaly indicators and identify patterns of anomalous behaviour to guide reporting entities in detecting suspicious transactions.

1.1. Reporting flows

In 2018, the Unit received 98,030 suspicious transaction reports (STRs),[1] about 4,200 more than in the previous year (+4.5 per cent; Table 1.1).

Table 1.1

Reports received

	2014	2015	2016	2017	2018
Number of reports	71,758	82,428	101,065	93,820	98,030
Percentage change on previous year	*11.1*	*14.9*	*22.6*	*-7.2*	*4.5*

Following the decrease in the overall reporting, attributable to the gradual fading of the effects of the voluntary disclosure measures to regularize funds held abroad,[2] the number of reports rose again, thanks to the greater contribution of operators in the gaming sector

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

[2] The peak recorded in 2016, with the biggest increase in the number of reports of the last five years (+22.6 per cent), was largely motivated by the effects of the voluntary disclosure introduced by Law 186/2014, as well as the voluntary disclosure bis, provided for in Legislative Decree 193/2016, converted with amendments into Law 255/2016.

(+94.9 per cent) and intermediaries and other financial operators (+20.9 per cent), while reports sent by banks remained essentially steady (-1.5 per cent; Table 1.2).

The reports submitted by the Banks and Poste Italiane SpA category (which from now on will simply be referred to as the 'banks' category) continue to be the main component of the overall total, at 72.5 per cent of the reports received in the year (76.9 per cent in 2017). Intermediaries and other financial operators remain the second category of obliged entities for the contribution of reports, increasing from 14.2 to 16.5 per cent. The number of reports sent by professionals is still limited, relatively speaking (4.9 per cent), while gaming operators reached a percentage of 5.2 per cent, almost twice that of the previous year (2.8 per cent in 2017). Finally, the communications received from general government,[3] which were already very few the previous year, decreased even more in 2018.

Table 1.2

STRs by type of reporting entity

	2017		2018		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2017)*
Total	**93,820**	**100.0**	**98,030**	**100.0**	**4.5**
Banks and Poste Italiane SpA	72,171	76.9	71,054	72.5	-1.5
Financial intermediaries excl. Banks and Poste Italiane SpA	13,347	14.2	16,139	16.5	20.9
Companies managing markets and financial instruments	5	0.0	11	0.0	120.0
Professionals	4,969	5.3	4,818	4.9	-3.0
Non-financial operators	658	0.7	898	0.9	36.5
Gaming service providers	2,600	2.8	5,067	5.2	94.9
General government offices	70	0.1	43	0.0	-38.6

Financial intermediaries other than banks

The increase in the number of reports from financial intermediaries other than banks, in line with the previous year's trend, is once again attributable to the contribution of Electronic Money Institutions (+86.9 per cent, from 1,444 to 2,699 STRs) and of payment institutions and the EU points of contact for payment service providers (+37 per cent, from 6,575 to 9,006 STRs; Table 1.3). The reports sent by Electronic Money Institutions are no longer as concentrated as they were the previous year, as two new operators sent reports. For payment institutions and their points of contact, money transfer operators were the main contributors, having submitted 87 per cent of the reports included in the category, against

[3] As of 4 July 2017, general government is no longer part of 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, listed in Article 10(4) of the abovementioned decree, provide that 'in order to enable financial analyses to be made, aimed at uncovering money laundering and financing of terrorism activities, general government communicates to the UIF any data or information concerning suspicious transactions that come to its attention in the course of its institutional activities (...)'.

79 per cent in 2017. The contribution from money transfer operators offset the lower numbers achieved by the other entities included in the category, which either decreased, as in the case of insurance companies (-11.4 per cent) and trust companies (-43.5 per cent), or displayed minor increases, as in the case of asset management companies, SICAVs and SICAFs (+6.7 per cent).

Table 1.3

STRs by category of banking and financial intermediary

	2017		2018		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2017)*
Banks, intermediaries and other financial operators	**85,518**	**100.0**	**87,193**	**100.0**	**2.0**
Banks and Poste Italiane SpA	**72,171**	**84.4**	**71,054**	**81.5**	**-1.5**
Financial intermediaries excl. Banks and Poste Italiane SpA	**13,347**	**15.6**	**16,139**	**18.5**	**20.9**
Payment Institutions and points of contact of EU payment service providers	6,575	7.7	9,006	10.3	37.0
Insurance companies	2,721	3.2	2,412	2.8	-11.4
Electronic Money Institutions and points of contact of EU Electronic Money Institutions	1,444	1.7	2,699	3.1	86.9
Trust companies - Article 106 of the 1993 Banking Law	1,054	1.2	595	0.7	-43.5
Financial intermediaries – Article 106 of the 1993 Banking Law	781	0.9	799	0.9	2.3
Asset management companies, SICAVs and SICAFs	329	0.4	351	0.4	6.7
Investment firms	62	0.1	60	0.1	-3.2
Intermediaries and other financial operators not included in the previous categories (1)	381	0.4	217	0.2	-43.0

(1) The category includes the entities listed in Article 3(2) and (3), Legislative Decree 231/2007, as amended by Legislative Decree 90/2017, not included in the previous categories.

Professionals

Following the sharp contraction of last year,[4] the category of professionals remained substantially stable (-3 per cent), mainly thanks to the contribution of notaries (+2.9 per cent), which balanced out the decrease in the contribution of other professional groups, mainly lawyers (-62.4 per cent), law firms, law and accounting firms and law practices (-63.5 per cent; Table 1.4).

Notaries continue to submit reports almost exclusively through the National Council of Notaries (CNN) (97.8 per cent). The reports submitted by accountants and bookkeepers showed an increase in those sent through the category's National Council of the Order of

[4] In 2017, the reports submitted by professionals showed a 44 per cent reduction compared with the previous year in relation to the steady decline in applications for activation of the voluntary disclosure procedure.

Accountants and Bookkeepers (CNDCEC) to 72.3 per cent, up from 40.7 per cent in 2017. However, the gradual implementation of this reporting modality has yet to have a significant impact, as shown by the decline in the overall numbers for the category of accountants, bookkeepers and employment consultants (-11.6 per cent, down from 361 to 319).[5] In 2018, both National Councils drew up technical rules aimed at increasing the effectiveness of due diligence and data storage activities, with positive effects expected in terms of active cooperation (see Chapter 9 'The regulatory framework').

Non-financial operators

The number of reports sent by gold manufacturers and traders and retailers of precious stones continued to increase (+72.1 per cent) as did the number sent by cash-in-transit and valuable items transport companies (+9.5 per cent).

Table 1.4

STRs received from professionals and non-financial operators

	2017		2018		
	bsolute va lues)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2017)*
Non-financial obliged entities	**8,227**	100.0	**10,783**	**100.0**	**31.1**
Professionals	**4,969**	60.4	**4,818**	**44.7**	**-3.0**
Notaries and Nat. Council of Notaries	4,222	51.3	4,345	40.3	2.9
Law firms, law and accounting firms and law practices	222	2.7	81	0.8	-63.5
Accountants, bookkeepers and employment consultants	361	4.4	319	3.0	-11.6
Lawyers	101	1.2	38	0.4	-62.4
Auditing firms and auditors	26	0.3	13	0.1	-50.0
Other professional services providers (1)	37	0.4	22	0.2	-40.5
Non-financial operators	**658**	8.0	**898**	**8.3**	**36.5**
Gold traders and manufacturers and retailers of precious stones and metals	251	3.1	432	4.0	72.1
Cash-in-transit and valuable items transport companies	388	4.7	425	3.9	9.5
Other non-financial operators (2)	19	0.2	41	0.4	115.8
Gaming service providers	**2,600**	31.6	**5,067**	**47.0**	**94.9**

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

The share of reports from less consolidated operators such as gaming service and payment service providers has become increasingly important. A debate on organization has been launched which will lead this year to the creation of units specialized in processing

[5] According to the memorandum, the CNDCEC is authorized to receive encrypted STRs from accountants and bookkeepers and to send them in complete and anonymous form to the UIF. This procedure ensures maximum confidentiality with regard to the identity of the reporting entity, thereby preventing the CNDCEC from seeing (or knowing) the content of the reports.

reports from these categories (see Chapter 10 'Resources and organization').

The flow of reports from gaming service providers, which had already grown in 2017, almost doubled (+94.9 per cent, from 2,600 to 5,067 STRs). The main contribution to this trend, displayed by all operators in this category, came from online gaming service providers for which the number of reports rose from 2,292 in 2017 to 4,552 in 2018. STRs submitted by casinos increased as well, to 382 in 2018 from 289 reports the previous year.[6]

Voluntary Disclosure

Reports stemming from the activation of the voluntary disclosure collaboration continued to decrease, from 6,112 to 2,154, representing 2.2 per cent of the total inflow (6.5 per cent in 2017; Table 1.5). The contribution from the banking sector remained clearly prevalent (80.7 per cent), followed by that of insurance companies (7 per cent).

Reporting in the first quarter of 2019

The increase in the number of suspicious transactions reported has continued in 2019 as well. In the first quarter, the UIF received 25,446 reports, 339 more than those received in the same period of 2018.

New reporting entities

The growth in the number of reports received by the UIF was accompanied by a progressive increase in the number of reporting entities, which reached 6,025 obliged entities, including 424 newly registered entities (646 in 2017). In 2018, 24 per cent of the newly registered entities sent at least one report in the first year, compared with 18 per cent in the previous year; in addition, the contribution of the new entities was higher than in 2017, with 1,047 STRs received (427 the year before). The new types of reporting entities show that there is an increasing level of involvement and awareness in sectors other than the already well-established one of financial intermediaries. In line with the previous year, new registration applications mainly involved professionals (253), accountants, bookkeepers and employment consultants (156) and lawyers (40). There were also a significant number of new entities in the category of gold traders (44). The first four registration applications of virtual currencies service providers are particularly significant, as they are the result of additional types of obliged entities being included in Legislative Decree 90/2017.[7] Finally, the new regulatory framework has changed the perimeter of public administrations as obliged entities, prompting 23 new registration requests from members of the public sector, a higher number than in 2017.

The active cooperation of general government

Following the amendment to Article 10 of Legislative Decree 231/2007, which redefined the scope of application of the anti-money laundering legislation for general government, in 2018, the UIF published the anomaly indicators for public offices and the instructions for sending the communications relating to the suspicions detected (see Chapter 9 'The regulatory framework'). Nevertheless, communications from the public sector remain very limited.

The low number of communications from general government suggests a lack of awareness of the potential contribution that this sector could make to preventive action.

[6] The contribution of physical gaming operators remains less significant but is increasing (133 reports compared with 19 last year).

[7] The contribution of these types of reporting entities is still in the early stages, as only two reports have been submitted. We also need to take into consideration the legislative uncertainty linked to these subjects, pending the adoption of the Ministerial Decree which will officially include these types of entities in the register kept by the OAM (see Chapter 9: 'The regulatory framework').

Greater public participation in the operational and methodological paradigm of anti-money laundering, which also integrates an approach that aims at identifying users' subjective and operational anomalies in their interactions with public administrations into the ordinary work processes, could help improve the quality of the administrative action itself. In order to achieve this, a targeted investment is not always needed, considering that in most cases the same information required of users for initiating administrative proceedings can also be utilized for anti-money laundering purposes, but it is essential to strengthen training and spread awareness of anti-money laundering.

The contribution of public administrations can be a valuable source for the UIF's information database and it could give a deeper and wider meaning to financial transactions reported by intermediaries.

In 2018, requests for training sessions received by the UIF increased, above all from local governments. The training sessions were promoted by entities located in central and northern regions, and they also involved representatives and managers from local governments in the South and the Islands. The outcome was the idea that the tasks relating to anti-money laundering investigations, far from being a bureaucratic burden, may represent a further significant safeguard for the law. At the same time, these sessions provided an opportunity to expose the false assumptions that prevent the development of active cooperation in the public sector. For example, it came to light that there is an incorrect and widespread conviction that anti-money laundering legislation is exclusive to the banking and financial sector and that the reporting system can only accept and process information pertaining to financial transactions. A consequence of such assumptions is the difficulty in identifying anomalies and the consequent detection of suspicious patterns that must be represented in the reporting flow. Finally, problems relating to the adoption of those 'internal procedures, proportionate to their organizational and operational dimensions, capable of assessing the level of exposure of their offices to the risk' of money laundering laid down in Article 10(3) of Legislative Decree 231/2007 have emerged, especially in small and suburban contexts.

The perceived overlap between anti-money laundering and anti-corruption safeguards is one of the factors slowing down active cooperation. The misunderstanding stems from the fact that in both cases the focus is on the detection of symptomatic factors of possible illegal activities that could affect administrative activity. Anti-money laundering analyses must focus on profiling the risks of the user's activities, while interacting with the public offices (for example, an administrative procedure) and referring to all activities of potential significance, regardless of possible corruption circumstances. The possible disclosure of conflicts of interest between the person responsible for the proceedings and the final beneficiary, on whom the activity of combating corruption is focused, while worthy of attention, is not an essential requirement of active cooperation. Another quite widespread idea is that AML detection can slow down or obstruct administrative procedures, particularly in public procurement procedures, which are already characterized by highly complex and burdensome processes. This conviction can, however, be refuted by the fact that the anti-money laundering analyses, useful for assessing the operations of the parties involved with public administrations, can benefit from the extensive information required and collected as part of the sequence of activities for issuing administrative measures.

In addition to the demands for training by local governments, the number of requests to register with the UIF's Infostat platform recorded an increase during the year; indeed, between 2017 and 2018, the number of public authorities applying for registration (40)

was much higher than the overall number for the decade 2005-2016 (only 26 entities). However, the information flow is still not taking off, but has remained stable at a total of 113 communications over the past two years. Among the public administrations that have so far joined the UIF's Infostat platform, local authorities are the most prevalent; however, many of those who registered have never sent a report. The lack of a reporting flow would seem to confirm a resistance from some administrations where the prevalence of a bureaucratic approach clashes with the purpose of anti-money laundering legislation. At present, there is a complete absence of central government authorities, probably due to the scale and complexity of their structure.

Investing in training and the dissemination of anti-money laundering knowledge are the two elements that will allow the sector to become more functional. Furthermore, the path taken shows that there is still room in the public sector to expand the number of public offices required to report to the UIF. Based on the UIF's experience, for example, the obligations could also be extended to the subjects managing and liquidating assets and to bodies that, regardless of their nature, manage activities of public interest.

1.2. Suspicious transactions

The reports involving suspicious transactions received in 2018, as in previous years, continued to be mainly concerned with money laundering, with a 98 per cent share of all reports received.

Reports involving money laundering suspicions have increased by 4.4 per cent (from 92,824 to 96,946), despite a decrease in voluntary disclosure reports. For the first time, reports regarding the financing of terrorism surpassed the 1,000 mark (+8.7 per cent; see Chapter 4: 'Countering the financing of terrorism'). With just 18 STRs submitted, reports on financing the proliferation of weapons of mass destruction continued to have a marginal impact (Table 1.5 and Figure 1.1).

Table 1.5

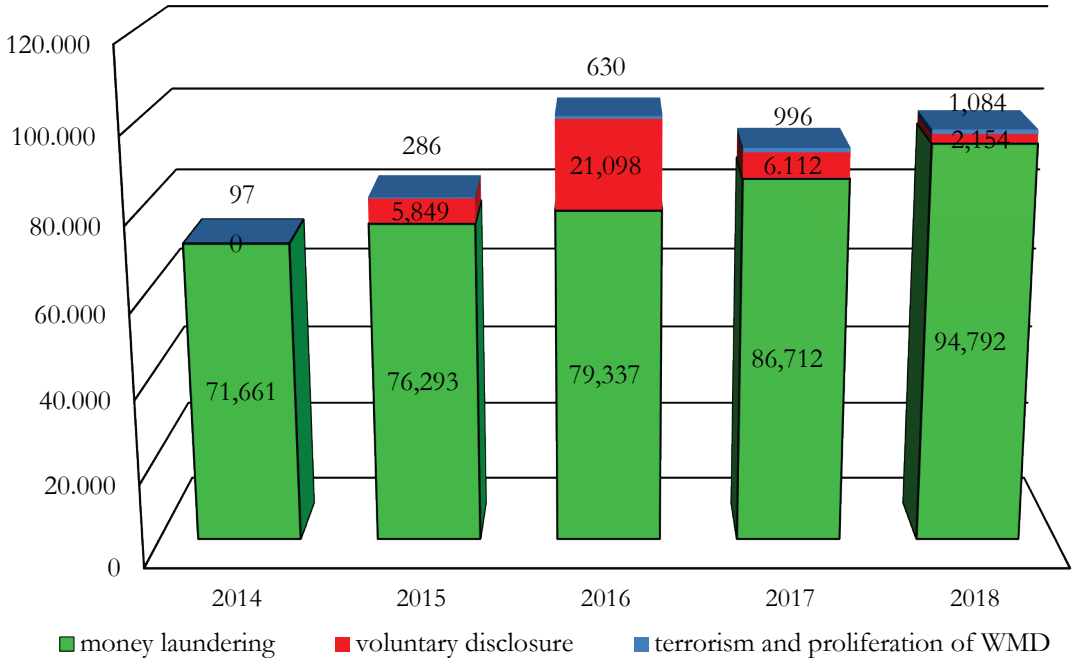
Distribution of STRs by category

	2014	2015	2016	2017	2018
	(absolute values)				
Total	**71,758**	**82,428**	**101,065**	**93,820**	**98,030**
Money laundering	71,661	82,142	100,435	92,824	96,946
of which voluntary disclosure (1)	-	*5,849*	*21,098*	*6,112*	*2,154*
Financing of terrorism	93	273	619	981	1,066
Financing of proliferation of WMD	4	13	11	15	18

(1) The data relating to the voluntary disclosure category only includes reports classified as such by reporting entities.

Figure 1.1

Reports received by category
(absolute values)



No significant changes were registered in the territorial distribution of transactions, with Lombardy still the leading region with 19.8 per cent of the total flow received, followed by Campania and Lazio (12.4 and 9.7 per cent of the total, respectively; Table 1.6). Relatively speaking, the regions where the most significant increase in the reporting flows were recorded are Marche (+17.8 per cent), Sicily (+17.1 per cent), Tuscany (+13.8 per cent) and in a more limited way, Molise (+15.9 per cent) and Valle d'Aosta (+13.7 per cent). The province where most transactions reported is Prato, ahead of Milan, which fell to second place (Figure 1.2). As for the other high-ranking provinces, Imperia, Naples and Crotone confirmed their contribution. Finally, in 2018 the lowest ranking provinces were again located in the south of Sardinia, Oristano and Nuoro, which sent between 36 and 50 reports.

Amounts reported

In 2018, the total value of suspicious transactions actually executed and reported to the UIF amounted to €71 billion against €69 billion in the previous year. Taking into account the reports of suspicious transactions attempted but not executed, the total value of the year's reporting flow reached €90 billion, against €83 billion in 2017.[8]

Transactions not carried out

The total value of transactions reported but not carried out – which in 2018 stood at €19 million – mainly includes transactions not carried out by the reporting entity owing to the high level of suspicion or because of suspension orders from the UIF.

[8] 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 overall. The calculation of the total value of the suspicious transactions is therefore heavily influenced by the assessments of this kind made by reporting entities. In addition, the same transaction may also be reported by more than one entity, leading to a multiplication of the amounts. This is an aspect that is even more important for voluntary disclosure reports, given the possible involvement of various reporting entities in the different steps of the procedure.

Table 1.6

Distribution of STRs received by region where transaction occurred

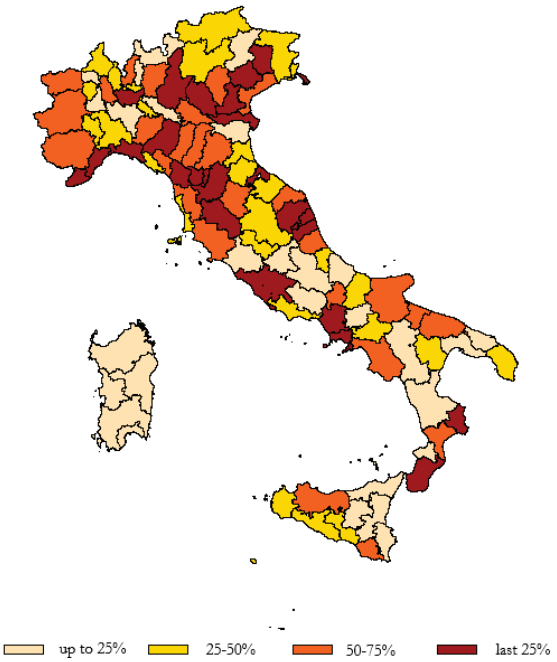
	2017		2018		
	(absolute values)	*(% share)*	*(absolute values)*	*(% share)*	*(% change on 2017)*
Lombardy	19,744	21.0	19,440	19.8	-1.5
Campania	10,863	11.6	12,183	12.4	12.2
Lazio	9,435	10.1	9,545	9.7	1.2
Veneto	8,181	8.7	8,254	8.4	0.9
Emilia-Romagna	6,338	6.8	6,887	7.0	8.7
Piedmont	6,165	6.6	6,341	6.5	2.9
Tuscany	6,129	6.5	6,977	7.1	13.8
Sicily	5,003	5.3	5,857	6.0	17.1
Puglia	4,759	5.1	5,157	5.3	8.4
Liguria	2,908	3.1	2,854	2.9	-1.9
Calabria	2,657	2.8	2,696	2.8	1.5
Marche	2,059	2.2	2,426	2.5	17.8
Friuli-Venezia Giulia	1,724	1.8	1,935	2.0	12.2
Abruzzo	1,464	1.6	1,312	1.3	-10.4
Sardinia	1,265	1.3	1,215	1.2	-4.0
Trentino-Alto Adige	1,210	1.3	1,317	1.3	8.8
Umbria	921	1.0	1,006	1.0	9.2
Basilicata	529	0.6	592	0.6	11.9
Molise	315	0.3	365	0.4	15.9
Valle D'Aosta	182	0.2	207	0.2	13.7
Abroad	1,969	2.1	1,464	1.5	-25.6
Total	**93,820**	**100.0**	**98,030**	**100.0**	**4.5**

Although they do not have an actual financial outcome, in both cases these transactions are of interest as they have a predictive value for operational cases that might be successfully attempted in other parts of the system. At the same time, this type of transaction appears to be symptomatic of the ability of the different actors in the financial system to refrain from carrying out transactions with an excessively high-risk profile.

Despite their limited numbers, the presence of transactions attempted and then withdrawn by the client before the final execution by the reporting agent should also be considered. This pattern is recurrent in reports linked with voluntary disclosure transactions that, however, as already highlighted, have recorded a marked contraction in the current year. Finally, some transactions were reported before they were carried out, making them only temporarily not carried out. Such transactions, which the reporting entity could decide not to carry out at a later moment if new aspects of potential risk have emerged, are closely monitored by the UIF, as it might decide to adopt a suspension order.

Figure 1.2

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

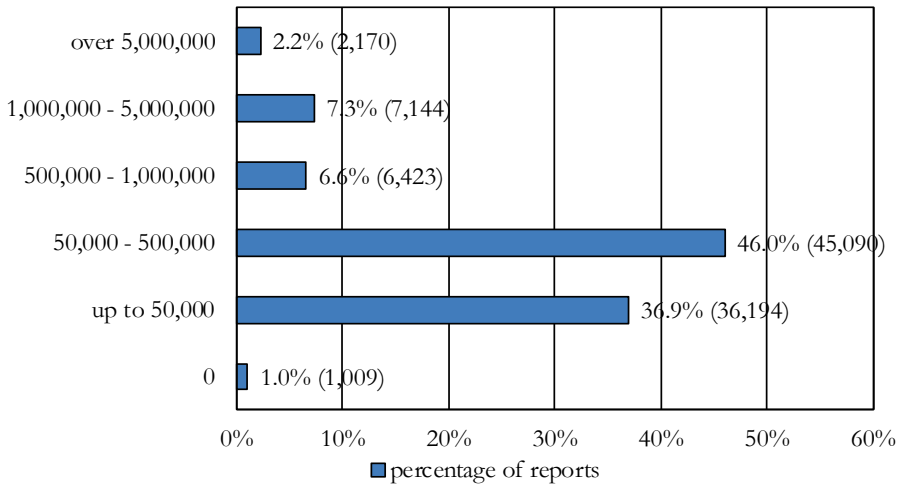


There is no significant change in the distribution of reports that, as in the previous year, involve transactions for sums between €50,000 and €500,000, representing a 46 per cent share, against 47.3 per cent in 2017 (see Figure 1.3).

Figure 1.3

Distribution of STRS received by amount

(in euros)



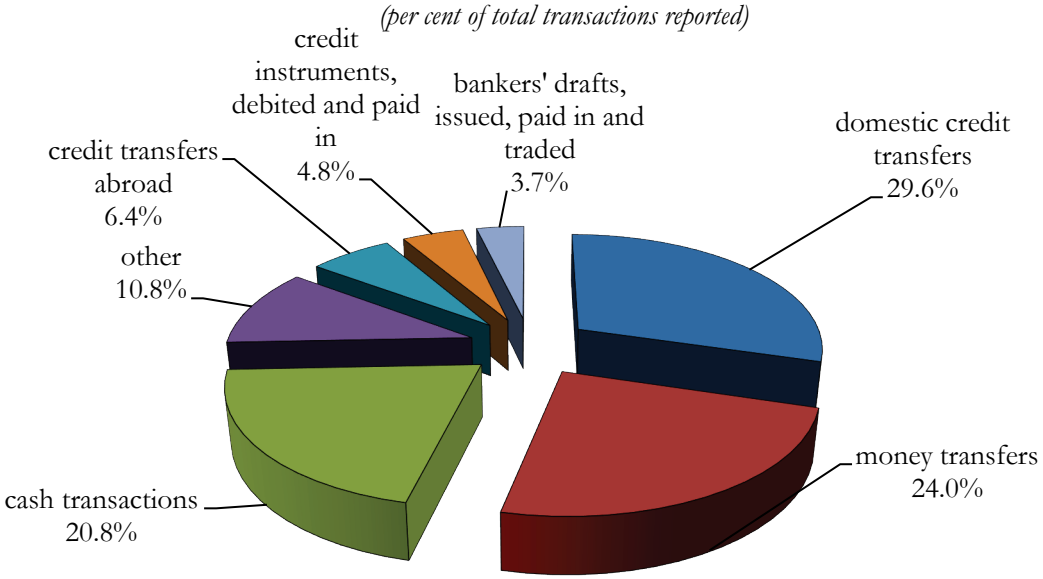
Types of transactions reported

The division into the main types of transaction reported is also in line with the previous year, with domestic credit transfers prevalent, whose share of the total rose by three percentage points, from 26.6 to 29.6 per cent. Cash transactions and payment remittances remained almost constant. After last year's decrease, credit transfers abroad remained stable (Figure 1.4).

Figure 1.4

Main types of transaction reported

(per cent of total transactions reported)



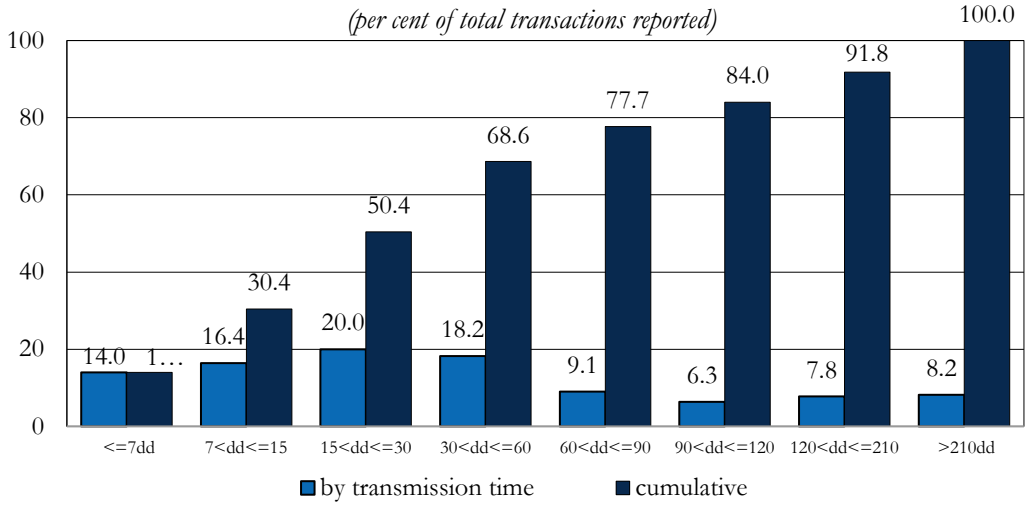
Transmission times for STRs

There was some improvement in transmission times compared with the previous year: 50.4 per cent of the overall number of reports (49.8 per cent in 2017) were received within one month of the transaction, 68.6 per cent (66 per cent in 2017) within two months and 77.7 per cent (as in 2017) within three months (Figure 1.5).

Figure 1.5

Distribution by transmission time of STRs received by the UIF in 2018

(per cent of total transactions reported)



The levels of responsiveness of operators with faster transmission times declined somewhat compared with 2017: the percentage of reports submitted within 15 days of the suspicion's detection was 30.4 per cent, a slight decrease compared with the previous year (33 per cent). In terms of transmission times, banks remain in line with last year's figure, with 33 per cent of reports sent within the first two weeks of the transaction. In the same transmission time group, the share of financial intermediaries other than banks (15.6 compared with 17 per cent in 2017) and gaming operators (10 per cent compared with 9 per cent in 2017) remained limited, while the timeliness of reports received from professionals within the first two weeks (55 per cent) is worthy of note.

1.3. The quality of active cooperation

Actions taken for reporting entities

Improving the quality, timeliness and comprehensiveness of reports is a primary objective of the system for the prevention and combating of money laundering and financing of terrorism, in which the reporting entities' contribution is crucial. The UIF's longstanding commitment to interacting with the reporting entities is an important tool for increasing the effectiveness of active cooperation in terms of the impact of the information provided. Each year, the Unit shares the results of specific indicators with the main reporting entities from the 'Banks' category.

In recent years, the UIF has developed a methodology aimed at monitoring reporting entities based on both a qualitative report assessment by the Unit's analysts and on the results of indicators developed for this purpose, resulting in activities of control and intervention involving formal meetings and communications.

In 2018, the UIF verified the corrective measures taken by the reporting entities that were the recipient of recommendations in the previous year, while at the same time launching new interventions. Overall, the activity involved 27 operators, accounting for 51 per cent of the reports received over the year, of which 16 were from the 'Banks' category, 9 were from payment institutions (including 8 from money transfers) and one was a gaming service provider. The Unit continued to provide brief feedback reports to the main operators of the 'Banks' category on their reporting activities.

The most problematic aspects observed refer to the reporting entities' lack of diagnostic ability, especially their insufficient focus on the grounds for suspicion, as well their inability to compile reports correctly and completely.

Special attention was paid to money transfer operators for which the monitoring activity considered, in addition to the usual indicators, the adequacy of the number of reports submitted by reporting agents in relation to their operational size, derived from the remittance data collected by Bank of Italy for the balance of payments. The comparison between the market share of individual operators and the percentage of reports submitted in total for the sector made it possible to identify operators who make big contributions compared with the volumes transacted and others who may need to improve their contributions.

The feedback reports provide some indicators that operators can use, based on their individual experience and type of activity, to gauge their own position in relation to others in the same reporting category and make further improvements. There are indicators for four different aspects of making a report:

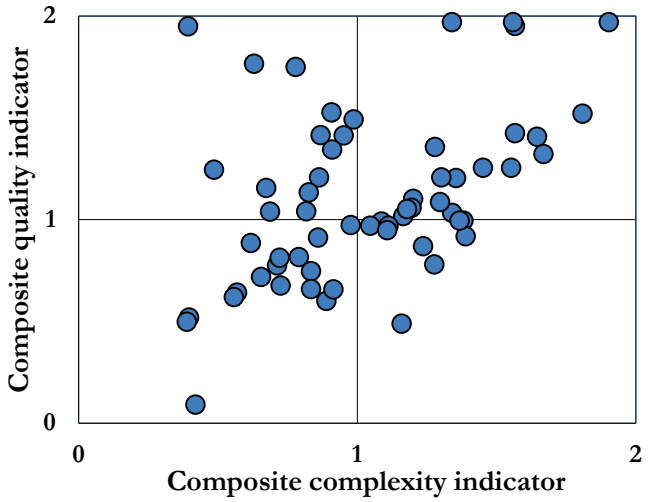
- *the extent of the cooperation*, measured by the number of reports submitted by the reporting entity in the relevant time period as a percentage of the total number of reports sent by the reference group. This provides a parameter for the entity to assess the quantity of the reports they provide;
- *timeliness*, shown by the percentage distribution of reports by time period and by median transmission time. This allows the reporting entity to assess their own speed of reaction to emergent suspicious elements;
- *quality*, measured by indicators that capture the importance of the reports (risk level, results of financial analyses and the interest of the investigative authorities). This summarizes the ability to intercept transactions that pose an effective money laundering risk
- *complexity*, in terms of the number of the transactions and of the persons indicated in the report. This sets out the ability to describe suspicious activities adequately and effectively

Assessment of the quality/complexity of the reports

As in previous years, the main reporting entities from the 'Banks' category have been assessed according to the results of the indicators for the quality and complexity of the reports sent compared with the average levels of their category. Figure 1.6 shows the positioning of the reporting entities in each of the four categories relating to the quality/complexity of their active cooperation. The scatter graph was plotted with reference to 60 operators from the 'Banks' category that submitted more than 100 reports in 2018.

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 2018 (1)



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

Compared with 2017, the average quality of reports included in the sample remained unchanged, while the number of intermediaries that submitted reports of above-average quality increased (55 per cent in 2018 against 40 per cent in the previous year). This appears to confirm the usefulness of the actions carried out by the Unit on the reporting system. More specifically, among the entities monitored, 19 of them, or 31.7 per cent (against 30.6 per cent in 2017), submitted reports of a quality and complexity higher than the benchmark.

There were 14 operators that submitted reports that were less complex but in any case of above-average quality (23.3 per cent): this is the group that showed the most improvement over the previous year, when only 6 operators (9.7 per cent) were given the same ranking. Ten operators sent reports with a high level of complexity but of below-average quality (16.7 per cent of the total), and 17 submitted reports below average in terms of quality and complexity. This number is considerably lower than that of last year (28.3 per cent against 38.7 per cent of the 24 reporting entities ranked lower in 2017).

2. OPERATIONAL ANALYSIS

The financial analysis conducted by the UIF is intended to redefine and expand the context of the original report, identify persons and objective connections, reconstruct the financial flows underlying the operations and identify transactions and situations linked to money laundering or the financing of terrorism, thereby increasing the set of information for each report.

This analysis is preceded by a phase that automatically enriches the data provided by reporting entities. It is carried out using the UIF's dataset and makes it possible to reclassify reports according to the risk and the transaction type. The most important reports are then selected and processed in the most effective way possible and shared for subsequent investigations. The process takes a risk-based approach as defined by the international standards and allows the work of the Unit to be adapted, taking into account the risks and vulnerabilities identified in the course of risk assessments and in the results of strategic analyses.

2.1. The numbers

In 2018, the Unit analysed and transmitted 98,117 suspicious transaction reports to investigative bodies, with an increase of 4.4 per cent compared with 2017 (Table 2.1).

Table 2.1

Reports analysed by the UIF

	2014	2015	2016	2017	2018
Number of reports	75,858	84,627	103,995	94,018	98,117
Percentage change on previous year	*-17.9*	*11.6*	*22.9*	*-9.6*	*4.4*

The flow of reports analysed and transmitted, slightly higher than that of reports received in the same period, was sufficient to balance the increasing incoming flow and to further reduce the stock of reports being processed.

2.2. The analysis process

The collection and management of the STRs are supported by a computer system (RADAR) which receives the reports and is the first point of data entry.

The RADAR system classifies the reports, identifying those with the highest level of risk and which are therefore given priority, on the basis of a rating assigned automatically to each report, which partly depends on the level of risk indicated by the reporting entity.

The growing number of reports submitted, despite some areas of significant heterogeneity, indicates an improvement in active cooperation, both quantitatively and in terms of

the quality and timeliness of the information.

Timeliness of the analysis

There was a further improvement in the share of reports sent to the investigative authorities within 30 days of receiving them, up from 74.5 per cent the previous year to 77.5 per cent. This result is largely attributable to the percentage of STRs submitted within 7 days, which was 45.2 per cent in 2018 against 43.2 per cent in 2017. The same rapid processing can also be observed in reports with a higher risk profile, 51.5 per cent of which are analysed and transmitted within 7 days, a share that reaches 89 per cent for reports submitted within 30 days.

Alongside timeliness, making the best possible use of the reporting flow received by the Unit remains crucial. The UIF has now consolidated the supplementation of the data from reports with the RADAR system's database. It remains necessary, however, to continue to increase the availability of information sources to be integrated into the analysis process, and at the same time to improve the tools that facilitate an understanding of the information framework as a whole.

Threshold-based communications

Regarding the first aspect, the collection of threshold-based communications is imminent, so that from September onwards, the Unit will be able to use analytical data on cash transactions, which will facilitate the analysis and implementation of suspicious transaction reports. The new database will also allow automated analyses and the monitoring of potentially abnormal flows to be launched (see the box: 'Instructions for transmitting threshold-based communications' in Chapter 9). Projects have been started to include new databases (Central Credit Register, shareholding data and financial statements) in the RADAR system, which are currently not automatically accessible.

As regards the second aspect, a project based on machine learning is at an advanced stage and could guarantee an automatic classification of reports, thereby freeing up resources to focus on newer and more complex anomalies (see Chapter 10: 'Resources and organization').

Feedback on investigation results

Providing feedback to obliged entities is an additional way to exploit STR analyses, though it is currently only being provided on reports that do not provide sufficient evidence to support suspicions of money laundering and terrorist financing, in light of the investigative bodies' feedback to the Unit (negative results). In 2018, the Unit set up a system for the automatic transmission of these flows through the UIF's Infostat platform, which in the future can be supplemented with positive results to enhance the educational and synergetic value of the relationship with the reporting entities.

The exchange of information with the obliged entities and with the various institutional counterparties is an integral part of the analysis process. Following the introduction of the SAFE component into the UIF's IT system in 2017, which enables information to be exchanged with foreign FIUs, the judicial authorities and the investigating bodies, a project was started in 2018 to provide a dedicated channel for information exchanges with the reporting entities integrated into the RADAR platform. Analysts will therefore be able to interact with obliged entities by sending out information requests directly through the RADAR system, thereby taking advantage of the high safety standards that the platform already has.

2.3. Risk assessment

A proper risk assessment in the various phases of the STR appraisal process is important for both the financial analysis and in the subsequent investigative phases.

The assessments summarize a number of factors. The main factor is the risk of money laundering or the financing of terrorism attributed to the transaction reported by the obliged entities. The risk level is expressed on a 5-point scale and helps to determine the automatic rating attributed by the RADAR system to each STR.

This rating, expressed on a scale of 1 to 5 and calculated by means of an algorithm structured on mainly quantitative variables, produces the first assessment of the reported transaction's risk level which, by incorporating internal and external factors, may differ from the risk profile assigned by the reporting entity. However, its accuracy also depends on a correct and thorough compilation of the STR by the reporting entities.

Though sophisticated, the automatic rating system is obviously unable to adequately capture the qualitative risk factors that can be detected by financial analysis. The automatic rating can therefore be confirmed or modified throughout the various processing phases in order to define the report's final rating, which is then transmitted to the investigative bodies.

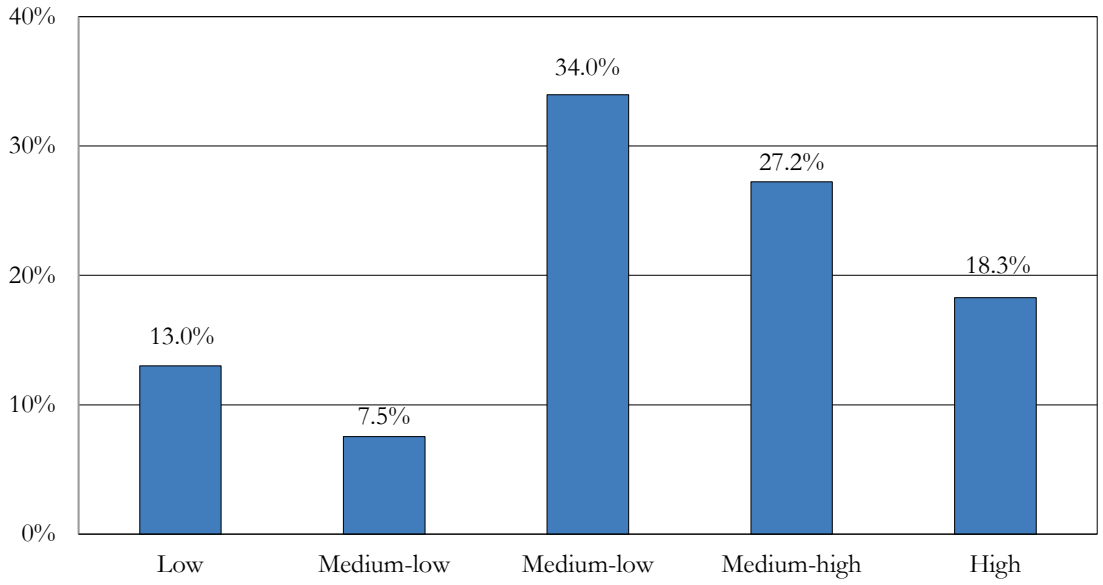
The UIF's final rating

In 2018, the distribution of the final ratings assigned to the reports analysed and processed was very similar to that of the previous year. Some 45.5 per cent of the reports were considered to be high risk (high and medium-high ratings), while in 2017, the share was 44 per cent (Figure 2.1).

Figure 2.1

Reports analysed: distribution by final rating

(per cent)



No significant changes emerged in the distribution of the other risk levels: 34 per cent of the STRs received a medium rating (35 per cent in 2017), and 20.5 per cent a lower risk level (21 per cent in 2017).

The reclassifications made by the analysts mainly involved reports initially rated by the RADAR system as low or medium-low risk: 46 per cent of these STRs were given a final assessment of medium risk and 5 per cent received a medium-high rating. The opposite trend was more modest: STRs in the medium-high and high groups whose final risk rating level was medium or medium-low accounted for 11.8 and 4.7 per cent respectively.

A comparison between the risk assessments of reports made by the reporting entities and by the UIF shows a substantial convergence, with 42.7 per cent of the cases (44 per cent in 2017) given a final rating consistent with the level of risk assigned by the reporting entity (15.7 per cent in the low risk category, 16.7 per cent in the high risk category; Table 2.2). Conversely, 29.5 per cent of the reports rated low or medium-low risk by the reporting entity received a final rating of medium (18.2 per cent) or medium-high and high (11.3 per cent).

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**	15.7	3.7	1.2	**20.5**
	Medium	18.2	10.3	5.5	**34.0**
	Medium-high and high	11.3	17.5	16.7	**45.5**
	Total	**45.2**	**31.5**	**23.3**	**100.0**

2.4. The methodology

The processing of STRs starts with a 'first-level' analysis, which applies to all reports received, in order to evaluate the actual level of risk and decide on the most appropriate type of processing. On the basis of the information acquired automatically or from other sources, the grounds for suspicion of money laundering and the need for further action are evaluated.

If some of the preconditions are present (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 chance of sharing the information rapidly with the investigative bodies), the STR can be accompanied by a simplified report, thus optimizing processing times.

When it is necessary to investigate further to reconstruct the financial tracks of suspicious funds, the STR undergoes a 'second-level' analysis, ending with a report detailing the results of the financial checks carried out.

At this stage, there are many investigative options and tools available to analysts. It is possible to: contact the reporting or other obliged entities to obtain further information; and access the national tax database; and involve the foreign FIU network, as well as make use of all the information stored in the UIF's database.

The methodology of this detailed analysis, implemented within the perimeter of individual reports and aimed at retracing the financial flows of STRs, is constantly being updated in line with the changes in the risks emerging from the reporting inflow. The areas of potential risk identified by the National Risk Assessment are particularly important and have led to the gradual consolidation of specialized analysis focused on organized crime, corruption and tax evasion. During the year, there were methodological discussions aimed at developing more precise indicators and criteria for the timely interception of reports considered to be riskier in terms of their relevance to each of the three threats mentioned above, while also taking account of the recurrent and reciprocal overlapping of the respective risk areas (see Chapter 3: 'Risk areas and types').

In addition to second-level analysis, an innovative method has been tested for evaluating reports submitted by money transfer operators. It uses an aggregated approach that, by means of an overall assessment of the information contained in the reports, within a set time frame or specific operating modalities, aims at identifying relationships and links between subjects and transactions that are not immediately evident in the examination of individual reports.

An aggregate analysis of money transfer reports

Reports containing multiple low-value transactions carried out by a large number of subjects, none of whom can be considered more relevant than the others, or where a specific phenomenon cannot be identified, are more effectively analysed using the aggregate method.

When this method is applied to reports pertaining to money transfer transactions, it enables the detection of cases of particular significance, whereas if taken individually they could appear less important.

During the year, the ability of reporting entities to present increasingly complex cases and the fine-tuning of the methodology used led to the information made available through this type of analysis being used by identifying suitable risk indicators able to determine the most problematic cases.

These indicators define the different profiles of the subjects involved (both agents and clients) and of the money transfer channels between the Italian province where the transactions were carried out and the counterpart (hereinafter routes). The goal is to identify subjects who carry out a significant number of transactions for high total amounts, reported by various obliged entities, thus involving more than one circuit of money transfers and, above all, to define the characteristics of anomalous operations, which take on different specificities according to the profile assessed (agents, clients or routes).

The indicators enable the identification of agents who are suspected of splitting up transactions (thereby bypassing the thresholds imposed by money transfer operators) and who appear to facilitate transfers of funds of dubious origin, such as when customers send/receive money to/from places other than their country of origin.

The indicators identify above all senders who carry out transactions that cannot be considered typical remittances of emigrants, such as those interacting with counterparties located in different countries who alternate between the roles of sender and receiver. These transactions fuel suspicion of illicit activities, including participation in internationally organized networks. There are also cases found where transactions take place in different provinces in Italy, raising doubts over the origin of the funds. Another aspect considered involves transactions related to prepaid cards, often linked to phishing.

The indicators also aim at identifying routes used by organizations involved in opaque activities, both national and foreign, which are firmly established in Italy. The analysis considers transactions involving subjects of different nationalities from the countries where the transfers are made and cases where more than one country is involved in the flows, thereby showing a more complex network of transfers than might be inferred from the analysis of individual reports. Within the routes, there is an assessment of all the subjects involved, be they agents or senders.

The aggregate analysis methodology, carried out on a regular basis, enables a re-evaluation of the content of individual STRs which did not immediately present high risk profiles and which were promptly disseminated on the basis of the first level analysis. In addition, analysts may carry out further studies targeted at cases more worthy of attention, because they are considered potentially riskier or relate to aspects of particular interest, thus providing the analysis of suspicious transactions of money transfers with a broader viewpoint.

Memorandum of Understanding with the DNA

As regards second-level analysis, the use of investigative data continued, which is helpful for guiding choices regarding further analysis of cases that are potentially interesting given the subjects involved in the reports. The UIF has been receiving information in the indicators of investigative interest relating to any previous offences committed by reported subjects from the Finance Police since 2014. The new anti-money laundering legal framework provided an additional data contribution thanks to the Memorandum of Understanding signed on 7 May 2018 between the UIF and the National Anti-Mafia Directorate (DNA). According to this Memorandum, the Unit promptly communicates the reported subjects' personal data to the DNA, which cross checks these data with those stored in their databases and, for each subject matched, transmits to the UIF any involvement in ongoing judicial proceedings, together with the communication to the competent Public Prosecutor's Office. This information exchange allows the Unit to integrate the analysis results with elements relating to any 'criminal history' a reported subject may have. Since March 2019, along with the presence of subjects in its databases, the DNA has disseminated a rating to the UIF based on the extent of the subject's involvement in the investigation (see the box 'Cooperation with the National Anti-Mafia and Anti-Terrorism Directorate' in Chapter 7).

Joint analysis

Experiments on joint analysis with various FIUs have also continued within the EU FIUs Platform (see Chapter 8 'International cooperation'). Specifically, two trials were completed in 2018, one of which was on a complex case of intra-Community fraud, with the purpose of identifying a common methodology shared by the European FIUs.

2.5. Reports requiring no further action (NFA)

One of the UIF's core functions is the selection of the information to disseminate to the investigative bodies.

The UIF stores reports that do not raise suspicions of money laundering or terrorist financing for ten years, following procedures that allow the investigative bodies to consult them if necessary. If analyses do not detect any elements supporting the suspicions of the reporting agent, it does not mean that the report is cancelled, and it can be recovered for financial analysis if new information becomes available.

Reports that are analysed and deemed not to require further action in terms of risks of money laundering or financing of terrorism are the other possible outcome of analyses. This assessment, in line with the new Legislative Decree 90/2017, which no longer uses the ambiguous term 'dismissal', continues to represent the UIF's core function, namely to select cases considered worthy of investigation from a financial point of view. Identifying reports that require no further action is also extremely important in the relationship with reporting entities, making it possible to improve active cooperation.

In 2018, the share of reports analysed that showed no evidence of any risk stood at 16.3 per cent, broadly in line with the figure of 17.1 per cent for 2017 (Table 2.3).

Table 2.3

Reports requiring no further action (NFA)

	2014	2015	2016	2017	2018
Reports analysed	**75,858**	**84,627**	**103,995**	**94,018**	**98,117**
NFA reports (1)	16,263	14,668	10,899	16,042	15,952
NFA reports as a percentage of all reports	*21.4*	*17.3*	*10.5*	*17.1*	*16.3*

(1) For the years prior to 2017, refer to reports dismissed.

The NFA reports highlight cases where the grounds for suspicion that led the reporting entity to submit the report were not substantiated by the financial and investigative elements available. In choosing the level of analysis and the final rating to assign to the reports, the UIF also takes into account the presence of prior investigative interest. This information, taken from the indicators of investigative interest which the investigative bodies have been sending to the UIF since 2014 according to the subjects included in individual reports and to the cross-checks with evidence from the DNA (see the section 'The analysis process'), is therefore an integral part of the analysis that particularly characterizes reports with a low level of risk.

In compliance with the regulatory framework, in 2018 the UIF continued to send NFA reports to the investigating bodies, which can therefore consult them if necessary. At the same time, the UIF returns this information to reporting entities using the new functions that make this possible via the UIF-Infostat platform (see the *Statement* by the UIF of 24 May 2018).

The reports deemed as NFA by means of a final rating of low and medium-low risk showed a significant rate of convergence with the risk indicated by the reporting entity (79.3 per cent; Table 2.4).

Table 2.4

For each NFA report, a comparison of the reporting entity's STR risk rating with the UIF's final rating
(percentage composition)

		Risk indicated by the reporting entity			
		Low and medium-low	**Medium**	**Medium-high and high**	**Total**
UIF Rating	**Low**	71.7	0.4	0.1	**72.1**
	Medium-low	7.6	17.5	2.8	**27.9**
	Total	**79.3**	**17.9**	**2.8**	**100.0**

The cases where the high level of risk perceived by the reporting entity was not confirmed by the outcome of the analyst's assessment amounted to less than 3 per cent. The share of NFA reports, received with a medium risk rating and reassessed with a low or medium-risk rating, stood at 17.9 per cent, against 20.5 per cent in 2017.

2.6. 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, as long as this does not jeopardize the investigation. Suspensions are usually ordered in response to unsolicited communications from banks that provide advance information on the contents of suspicious transaction reports or derive from transactions reported but not yet carried out.

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 329 investigations for suspension purposes, compared with 214 in 2017. The relative value increased by 13.5 per cent, standing at just over €153 million. The growth in the number of transactions assessed for a possible suspension order can also be attributed to a more proactive approach taken during the year by the UIF, which on its own initiative assessed 30 cases submitted to the RADAR system and involving attempted transactions.

Overall, the investigation conducted by the Unit together with the investigative authorities led to a transaction suspension order in 47 cases (14.3 per cent of transactions assessed against 17.8 per cent in 2017, for a total value of €38.8 million; Table 2.5).

Table 2.5

Suspensions

	2014	2015	2016	2017	2018
Number of transactions	41	29	31	38	47
Total value of transactions (*millions of euros*)	45.5	16.7	18.9	66.4	38.8

In 2018, the dominant category of reporting entity was again that of insurance companies (81 per cent of the total, mainly involving insurance policy redemptions), followed by banks (14 per cent). For the first time, a company controlled by a public entity and a payment institution sent information. In almost all cases, the grounds for suspicion pertained to subjects involved in investigations and in slightly less than half of such cases there was evidence of links to criminal organizations. Additionally, in 2018 there was an increase in investigations concerning financing operations stemming from cyber-crime against foreign citizens holding foreign accounts. In such cases, the competent FIUs were also consulted in order to verify an interest on the part of the foreign judicial authority.

A virtual currency exchange was assessed for a suspension order for the first time. Following the suspension order issued by the UIF, the judicial authorities seized the assets both in euros and in virtual currency held on a virtual currency service provider's account, as part of an investigation into a theft of virtual assets worth approximately $150 million.

2.7. Information flows and investigative interest

The UIF receives feedback from the investigating bodies on the level of interest in the STRs sent to them. This communication concerns the overall results of the assessments made of the reports and the financial analyses sent by the UIF.

The STRs' process cycle ends with the sending of the reports and the UIF's analysis to the investigative bodies, who periodically give the Unit feedback on the investigative interest in the reports received. In 2018, the investigating bodies sent the UIF approximately 173,000 feedback reports.

While the indicators of investigative interest sent by the investigating bodies and the DNA are available to the UIF in the course of the report analysis, the feedback informs the analyst of the outcome of previous UIF analyses. It also offers a significant contribution to the decisions on the processing of subsequent reports that highlight subjective or operational contact points with previous cases. Though influenced by elements external to the Unit and independent from its activity, the feedback from the investigative bodies is a valuable way to verify the effectiveness of the analysis. More than three quarters of the positive feedback from the Finance Police involved reports that the UIF analysed and classified as high and medium-high risk in the two years 2017-18. Only 1.5 per cent of the low and medium-low risk reports received positive feedback. The same convergence is found for positive feedback provided by the Anti-Mafia Investigation Department, 88.2 per cent of which was concentrated in the reference period on reports classified as high or medium-high risk.

3. RISK AREAS AND TYPOLOGIES

The UIF's operational analysis of suspicious transaction reports makes it possible to identify typologies characterized by recurring elements that are important for assessing the threat posed by money laundering and the financing of terrorism.

The UIF uses the operating typologies to classify STRs and to provide updated information to obliged entities in order to help them detect suspicious transactions. In a spirit of active cooperation, the UIF publishes its results as 'Cases of money laundering' in the *Quaderni dell'Antiriciclaggio* series.

3.1. The main risk areas

The areas considered to be most at risk by the National Risk Assessment (tax evasion, corruption and organized crime), took on a significant role in the analysis of the reports in 2018 as well. Given the strategic significance of these threats, the use of more established methods was accompanied by the identification of new methodological approaches, which involve a more transversal analysis of the information available. These efforts, launched partly in previous years and partly during 2018, led to the establishment of criteria and indicators that are being tested and then implemented into the analytical process.

3.1.1. Tax evasion

In 2018, about one fifth of the suspicious transaction reports submitted to the Unit pertained to potential violations of tax laws. Financial analysis confirmed the versatility of tax offences that, as observed in the past, often form part of a broader context than the fiscal one, as tax violations are frequently part of complex fraudulent schemes that are set up to conceal the illicit origin of assets.

The number of reports relating to this type of violation was about 20 per cent of the total, down from 24 per cent in 2017. The decrease is attributable to the conclusion of the period of availability for activating the voluntary disclosure process.[9] Excluding those involving the voluntary disclosure process, reports of tax violation increased, totalling over 17,000 units.[10] About 72 per cent of the cases from this risk area were linked to established operational models consisting of several transfers of funds between natural and legal persons, possibly false invoices, apparently commercial transactions registered on accounts held by natural persons, and withdrawals of cash from accounts held by firms. Integrated analyses using the information at the Unit's disposal have confirmed frequent links with organized crime, such as usury, extortion and corruption.

Tax credit sales

Other suspicious transaction reports have alerted the UIF to payments linked to transfers of VAT credits and debts with anomalous elements. Generally speaking, purchasing VAT credits, in compliance with sectoral regulations, allows purchasers to offset their debts

[9] Reports relating to the voluntary disclosure process pertain in particular to the repatriation of assets declared as part of voluntary disclosure or to the subsequent use of sums already repatriated. Reports of this kind accounted for around 11 per cent of the overall number.

[10] In the previous two years, in 2016 there were just over 15,000 reports pertaining to tax violations, excluding those relating to the voluntary disclosure process, and about 16,700 reports in 2017.

toward the tax authorities, and sellers to liquidate their tax credits in a short space of time. In some cases, however, technical analysis has highlighted the recurrence of elements typical of invoice fraud aimed at creating fictitious credits to present to the tax authorities. It is alleged that false tax credits were often traded at prices well below their actual value.[11]

Wrongful compensation for tax debts

There have also been cases of firms taking over tax debts declaring presumably fictitious credit positions to the tax authorities, sometimes involving considerable amounts. From an economic point of view, the original debtor firm allows a third party to pay its tax debts, to which it provides only a part of the capital required for settlement of the tax debt (the profit consists in the difference between the nominal value of the debt and the capital actually provided to the third party paying the debt). In order to settle the acquired debt, the third party uses its own credits as compensation. This way, on the one hand it obtains funds from the original debtor, while on the other hand it liquidates its credits toward the Revenue Agency. This practice, which has already been the object of a resolution by the Revenue Agency declaring it inadmissible for tax purposes,[12] continues to be carried out and is often associated with fraudulent behaviour, with the help of tax accountants and professional advisers, and in connection with the use of non-existent tax credits.

Some reports have highlighted the possible recurrence of tax crimes involving failure to pay VAT and/or taxes withheld on salaries and consulting fees or, to a very limited extent, failure to make an annual tax declaration. In these cases, the Unit forwarded the reports, along with the relevant technical analyses, to the competent investigative authorities, also in accordance with Article 331 of the Penal Code. In 2018, STRs relating to tax crimes accounted for about one quarter of all reports forwarded under this Article, with no variations in absolute numbers over the previous year. As of 31 December 2018, almost all of them were the object of further investigation. In some cases, the investigating authorities charged the offenders shortly after receiving the Unit's report.

Countries at risk

At the methodological level, after having launched a geographical and functional mapping of countries at risk (tax havens) in 2016, based on a sample of countries chosen, in 2018 the sample was enlarged and the analytical methodology was refined. During the year in question, the number of reports involving transactions with counterparts in countries considered at high risk of money laundering (barring those belonging to the voluntary disclosure category) increased significantly (+16 per cent). The investigative interest in these reports is significant, especially in the cases investigated by the UIF as a result of a better selection mechanism and the involvement of foreign FIUs.

In order to achieve a more balanced and reliable outcome in screening reports of this kind, the Unit is currently evaluating adjustments to the established criteria (favourable conditions inherent in the commercial, business and fiscal regulatory set-ups and persistently opaque information about beneficial ownership) by taking into consideration other distinctive characteristics of countries from a socio-demographic point of view. As an example, the reliability of financial intermediaries could make a country particularly attractive for investments by non-residents; the geographical location could also be an attractive element. These considerations are additional assessment elements used in separating physiological situations

[11] For a more detailed description of the topic of selling non-existent VAT credits, see Section 3.5.2. of the UIF's *Annual Report for 2017*.

[12] The Revenue Agency has taken action on this issue by means of Resolution No. 140/E of 15 November 2017, which rules against the settlement of a debt acquired by a third party by using credits claimed against the Treasury.

from pathological ones.

No less important when considering a country's risk level is knowing whether or not it uses the Common Reporting Standard (CRS), which enables an automatic exchange of fiscal information between countries.

Shell companies

Again as regards methodology, a survey was carried out on the reports that reveal the transactions of shell companies used as part of fraudulent tax schemes based on false invoicing. Starting from the well-known characteristics of such entities (an underdeveloped, even non-existent productive structure with a high business revenue, minimum required capital, lack of bank credit lines, and marginal profitability) the Unit is developing a synthetic indicator based on balance sheet data. This indicator is based on a series of specific components for each management area: capital, profitability, production structure and financial debt. The goal is to identify entities of interest within the complex company networks where these financial schemes usually take place.

For the time being, the first tests on the indicator have given interesting results: in most cases, not only did the indicators confirm the conclusions of the financial analyses of the suspicious reports selected, but other shell companies were identified within the more complex networks. If the trial process were successfully completed, the synthetic indicator would contribute to the enrichment of the anomaly patterns by making available a process that the reporting entities can follow to analyse their client's financial statements, thus integrating the description of the account movements with accounting information.

3.1.2. Corruption and misappropriation of public funds

In-depth financial analysis of cases potentially pertaining to corruption was further expanded during 2018, with regard to both suspicious transaction reports and inspection activity, or rather in the course of specific cases of cooperation requested by the judicial authorities.

Given the variety of the financial patterns of corruption and how difficult it is to trace them to predefined schemes, the in-depth analysis of STRs has mainly focused on subjects' profiles and on direct and indirect links with functions of a public nature, also in light of the transactions, even if they are not immediately attributable to cases involving corruption.

The analysis of the financial activity reported and especially of the counterparties, characterized by various kinds of links to public administration offices, made it possible to trace back the transactions observed to illicit payments or transfers of asset ownership for corruptive purposes.

Investments by social security institutions

The analysis of some investment initiatives taken by social security institutions continued. The anomalies observed can be traced to the investment choices made by these institutions, which are often shaped by potential conflicts of interest; the in-depth analysis carried out has shown possible cases of corruption involving representatives of the institutions and the companies entrusted with managing their assets or the professionals providing the companies with advisory services. This resulted in investments, particularly in the real estate sector, with both domestic and foreign counterparts linked with the abovementioned advisors and management companies, at the expense of any logic based exclusively on standards for profitability and propriety. An additional effect of these suspicious management policies has been the adoption of accounting practices designed to give artificial support to the companies' financial results.

Manipulation of court proceedings

Some analyses that were begun in 2017 and expanded in 2018, also as part of the cooperation with the judicial authorities, have made it possible to reconstruct an organization, created by entrepreneurs and lawyers operating throughout Italy, with links to politically exposed persons, able to influence important judgments issued by various regional administrative justice councils and by the Council of State. The in-depth analyses brought to light payments made to public officers, their relatives and other persons with various kinds of connections to them, of different types of assets, or rather the chance presented by the group of entrepreneurs involved to shield financial assets abroad through foreign companies. In some cases, the Unit was able to identify these dealings thanks to the crucial cooperation at international level with other FIUs.

False ownership of assets

In some cases, it has emerged that corruption, especially at local level, is rooted in contexts heavily infiltrated by mafia-style organized crime. Under these circumstances, recourse to false ownership of assets (especially shareholdings) to cover up illegal business makes it more difficult to reconstruct the relationships between the corruptors and the corrupted, even in situations in which the mutual assets obtained by them, or rather those that could be obtained, seem relatively clear. Financial flows to high-ranking local government officials have been detected - under whose responsibility several administrative proceedings are carried out (granting authorizations, concessions and so on) – coming from subjects seemingly unconnected with criminal organizations but actually closely linked to them by financial, business or family relationships. All of this is based on justifications that are scarcely or not at all in line with the nature of the relationship between the counterparties and are therefore potentially suitable for hiding the corruption involved in the transactions made.

Companies and PEPs

As part of the initiatives for setting out the systematic approaches to assessing STRs concerning corrupt behaviour and contexts, the UIF launched tests on a method designed to exploit the existence of connections between the companies reported and politically exposed persons (PEPs). The focus was on the transactions of firms for which (either based on the reporting entity's indications or via feedback from other databases included in the UIF's data warehouse) it was possible from the first evaluation of the report to find a link – often neither explicit nor immediately identifiable according to the parameters defined for beneficial ownership – between companies and a PEP that could create potential conflicts of interest.

The methodology described influences the analysis process, aimed at discovering the presence of additional risk elements such as the economic sector of activity, participation in and/or awarding of public procurement projects and the acquisition of public resources. In cases where information on the existence of a connection between a company and a PEP is combined with some of these elements, thus classifying and strengthening the suspicion of conflicts of interest, the analyses have generally revealed situations that are compatible with possible irregularities indicating the most serious threats.

A political connection can form part of a more complex methodological approach which, starting from companies at specific risk, attempts a financial reconstruction of relationship networks, also using information available from reliable public sources. From this specific point of view, the increased availability of information on the official general government websites may be vital in guiding financial analyses towards cases that are worthier of investigative attention. The in-depth financial analysis of reports concerning successful bidders not complying with financial traceability obligations pertaining to the public contract, on the one hand, made it possible to reconstruct significant subjective links in terms of corruption risk. On the other hand, by using publicly available information on the successful

bidding companies and contracting authorities, it was possible to uncover the association between financial anomalies and the presence of indicators of potential corruption risk in tenders, such as excessive down bidding, contracting authorities making direct awards (often classified as urgent), the limited number of bidders allowed to participate, and the large gaps between planned and actual procurement costs. Moreover, in some cases it was possible to ascertain that financial transactions directly involved subjects later found to be contractors from the same contracting authority, suggesting the possible existence of systems for taking part in tenders that divide the proceeds or form cartels.

Regarding this methodology, the information available in some sources open to the public is particularly useful in understanding the financial anomalies reported, mainly the Public Procurements National Database, along with the database for the Public Administration's suppliers, the lists of the attestation bodies (SOA) certified by the National Anti-Corruption Authority (ANAC) (and the natural persons involved) and in the future national register for tender committees members.

3.1.3. Organized crime

In 2018, there was an increase compared with 2017 in the number of cases concerning transactions and contexts at least potentially associated with the main mafia factions. This increase is due not so much to the high number of reports as to the improvement in the ability to make use of the information already available in the Unit's database, to the launch, in the second half of the previous year, of the systematic exchange of information with the DNA and to the increased sharing of information with the investigative bodies, as part of the institutional cooperation defined by the regulatory framework.

As well as improving the capacity to select, all of these factors have led to the consolidation of specific skills and to the identification and analysis of increasingly complex contexts.

The exchanges and the growth in the number of meetings with the authorities responsible for combating organized crime have led to a positive integration between information factors and elements of an economic and financial nature and information of a different kind: this becomes particularly important in light of the substantial neutrality of mafia financial activity, the dynamics of which are not usually very different from those of ordinary crime.

Financial operation schemes traceable to potential mafia interests seem to be spread throughout Italy (though sometimes to different degrees), with investigative evidence to confirm cross-regional projections. Transactions involving foreign countries were frequent and in some cases especially intense. Cash flows toward foreign financial hubs (first or second destination accounts) are on the increase as a result of significant domestic transactions (often aimed at concealing resources from the revenue agency, but which also often involve flows which appear to be lawful), making it particularly difficult to determine the nature and origin of the financial transactions. In the absence of any further evidence, it cannot be excluded that the financial assets held on foreign accounts (mainly in the Balkan area and Eastern Europe) may be used in various ways, for example as a guarantee for bank loans for significant amounts, considering the large sums deposited, or for additional foreign-to-foreign payments. The in-depth analyses also show an increase in return flows to Italy by means of credit cards issued abroad used for ATM withdrawals in Italy, financing for entrepreneurial and/or real estate initiatives as well as payments for foreign supplies and/or services.

The improved ability to identify contexts potentially relating to organized crime interests

was reflected in the increase in the number of reports considered to be of interest by the investigative bodies: in particular, about 58 per cent of the reports assessed as being potentially related to organized crime received at least one positive feedback of investigative interest in 2018, with a significant increase compared with 2017. In this context, the firms reported are mainly limited liability companies, often simplified, which provides greater managerial and regulatory flexibility, the possibility of breaking up company ownership, and therefore a reduction in the risk of the entire share capital being seized, although in most of the cases examined, this has a very limited nominal value.

In addition, the economic and business sectors are those traditionally infiltrated by organized crime: among the main ones, trade (monopoly goods stores, oil and petroleum products, motor vehicles, electronics and large retailers) and construction (including real estate services), but other sectors of activity (albeit with lower percentages) were also involved, such as manufacturing, food services, communication, business support activities as well as transport and storage. More in detail, even in cases of a lower percentage of companies operating in a specific field, sectors at high risk emerge due to the fact that such companies provide services in collaboration with or in competition with the public sector (such as health and welfare, electricity, gas and water supply, and sewage and waste management) or, in any case, receive public funding also through public tenders.

In 2018, an experimental study was launched in Italy to verify the quantity and quality of suspicious transaction reports submitted by intermediaries operating in areas deemed to be particularly at risk of mafia infiltration. The methodology adopted allowed the preliminary identification of areas potentially affected by this phenomenon at the level of individual municipalities, using more or less recent cases of municipal councils dissolved due to mafia infiltration as a criterion. The geographical data were completed with a comparative sample made up of an equal number of municipalities located in regions traditionally less affected by organized crime infiltration but considered analogous as regards specific variables (population, income per capita, number of banks, financial inclusion and so on) aggregated into a plausibility indicator. The difference (in terms of quantity and quality) between the reporting flows associated with the two clusters, not explained by these variables, will make it possible to obtain useful information on potential changes to the intermediaries' evaluation process which fulfils the active cooperation requirements.

3.2. Further results of the operational analysis

The operational analysis identified additional cases worthy of attention, which have been subjected to a more specific investigation.

3.2.1. Abnormal financial flows connected to the import of textiles from China

For a number of years now, financial flows from Italy to China have been characterized by anomalies allegedly attributable, at least for a significant part, to the under-invoicing of imported Chinese goods, which consists in declaring a false value for the goods in customs declarations in order to avoid tax payments (VAT and duties).

Under-invoicing requires the Italian companies buying the goods to pay the Chinese suppliers the difference between the value invoiced and the real value of the goods exchanged, generating financial flows toward China that are added to legitimate transactions, using methods and systems less easily traceable than the traditional banking channel, so as to

obstruct verifications and controls by customs and tax authorities.

In previous years, it was observed how the money transfer channel for remittances was used improperly for large transfers to China. The analyses carried out on suspicious transaction reports, also confirmed by on-site inspections, showed that funds were sent via numerous transactions for an artificially split unit amount to bypass the regulations limiting the use of cash transactions.

The various authorities in charge of supervising and combating illicit behaviour concerning financial flows and goods trading, as well as the supervision of financial intermediaries (the Customs and Monopolies Agency, the Finance Police, the UIF and the Bank of Italy) have taken decisive action over the years to contrast these phenomena, leading to important judicial investigations and sanctions on several payment institutions involved in cash transactions.

Over the years, however, the subjects involved in this field have been able to change their operational modalities both for importing goods (changing the port of arrival and customs clearance location), and for transferring financial flows to export companies (using different money transfer agents and other types of financial services).

In this context, based on information provided by the Customs Agency, it was found that since 2017, there has been a significant increase in the quantities of textile products of Chinese origin cleared in Hungary and subsequently transferred to other European countries where the companies buying the goods are located. Alongside this trend, the average value per kilogram of the goods declared at the Hungarian customs offices has decreased significantly.

Recent in-depth analyses carried out by the UIF have highlighted unusual financial flows between Italy and Hungary traced back to subjects of Chinese origin active in the textile sector. More specifically, a large number of companies, based mainly in the provinces of Prato and Rome, transferred large sums (more than €120 million in the years 2017-18) to Hungarian companies controlled by Chinese subjects that in turn sent funds to companies located in Eastern Asia. Moreover, the information acquired through the international cooperation channel allowed cash deposits in euros for considerable amounts (over €1 billion in 2017 and 2018) to be detected in accounts held by some of the Hungarian companies involved in these movements. The cash could arrive in Hungary via undeclared cross-border transfers from other European countries where the companies buying the goods are located (Italy, but also France, Germany, Spain and Portugal), thereby violating the Currency Law.

3.2.2. Financial anomalies in the gold sector

An in-depth analysis of several STRs exposed anomalies in the transactions carried out by the key players in the gold and precious metals market, namely cash-for-gold businesses and professional gold traders.

Gold trading, both in the form of investment gold and industrial gold,[13] can be carried out exclusively by banks and by licensed gold traders who, after giving advance notification

[13] See Article 1 of Law 7/2000 which defines investment gold as 'gold in the form of a bar or a wafer of weights accepted by the bullion market but in any case of more than 1 gram, of a purity equal to or greater than 995 thousandths, whether or not represented by securities: gold coins of a purity equal to or greater than 900 thousandths and minted after 1800 and that have been legal tender in the country of origin, normally sold at a price

to the Bank of Italy[14] and if in possession of the required attributes, are listed in an official register.

Cash-for-gold business, on the other hand, is generally carried out by individual companies[15] and consists in the purchase or exchange of used precious metal items, at wholesale or retail level, which can subsequently be resold on the market, after repair or maintenance work, or acquired by goldsmiths or professional gold dealers who then melt them down.

From a financial point of view, cash-for-gold operators generally buy jewellery items from private citizens and then resell them, in the form of gold scrap, to gold fusion operators, who pay the invoices using traceable instruments, such as cheques and credit transfers.

In some cases, the anomalies reported to the Unit concerned cash-for-gold shops purchasing gold items of suspected illicit origin, subsequently reselling them to professional operators.

In addition, some declarations submitted to the Unit led to a focus on cash-for-gold agents and gold traders active in areas geographically distant from known gold manufacturing districts, and who carried out credit and debit transactions, as well as purchasing and selling gold materials mainly for industrial use and investment gold that appeared to be well above the sector average, involving counterparts active in different business fields and sometimes involved in criminal proceedings before the judicial authorities.

The reports were the object of in-depth analysis, which focused on financial transactions registered on the accounts held by the traders reported and on the gold declarations submitted to the Unit, where they appear both as the declarers and as gold purchasers or sellers. The analysis showed that the amounts declared to the Unit were lower than the amounts registered overall on the accounts observed, leading to the suspicion that the actual gold trading business is bigger than that officially declared.

The analysis of the reports also exploited information exchanges with foreign FIUs, which have been involved in connection with purchases of gold by the traders reported as counterparts of companies operating in the precious metal sector, located in both EU and non-EU foreign countries.

In many cases, the Italian gold traders turned out to be shareholders or managers of the foreign companies, while in other cases the companies' shareholders and managers were foreign citizens, in any case linked to Italy, especially through residency, and probably acting as figureheads.

Following a scheme already delineated during court proceedings too, these are often shell companies, used to issue invoices in the name of the Italian counterparts, in order to

---

which does not exceed the open market value of the gold contained in the coins by more than 80 per cent, included in the list drawn up by the Commission of the European Communities and published annually in the C series of the Official Journal of the European Communities, and coins with the same characteristics, even if not included in the list'. Industrial gold is 'gold other than investment gold, for mainly industrial use, both in the form of semi-finished products of a purity equal to or greater than 325 thousandths, or in any other form and purity'. This definition of gold does not cover jewellery, which is included among precious metals (Legislative Decree 92/2017 containing the 'Provisions for carrying out cash-for-gold business, in compliance with Article 15(2) letter l), Law 170/2016').

[14] Law 7/2000, Article 1(3).

[15] Legislative Decree 92/2017 laid down the obligation for cash-for-gold businesses to apply for inclusion in the register for cash-for-gold traders, which is kept and managed by the OAM.

'launder' gold of illicit origin, which is then traded within the EU Community, thus justifying the financial flows transferred abroad by the Italian companies acting as buyers. In light of this kind of funding, the international cooperation channel has made it possible to verify how the amounts moved through credit transfers made by the Italian companies have been wiped out by means of considerable cash withdrawals.

In the context described above, the financial transactions of one particular licensed gold trader have been reported and analysed; this trader is part of a criminal organization dedicated to melting down gold of illicit origin, purchased in cash by foreign citizens. Ingots were then placed on the legal market using a shell company with its registered office in an eastern European country.

Finally, the gold sector was also affected by more peculiar phenomena, identified thanks to the financial analyses carried out. In particular, investigations of corruption cases traced back anomalous financial flows of significant amounts to sales of investment gold.

3.2.3. Other operating typologies

Cash

Among the typologies most frequently encountered while analysing reports, the percentage of reports involving the abnormal use of cash remains the same as in the previous year (33 per cent of the total). The central role that cash still plays in trade in Italy is reflected in the decision to focus the new threshold-based reporting flow on this typology for the initial phase.

Attention is still focused on reports involving ATM cash withdrawals in Italy made using foreign debit cards. Although banks do not have access to information regarding the identity of those using the cards, the recurrence of withdrawals made with the same card constitutes an element of risk, especially when significant amounts of cash are withdrawn. In the cases assessed as high risk, the international cooperation channel has been activated in order to identify the cardholders and the correlated current accounts. In many cases, especially involving eastern European countries, the account holders turned out to be Italian citizens, sometimes linked to criminal organizations, who had used credit transfers to move their funds to foreign bank accounts. Given that it is impossible for a bank to trace the name of the person making the withdrawals, this operational modality facilitates the use of apparently foreign assets in Italian territory, thereby complicating the investigation of the funds' origins. In other cases, the exchange of information with other FIUs made it possible to intercept cloned cards, as the withdrawals were unauthorized by the lawful holder.

Fraudulent loan applications

Some reports were received that involved fraudulent applications for loans, supported by false income documentation; a joint analysis made it possible to identify a peculiar and interesting scheme, namely the submission at the same branch of a high number of applications for small loans by new customers with no apparent link between them. These individual applications were traced to a unified scheme thanks to an analysis of the use of the amounts granted as a credit line where credit transfers or transactions on prepaid cards for recurrent third parties could be identified, as well as the monetization of the residual credit over a fairly short period. This recurrence, which was not explained by the relationships between the loan recipients and the final beneficiaries, fuelled the suspicion that a small group of subjects was the real beneficiary of the numerous loan applications submitted, given the brief timeframe, the geographical distribution and the similarities in the methods used by the various applicants. Lastly, a cross-check of the financial flows between the final beneficiaries seemed to point to a potential network of entities that both steered the subjects towards the same branch and also helped by providing them with the documentation required. The financial

flows were therefore a kind of commission on the illegal services provided.

Fraud against the State relating to social security contributions

Some reports were analysed over the year that highlighted the misuse of social security contributions to pension funds in order to carry out an aggravated fraud against the State. More in detail, a few companies, some of which are owned by the same subjects, carried out suspicious transactions characterized by payments of contributions to pension funds in the name of employees not participating in the funds. Subsequently, claiming they had made erroneous deposits, the companies asked for the payments to be reimbursed on their bank accounts. A crucial element was how the social security contributions were paid: the above-mentioned companies used their faculty as employers to pay complementary contributions by using the compensation for tax credits that are actually non-existent. The entities involved in these reported transactions are companies active across various sectors (construction, motor vehicle trade, manufacture of metal structures, and consultancy), many of which are newly established, without employees and with a minimum share capital. The UIF issued suspension orders involving reimbursement requests followed by the urgent preventive seizure ordered by the judicial authorities on the total amount of the sums paid to the funds. The decree for seizure also provided not only for a block on the sums still available in the pension funds and subject to suspension orders, but also on those already reimbursed to the relative company accounts.

Usury

In 2018, a review was begun of the STRs submitted in 2017 and 2018 that, based on the reporting entity's indications or following in-depth financial analyses, are traceable to usury. The aim of the review was to verify the influence that publishing the relative form of anomalous behaviour has had over the past few years in detecting cases involving usury or other typologies worthy of attention.

The ongoing analysis shows that the system is limited in its capacity to intercept cases of usury. The percentage of reports referring to usury remains very low and is mostly induced by the dissemination of press statements revealing the involvement of clients in court investigations into cases of usury. The hypothesis being examined is that this form of anomalous behaviour is highly complex, which leads the reporting entities to submit reports that highlight a few easily detectable elements, with no thorough analysis of the supposed underlying phenomenon of usury.

Some subjective profiles are found in the reports that recur as being those of alleged usurers. They are often small business owners (38 per cent of reports) or pensioners (15 per cent), and almost always male; there is also a significant share (8 per cent) of unemployed persons in the reports analysed. Alongside the frequent and significant use of cash and cheques, there are some previously undetected new anomalies, such as the alleged usurer replacing the victim as shareholder, sales of real estate properties (apartments, shops and so on) at prices significantly lower than the market value, as well as less recurrent operating modalities, such as adding money to prepaid cards. Further improvements in the ability of reporting entities to detect usury could be made by integrating the new elements observed into the anomaly scheme.

Professionals and innovative start-ups

The contribution of professionals has been important, especially in identifying transactions in areas subject to sectoral rules, knowledge of which is crucial for intercepting new money laundering techniques. In 2018, reports were submitted regarding the potential abuse of the incentive and tax subsidy system available to innovative start-ups. Suspicion was rooted in the concentration of applications to sign up with the special section for innovative

start-ups on the business register made by some recently established limited liability companies, with no links between them but located in the same area. The applications to register occurred in a short period of time and were accompanied by large increases in capital, inconsistent with the size of the companies, which were all barely active, and in almost all cases were reserved for the beneficial owners of the companies making the decision. This circumstance is not consistent with how start-ups increase capital, which is usually by allowing new partners to join and bring fresh resources to support development plans.

Irregular corporate transactions

Several anomalies were detected in notarial procedures, mainly concerning irregular corporate transactions (purchases and sales of shareholdings occurring close together, sudden or illogical changes of registered offices and transfers of goods and services as a share of the corporate capital).

Several reports were submitted by the auditing category, which involved tax irregularities including in particular failure to pay VAT, failure to pay social security contributions, and false invoicing.

Abuse of public funds intended for assistance to migrants

In 2018, a number of reports were submitted that drew attention to the anomalous use of the funds for receiving migrants, distributed by Prefectures to cooperatives, in most cases recently established. A recurring element in the cases examined was that a considerable amount of public funds were used by the beneficiaries to make cash withdrawals with no appropriate supporting documentation. Credit transfers were also made in favour of the accounts held by the cooperatives or by subjects connected to them, followed by cash withdrawals. The use of cash makes it impossible to detect the final destination of the funds allocated and increases suspicions that they may be used illegally. Reports of this kind were frequently followed up with investigations.

Reports on money transfers

Reports on money transfers are typical of the sector, characterized by granular transfers and a large number of subjects involved which influences how the work is carried out. In addition to the first and second level analysis, the Unit carries out a regular aggregate analysis on this type of STR (see the box: *'Aggregate analysis of money transfer reports'* in Chapter 2), which is necessary to identify cross-sector risks and contexts that are only detectable through a cohesive assessment of the information contained in the reports.

The most frequently reported anomaly was the disparity between the country of origin of those sending remittances and the country where the money was transferred, which means it is not possible to link the flows with the typical remittances of emigrants. This anomaly conceals various cases.

Migrant smuggling

The main anomaly of recent years is linked to migrant smuggling, characterized by the highly fragmented nature of transfers, often for very low sums, received in wealthy nations and with very few transfers to the areas of origin of the persons involved, who are mostly from Africa or the Middle East. These characteristics, paired with the senders being located in Sicily, Calabria and Puglia, trace the phenomenon to the migrants' points of arrival, as is also confirmed by investigative evidence. The same characteristics were found in transactions located on the northern Italian border (mainly in Trieste and Imperia) and may presumably refer to flows of migrants by land.

Cases involving migrant smuggling include increasingly complex criminal activities carried out after the arrival of the migrants in Italy. This phenomenon can be attributed to a number of complicated activities, such as senders interacting with more than one country of destination as if they were contact points for large organizations, and which mainly affect big

cities. The forgery of documents for persons who enter Italy illegally, and then travel on towards other European countries can be included in this category as well.

Human trafficking

A particular phenomenon that can, however, be linked to aiding and abetting illegal immigration, is human trafficking; this includes various types of exploitation, often hypothesized by the reporting entities in response to the requests for information about subjects under investigation, including from abroad. In cases of this kind, transfers for small amounts are sent to the country of origin of the senders who, unlike in cases of migrant smuggling, can be both exploiters and victims of trafficking and are found all over Italy.

Online fraud

One recurring anomaly, similar to a well-known scheme, is that of various types of online fraud, especially involving subjects from certain areas of central Africa. This kind of fraud typically involves subjects in North America or northern Europe receiving funds (also via credit transfers) and the immediate use of the sums received via cash withdrawals or transfers to other accounts, or beneficiaries in Africa receiving money from subjects located in various parts of Italy who did not authorize the transactions. Sometimes these flows hide actual criminal organizations settled in the country that use other financial instruments, such as payment cards, not only to carry out fraud, but also for other crimes such as drug dealing or prostitution rackets. The most complex operations are located in Turin and in some parts of Campania.

Splitting of transactions

Another well-known anomaly is the artificial splitting of transactions that exceed the threshold imposed on money transfer operators in order to send money in a short period of time, while at the same time shielding the actual senders. This anomaly was particularly marked in the past for transfers to China made by senders of Chinese origin, with the complicity of agents often of the same nationality; over the last few years, however, transfers of this kind of flow, presumably of illegal origin, have been carried out using different channels that are possibly even more difficult to trace. In 2018, there was an increase in this type of anomalous money transfer, reported by money transfer operators based in Bologna and Rovigo.

Securities trading and market abuse

In 2018 too, some reports were analysed that highlighted suspicious transactions involving securities potentially related to cases of market abuse. Specifically, these reports looked at interlinked transactions using financial derivatives with low liquidity and that are traded very little, carried out via placing methods and with timeframes that are symptomatic of exchanges based on prior agreements. Financial analysis showed that sale prices were higher than the theoretical values of the underlying securities or that purchase prices were lower than such values. These practices generally resulted in the potential transfer of funds by means of the abovementioned agreed transactions, given the low liquidity of the financial instruments traded and the timeframe of the orders. This could also influence the market pricing mechanism for the financial instruments traded: this would seem to be supported above all by the evidence of transactions at higher and lower prices than the theoretical values that lead to a new maximum and minimum price for the instrument. In-depth analysis revealed that in some cases the seller and buyer were the same individual, which backs up the suspicion of 'wash trading', i.e. transactions that do not lead to an actual change in financial instrument ownership.

Computer fraud

In 2018, there was an increasing number of reports concerning the anomalous use of personal bank accounts and prepaid cards that could be traced back to computer fraud. In particular, the reports focus on the use of prepaid cards and personal bank accounts that

suddenly receive credits that are either quickly withdrawn in cash or transferred to third parties, sometimes abroad. More recently, conversion into virtual currencies has been used alongside the usual cash withdrawals. The account holders reported are often foreign citizens, unemployed or retired persons, or persons with a bad business record. The reporting entities detect inconsistencies in personal profiles during due diligence procedures, together with a sudden growth in transactions on personal accounts, which have often been recently opened for household expenses. The reconstruction of the financial flows, making use of the cooperation of foreign FIUs, made it possible to determine the fraudulent origin of the funds, which were subsequently split up and transferred using bank accounts and prepaid cards. The types of fraud detected in 2018 often included payments for supplies being diverted to IBANs other than those of creditors (e.g. a supplier company or the beneficiary of an insurance claim payment) via fraudulent access to communications with the debtor in order to change the bank account details and send the payment to someone else (the 'middle man').

3.3. Sectors and areas of emerging risk

Together with the known and consolidated risks, there is a constant focus on the emerging and innovative sectors, potentially the sources of new risks and opportunities for illicit uses.

Virtual assets

The reports concerning virtual currencies received by the Unit were submitted more because of a perception of the risks inherent to operational typologies than because of genuine suspicions, especially in cases of natural persons trading virtual currencies for investment or speculative purposes. However, there are cases where the investment in virtual currencies has anomalous features, such as the significant amounts involved or the context in which the transactions occurred. Some reports highlighted how subjects investigated for drug offences, money laundering and self-laundering are often involved in financial operations apparently connected with the purchase of bitcoins. The transactions registered on the bank accounts held by these subjects are characterized on one hand by significant and frequent cash deposits and withdrawals, not coherent with their business activity, and on the other hand by numerous credit transfers to and from foreign companies specialized in trading cryptocurrencies and bank accounts held by persons residing abroad involved in the same criminal proceedings. The international nature of the transactions carried out required cooperation from the FIUs of the countries involved in the financial flows.

Another case examined by the UIF concerned a company purchasing virtual assets worth a significant amount. The funds used for the purchase were provided by a sole counterpart and were transferred to the virtual currency buyers following multiple transfers involving subjects operating in the IT industry, previously reported to the UIF several times in connection with false invoicing/tax fraud. A further anomaly was found in the transactions following the purchase of virtual currencies, consisting in the immediate withdrawal of these funds without using the trading services provided by the IT platform used for the exchange.

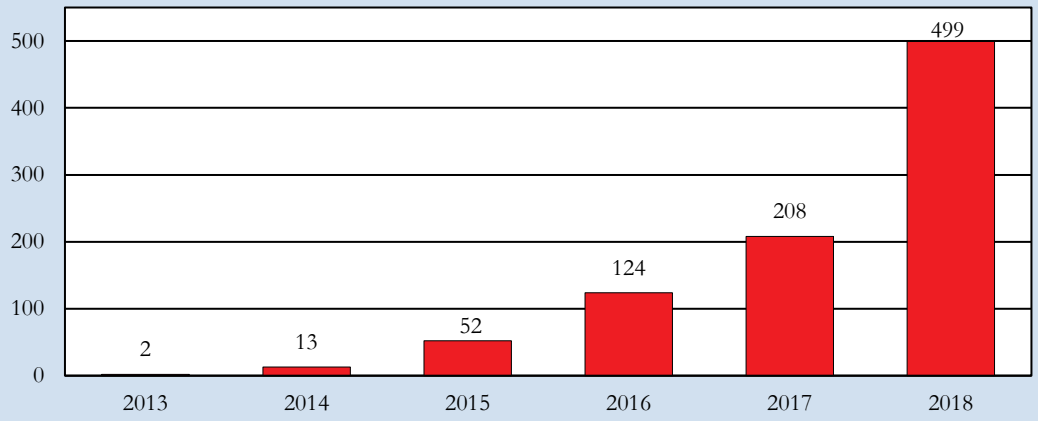
Given the expected progressive increase in the number of reports concerning virtual assets, the Unit began a survey in 2018 in order to better understand the importance and recurrence of these types of cases in the banking data, which has shown that the issue is still under-reported. This initiative was also based on an expected increase in the reports submitted by obliged entities operating in the sector, based on the requests sent by virtual currency exchangers to register on the UIF's Infostat platform (see the section on 'The reporting flows' in Chapter 1). Moreover, there will be further contributions to the sector from virtual

wallet providers who will become obliged entities as a result of the implementation of the Fifth Directive.

Suspicious transaction reports and virtual assets

The spread of virtual currencies and the inherent risks of these instruments given their specific characteristics in terms of potential uses for money laundering or the financing of terrorism led the UIF to launch a review in 2018 of the STRs involving virtual assets. An analysis of approximately 900 reports on this phenomenon dating back to 2013 shows a constantly growing trend, coupled with the gradual diffusion of this instrument and the growing attention paid to this sector by the financial world.

Number of STRs received referring to virtual assets



The STRs examined were mainly submitted by reporting entities belonging to the Banks and Poste Italiane category (95.5 per cent), with the rest being sent by payment institutions (2.3 per cent) and Electronic Money Institutions (1.3 per cent). Almost all of the cases observed described financial flows to or from virtual currency exchangers for the buying or selling of virtual assets, or for more complex trading transactions, presumably for investment or speculation purposes. The overall amount of the reported transactions in virtual currencies is approximately €96 million.

Analysis of the selected reports showed that in almost 70 per cent of cases, the persons reported, often young and likely to be more expert in using IT technology, were listed in the internal databases for operators exclusively because of transactions in virtual assets. Most of the reports examined, in particular the oldest ones, do not contain specific and detailed suspicions, but appear to have been submitted mostly due to the reporting entities not trusting this instrument, to the uncertainty about the sector regulations, or to the inconsistency between the virtual asset transactions carried out and the subjective and economic profile of the subject reported. In many cases, the suspicion focused on the origin of the funds used for virtual assets. The role played by some individuals often appeared to be significant, as they seemed to collect funds from numerous subjects, through split payments on prepaid cards, foreign credit transfers or repeated cash transactions, for small individual amounts but for significant sums overall.

Many reports were submitted due to suspicions of connections to illegal activities, especially the use of funds originating from clandestine commercial activities, often carried

out online, or from crimes such as fraud or cyber fraud. Examples include cases of trafficking cloned cards, online extortion requiring payment of ransoms in virtual currencies (ransomware), online sales of goods never delivered, phishing, and fraudulent activities traceable to pyramid schemes. In some cases, more complex anomalous elements were detected that are not attributable to a predetermined scheme. This refers to reports focusing on the misappropriation of public funds, transactions with counterparties in countries at risk or on contexts characterized by subjective links with forms of organized crime.

As regards the financing of terrorism, the STRs analysed did not provide a significant sample, since the suspicions raised by the reporting entity were only traced to this phenomenon in 15 cases. In strictly numerical terms, this figure would seem to confirm the idea that virtual assets are not easy for terrorists to use, especially those affiliated to ISIL.[16]

Among the 100 or so counterparties involved in the transactions reported and examined, over 77 per cent of the sums were attributable to nine recurring companies in particular.

Also in light of the new rules for prevention introduced by Legislative Decree 90/2017,[17] the UIF issued a new *Communication on the anomalous use of virtual currencies*[18] on 28 May 2019 containing, among other things, operating guidelines on how to make reports.

The emergence of new technology applied to the financial industry (FinTech) is drastically changing the world of payment services and subsequently the nature of the inherent risks of money laundering. Regulators and FinTech companies need to augment their cooperation in order to support the development of new services, while at the same time mitigating the relative risks.

FinTech payments and risks of money laundering

Until quite recently, payment services in legal tender were mainly provided by the banking system. Payment institutions (PIs) and Electronic Money Institutions (EMIs) have gradually begun to work alongside banks, but are different from banks because they have limited operations, reduced costs and a simplified organizational structure.

The long-established structure of the payment services market is rapidly changing with the advent of FinTech, which refers to the supply of financial products and services using information technology (cloud computing, the internet of things, big data, artificial intelligence, and so on). The opportunity to use mobile phones (and now smart phones)

[16] On this point see: *Terrorist use of virtual currencies* and the European Parliament study *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*.

[17] Virtual asset service providers (only as regards the conversion between virtual currencies and currencies that have legal tender) are included among the recipients of customer due diligence, and have obligations regarding the conservation of data, documents and information, and the reporting of suspicious transactions. They are subject to the regulations established for currency exchange and they must be included in a special section of the register kept by the OAM.

[18] The communication follows that of 30 January 2015, in which the UIF called the attention of those addressed by Legislative Decree 231/2007 to the need to monitor transactions in virtual currencies and to identify any suspicious elements, in order to prevent money laundering and the financing of terrorism.

to make payments has been facilitated by the introduction of near-field communication (NFC) and of biometric sensors (fingerprints, voice, facial and iris recognition, and so on) that allow the identification of customers and direct access to an account or to another device. Finally, the spread of Application Programming Interface (API) technology has enabled the development of applications for accessing bank accounts and the relative information. Further impetus to changing the structure of the payment services market came from the PSD2 directive (2015/2366), which was implemented in Italy with Legislative Decree 218/2017 and came into force in January 2018. The same decree adapted the internal measures included in IFR Regulation (2015/751). The Directive allows new operators to access information on bank accounts held by their clients and carry out transactions on their behalf.

The integrated use of these technological innovations for payments and the market access provided by PSD2 have facilitated the introduction of new types of services, the diversification of customer access methods, and the entry of new operators supplying this service, cooperating in various ways also with companies whose main activity is external to the financial world. These newcomers or Third Party Providers (TPPs) include Account Information Service Providers (AISPs), who provide account information services, and Payment Initiation Service Providers (PIPSs) who provide payment initiation services. The main services provided by TPPs are digital wallets, virtual spaces holding data on the user's bank accounts, payment instruments, electronic money and other information the user manages through applications or web services for sending or receiving payments and money transfers.

In the payment service market model led by FinTech, the data are the main source of value added and at the same time are the main source of risks concerning money laundering and of opportunities for combating it. The involvement of several operators in providing services creates a dispersion of the stored information, so far managed almost exclusively by the banking system, and of the responsibilities for preventing money laundering risks. The same financial transaction is no longer seen as such by customers as they have a much broader and complex experience regarding purchases. This may also mean less awareness of the risks of money laundering.

The UIF launched a close cooperation with operators for the purpose of sharing anti-money laundering strategies in the new context, and these operators report that the most problematic issues relate to the remote verification of customer identity and the uncertainty about the regulations applying to TPPs. It is also clear how, in the new context, the information essential for customer assessment is not so much that acquired during customer onboarding (the process of becoming a customer), characterized by more regulatory requirements, but that based on the customer's subsequent financial behaviour, at various points along the supply chain in the new market. The technology and characteristics of FinTech operators also provide more room for international regulatory arbitrage, thereby limiting the effects of national controls.

However, the effectiveness of tools for combating money laundering in various strategic areas and of the analysis of STRs could benefit from the availability of a large amount of data and the reduced costs of their management in the FinTech sector.

The payment services market is evolving rapidly and its borders are still difficult to trace, both in terms of the type of payment service providers and of the instruments provided. This makes it difficult to identify the anomalies and vulnerabilities concerning

money laundering and the financing of terrorism. The dynamism of the market requires flexible and complex prevention strategies. The obligations for operators should be accompanied by information and training on the awareness of risks and the ability to detect and identify them, and by an ongoing cooperation between the institutions and the market.

4. COMBATING THE FINANCING OF TERRORISM

Despite the progressive decline in the Islamic State at military level, which has led to a significant downsizing of its territorial ambitions, especially in the Middle East, the threat of international terrorism continues to remain high all over the world.

In Europe, the authorities assigned to combat terrorism have focused their attention above all on the specific threat of foreign fighters returning from conflict zones (returnees) and on the increasingly fragmented forms of terrorism, characterized by small local cells that may also be disconnected from international networks, and by subjects that increasingly act alone (lone wolves). The growth in radical religious feelings among the latter may take place in local communities and meeting places, in detention centres, and more and more often through self-indoctrination, made easier by the new means of communication.

In recent years, the UIF has responded to the evolution of terrorist threats by publishing specific indicators intended to strengthen the capacity of the financial system to intercept suspicious flows (UIF's Notices of *18 April 2016* and *13 October 2017*), and by refining its own reporting processes and tools, thereby enhancing domestic and international cooperation. In this context, the review of Legislative Decree 231/2007 (2017) has increased the opportunities for liaising with the other institutions involved in combating terrorism (the DNA and State security organizations).

4.1. Suspicious transaction reports

There were more than 1,000 reports classified by obliged entities as containing suspicions of financing of terrorism in 2018, an increase of 8.7 per cent compared with 2017 (Figure 4.1). As a result, the growth that started in 2015 and continued considerably in the following two years has consolidated, coinciding with the rise of ISIS and the bloody terrorist actions that have affected Europe.

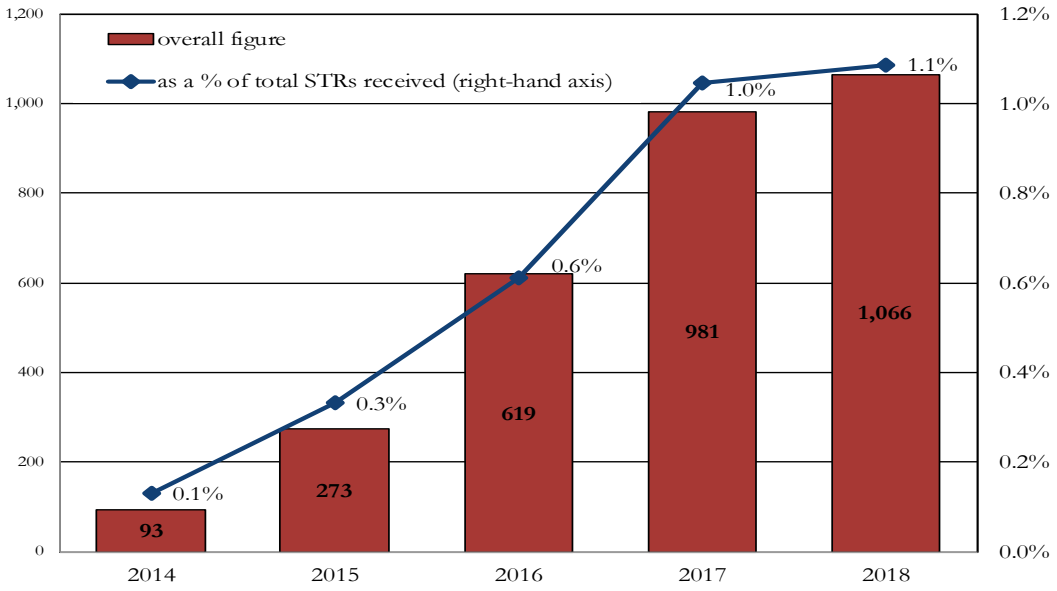
In the five years 2014-18, the reports involving the financing of terrorism increased more than tenfold, and the share of the total went from 0.1 to 1.1 per cent as a result of the increased responsiveness of obliged entities to suspicious financial movements, also helped by the publication of the UIF's Communications on the subject and by the adaptations of the intermediaries' data collection systems. The intensification of investigative and judicial activities against suspected terrorists and beneficiaries of preventive measures against radicalization has also contributed to this increase.

Types of reporting entities

Slightly less than 50 per cent of the reports received (514) were submitted by payment institutions and EU contact points, especially by money transfer operators, whose contribution - a 42.4 per cent increase compared with 2017 - has increased significantly since 2016, thanks to specific reporting mechanisms put in place by some institutions operating on a global scale (Table 4.1). The rest of the reports are almost entirely from banks and Poste Italiane (45 per cent of the total), the absolute number of which fell compared with last year (-16.5 per cent). The contribution from professionals and other non-financial operators (3.3 per cent of the total) which, by type of operations are less affected by the phenomenon, remains marginal.

Figure 4.1

Financing of terrorism reports received
(*absolute values and share in total*)



Reported transactions

The most frequently reported transactions are cash withdrawals and payments (34.3 per cent) and money deliveries and collections via money transfer circuits (26.2 per cent); the remaining transactions consist mainly of credit transfers (19.4 per cent, 3.5 per cent of which are foreign transfers) and cards and e-money use (15.9 per cent). The typologies of operations tend to reflect the socio-economic characteristics and financial habits of the persons reported (Figure 4.2).

Table 4.1

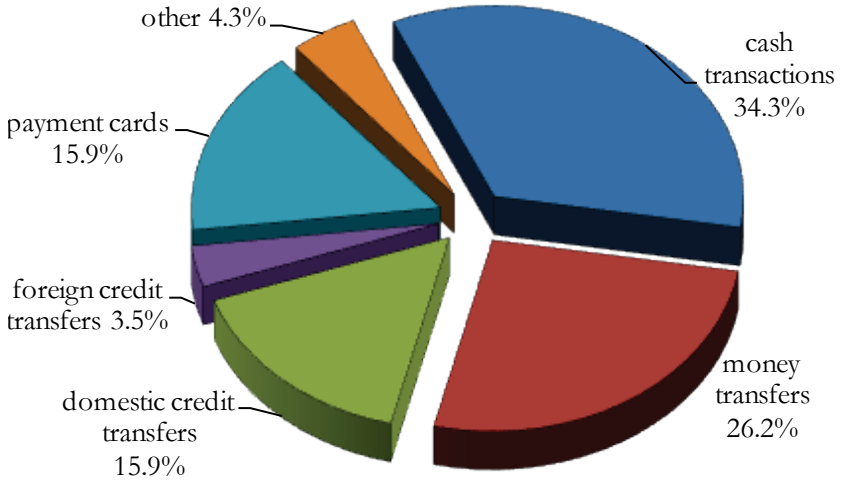
Reports on financing of terrorism by type of reporting entity

	2017		2018	
	(absolute values)	*(% share)*	*(abs. values)*	*(% share)*
Banking and financial intermediaries	**961**	**98.0**	**1,031**	**96.7**
Payment Institutions and contact points	361	36.8	514	48.2
Banks and Poste Italiane SpA	575	58.6	480	45.0
EMIs and contact points	1	0.1	17	1.6
Other intermed. and fin. operators (1)	24	2.4	20	1.9
Non-financial obliged entities	**20**	**2.0**	**35**	**3.3**
Notaries and Nat. Council of Notaries	18	1.8	12	1.1
Other non-financial entities (2)	2	0.2	23	2.2
Total	**981**	**100.0**	**1,066**	**100.0**

(1) Including financial intermediaries under Article 106 of the TUB, insurance undertakings, SGR, SICAVs and other intermediaries not included in the previous categories. - (2) Including gaming service providers, professionals and other non-financial operators not included in the previous category.

Figure 4.2

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

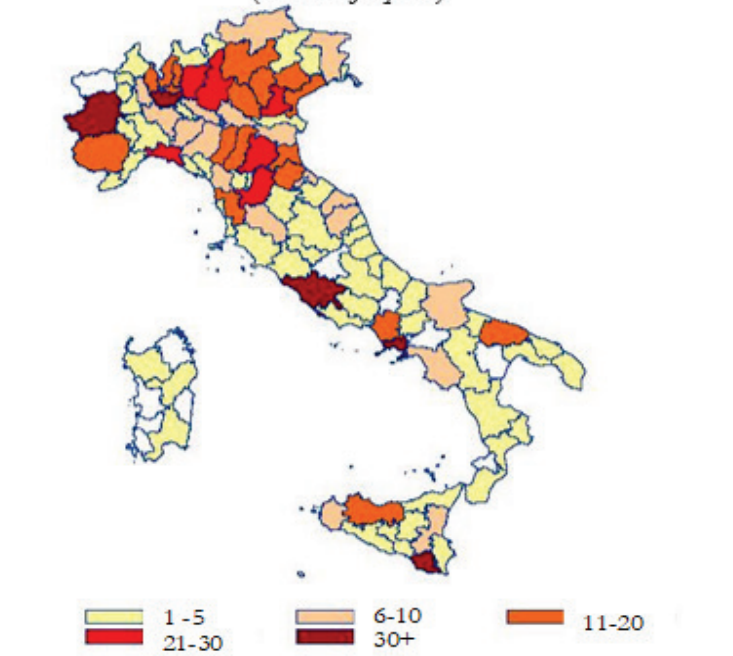


Territorial distribution

The territorial distribution of reports on the financing of terrorism tends to be characterized by a greater share in regions and province with a higher foreign population; one quarter of reports were from Lombardy (25.2 per cent), followed by Lazio (11.3 per cent), Emilia Romagna (9.8 per cent) and Veneto (8.5 per cent). The proportion of STRs in the southern regions is relatively lower, with the exception of Sicily (7.9 per cent; Figure 4.3).

Figure 4.3

Reports on financing of terrorism received by province
(*number of reports*)



The provinces with the highest numbers of reports, in addition to the large metropolitan areas and the northern industrial districts, also include parts of the Mezzogiorno (South) and the North, which, because of their geographical location, are known to be affected by transit migration and the associated criminal phenomena linked to immigration.

4.2. Types of operations suspected of terrorism

Compared with those of money laundering, the financial flows of terrorism may be of legal origin and, especially in the case of entities acting individually, are hardly relevant as regards the amounts. Money transfers are often implemented through non-traceable instruments (cash) or channelled into alternative money transfer circuits (hawala) which emphasize the mimetic aspect of the phenomenon, whose financial features are unlikely to be identified by systems for automatically detecting the abnormal transactions traditionally used by financial operators. It follows that the subjective element becomes the most common suspicious element, in many cases the only source for triggering the report.

Analysing reports on the financing of terrorism makes it possible to classify the reports into various recurring types, confirmed by the anomaly indicators of the financing of terrorism published in 2010 by the Bank of Italy, following a proposal of the UIF, and by the most recent Communications published by the UIF in 2016 and 2017.

Persons under investigation and included in lists

The most commonly identified type of report, in more than 50 per cent of the contexts reported, is that on the involvement of the clients of banks, payment service providers and other financial actors in court proceedings or investigative and preventive measures for terrorism or for religious radicalism. The public alarm associated with the terrorist threat results in a marked responsiveness on the part of the operators to news and to requests for information about their clients, which encourages them to carry out a careful examination of their customers' financial movements in order to support investigations.

Such reports, including the economic profile of those involved, are rarely characterized by complex transactions or significant sums of money. However, even in cases involving small amounts, the information potential of these reports has proven very promising for subsequent investigative activities, owing to the presence of clues, traces and financial links useful for interpreting behaviours, identifying possible suspicious activities and reconstructing their links, thus identifying possible networks of supporters and facilitators.

By far the most significant contribution to this type is still the one provided by some money transfer service providers, which a few years ago set up warning mechanisms triggered by requests for information on terrorist suspects received by the authorities. These mechanisms provide for the systematic reconstruction on a global scale of the money transfer networks involving entities under investigation by the authorities of various countries and their financial counterparties, and for the activation of the related reporting flows to all the FIUs of the States concerned in various ways regarding the transfers. This system makes it possible to considerably broaden the scope of the FIUs, which are made aware of the financial movements of persons under investigation abroad for terrorism and persons residing in their jurisdiction, who could be members or supporters of the same network.

Another recurrent type of case (10 per cent) originates in the system of international terrorism lists, which was a key area of protection adopted by the UN Security Council in the aftermath of the 2001 attacks. This system provides for the inclusion in public lists of persons convicted of terrorist acts, which impose the freezing of their funds and economic

activities, thereby blocking any further access to the financial system. In order to comply with these regulatory requirements, operators use a name database tracking system that identifies attempts to set up contracts or execute an out-of-account transaction by a designated entity, or transactions of their customers with this type of counterparty; in most cases, since operators do not have the full details, they turn out to be just homonyms.

Non-profit organizations

Another frequent case, though less so over the last two years, is that of reports referring to non-profit organizations of various types and of a religious nature (Table 4.2).

Table 4.2

Reports on non-profit religious entities (1)

	2014	2015	2016	2017	2018
Number of reports	30	50	125	81	71
Percentage share of the total reports classified as financing of terrorism	35.7	16.8	16.8	7.3	6.0

(1) The number and share are calculated also by taking account of STRs originally received under the category of suspicions of money laundering.

The Non-Profit Organization (NPOs) sector has always been at the centre of attention for the international bodies responsible for the fight against the financing of terrorism, not least because of the inherent vulnerability caused by exposure to certain specific risk factors. The FATF's Recommendation 8 emphasized, among other things, the risks of infiltration by terrorist organizations or individuals adopting radical positions, risks accentuated by the naturally international vocation of non-profit operators, and the ample availability of cash collected through donations from worshippers.

STRs on NPOs of a religious nature — not always classified under the category of suspected terrorism by obliged entities — originate in most cases from specific monitoring activities carried out by credit institutions on their current accounts and their representatives in order to detect anomalous financial movements in terms of size or characteristics that are not consistent with their corporate purposes or motives.

Operational anomalies

The most common anomalies, which take account of the anomaly indicators published in the Bank of Italy's Measure in 2010, include cash withdrawals and deposits for significant individual or overall amounts and domestic and foreign credit transfers with natural persons or with other associations. Transactions often arise from extraordinary collections of contributions from worshippers, to be used for purchasing and fitting out buildings as places of worship. In some cases, the report relates to the setting-up of new associations, where the funding arrangements are deemed suspicious due to the unclear origin of the funds.

The types described above, which all have individual suspicious elements in common (persons under investigation or designated persons, religious bodies), account for approximately two thirds of the total number of financing of terrorism reports. The remaining part is made up of reports resulting from operational anomalies based on suspicions of terrorism financing according to customer characteristics or behaviour or to the geographical element of transactions (risk countries).

Most of the cases are cash withdrawals or deposits of amounts not consistent with the subject profile, and the anomalous use of prepaid cards, which lend themselves to being used — especially in some immigrant communities — as a means for transferring money domestically, as part of activities that are not always lawful, through the reciprocal recharging of cards or cash refills followed by withdrawals. The classification of suspected financing of terrorism in this second group of typologies is mostly due to the fact that the customers reported are from geographical areas considered to be at risk. Suspicion can also be fuelled by the presence of transfers of funds nationally or across borders (domestic and foreign credit transfers, money remittances) between customers and third parties, especially if they are located in countries other than those of the customers and therefore not definable as remittance recipients. Sometimes suspicion can be justified owing to the behaviour of clients or overt manifestations of religious beliefs, made for example during the due diligence process.

In the absence of other more material elements, financial anomalies can in many cases be justified by the greater propensity of these clients – in part owing to cultural habits and fewer banking services – to use the abovementioned instruments and reciprocal loans or subsidies in lieu of traditional bank loans. In this context, a growing number of cases — which also involve numerous reports of money laundering — are those where transfers of funds between immigrants, set up by means of the alternative or sometimes combined use of prepaid cards and money transfer services, finally converge on the same entities that act as collectors. They then arrange to transfer the funds to the country of origin or to another country, making it possible to imagine the existence of organizations dedicated to managing alternative money transfer systems.

Hawala and the financing of terrorism

Emblematic of this type of set-up is Hawala, a system where funds are transferred through cash advances paid on trust among agents or hawaladars, and are then periodically cleared. In theory Hawala, if it were entirely managed in cash, might never intersect with the official financial system and thus not be detected by the reporting intermediaries, but in practice it can leave traces at both the collection stage (e.g. payment card flows or money transfer channels) and during the regular clearing phase (non-minimal amount external transfers to recurrent entities, identifiable as the corresponding hawaladars in foreign countries). In addition, in this system, the hawaladar that makes cash advances will of course need sufficient personal capital; finally, any trade activities carried out abroad will be useful for hiding the real reason for the periodical clearing.

Moreover, these informal fund transfer systems appear to be exposed to the risk of financing of terrorism, as seen at both international and national level. In particular, with reference to the Italian situation, recent investigations have revealed the existence of personal contacts between individuals linked to terrorist organizations and some hawaladars, thus providing investigative evidence for the assumptions made by UIF analysts in their technical reports. A scenario emerged in which funds for the financing of terrorism are entrusted to persons who, by transferring funds abroad for a profit, contact all kinds of clients indiscriminately, irrespective of the origin of the funding and of the economic rationale underlying the transfer. It follows that identifying forms of financial abuse, in particular in the transferring of funds to risk areas, for whatever purpose and regardless of specific suspicions of connections with radical environments or terrorist purposes, is instrumental in dismantling channels that are exposed to the risk of being used for the financing of terrorism. Therefore, for STRs referring to Hawala, also when sent by the reporting entities because of suspicions of money laundering, the financial analysis conducted by the UIF aims on the one hand, to reconstruct

the flows and the network of those involved by identifying and analysing the risk elements supporting the possibility of the financing of terrorism and on the other, to highlight the possible inclusion of financial abuse cases. The repeated mention of raising funds and their transfer abroad by recurring subjects (also via Hawala) suggests that they are operating on a stable basis for profit and for the benefit of third parties which, in the absence of the authorizations provided for by law, constitutes an unlawful exercise of reserved activities.

In light of this, the UIF carefully analyses the recurrence of such schemes in the reporting of suspicious transactions and in the subsequent financial analyses, regardless of the suspicion expressed by the reporting entity, especially when they occur in geographical areas at risk of financing of terrorism or in economic sectors that lend themselves to being used for trade-based terrorist financing: for example, the import-export, shipping or used motor vehicle and machinery sectors (see *Annual Report for 2017*, p. 72 and *Quaderni dell'antiriciclaggio, Analisi e studi*, No. 7, 2016, p. 43).

Over the past three years, following its participation in the working groups on this subject in international bodies and the experiences of the bloody attacks carried out in Europe, the UIF has raised awareness of the risk of financing of terrorism by creating a dedicated portal, constantly updated with documents from the most important international bodies. The UIF has also spread information in two Notices on the new risk factors relating to the phenomenon of foreign terrorist fighters and to the most recent phenomenon of returnees (see the beginning of the chapter). They draw attention to the unexpected behaviour of customers, which is symptomatic of the activity of foreign fighters upon departure or return (sudden liquidation of accounts, unjustified departures from Italy, non-payment of loan instalments, unusual ticket purchases and currency exchange requests). The indicators in 2018, similarly to the previous year, gave rise to a number of alerts, not always backed up by other risk elements that could help to orient the suspicion towards the financing of terrorism. In some cases, the presence of interesting financial or subjective elements led to the activation of targeted financial analyses, the findings of which were made readily available to the investigating bodies.

4.3. The UIF's analyses

The methods, pathways and tools for analysing financing of terrorism STRs, which are similar to those on money laundering, retain some specific features due to the characteristics of the phenomenon which, unlike money laundering, requires maximum exploitation of the subjective information and context (links) and of some information elements which may be of limited financial worth.

Since 2015, a dedicated area has been established within the UIF, which is also responsible for the financial analysis of STRs on money transfers, which are known to be more exposed to the risk of financing of terrorism and from which comes the greatest contribution in terms of information. The organizational choice contributes to developing specific knowledge and skills and to defining specific uniform practices, more oriented towards ensuring a more effective analysis of STRS. Those cases originally suspected of involving money laundering, but which have clear and significant connections — subjective elements, financial ties, strong operational connotations — with environments known for the financing of terrorism, or which are associated with religious associations, are also analysed. In this area, as in previous years, a large number of STRs on money laundering were reassessed in

2018; including these, the actual number of financing of terrorism reports would be 1,176 (1,106 in 2017).

In-depth financial analyses often involve a thorough reconstruction of flows on a broad spectrum, together with subjective profiling and the use of developed network analysis tools geared to analysing complex transfer networks. Financial analyses are a natural complement to traditional investigations, as they make it possible to detect subjective behaviour and links, also by going back in time and interpreting the financial traces.

The investigations carried out by the Unit on STRS have again highlighted, in particular in the provinces of the North and the Mezzogiorno affected by migration flows, the existence of criminal groups managed by foreigners, in some cases already reported to the UIF, having contacts with international terrorism.

For some years now, with a view to the prompt sharing of the most relevant information, an information alert mechanism has been active, through which the biggest risk contexts analysed by the UIF are forwarded to the Special Foreign Exchange Unit within the Finance Police (NSPV), also to enable the prompt dissemination of information to other authorities involved in the fight against terrorism.

4.4. Action at international level

The efforts to monitor financing of terrorism risks have continued at global level with the aim of identifying effective strategies for strengthening the prevention and combating of the financing of terrorism. In 2018, the FATF updated the Operational Plan for counter-terrorism, adopted in 2016 for the activities of the FATF and the Member States, within the framework of the Strategy on Combating Terrorism Financing, established in 2016.

Three lines of action are pursued: increase the effectiveness of the national implementation of standards, especially in the phase of inter-institutional investigations and cooperation; improve the assessment of the specific risks of terrorism and financing of terrorism; and facilitate the development of national systems for preventing and combating the financing of terrorism in line with the standards, especially in support of those countries with greater weaknesses in their systems.

The FATF published a report on the financing of recruitment for terrorist activities. This report explores how propaganda initiatives aimed at fostering radicalization and affiliation can be funded. Another document has been drawn up to define and share comprehensive strategies to combat the financing of terrorism ('Terrorist financing disruption strategies').

The FATF systematically updates the financing of terrorism typologies (*ISIL, Al-Qaida and Affiliates Financing*) and gathers together the experience of national authorities. Recent developments have shown that ISIL's loss of control over its territory is leading to a decrease in the resources stemming from the exploitation of the said territory.

Foreign trade is growing (especially oil); there has been an increase in the transfer (in cash or via Hawala) of previously accumulated funds to support local cells and to invest in trade or financial activities (currency exchange and money transfers). Kidnapping and extortion persist, and advanced payment and transfer instruments are also being used, albeit to a limited extent (e-money and virtual currencies).

The projects under way, in which the UIF is actively participating, are: 'Terrorist Financing Risk Assessment Guidance', 'The Criminal Exploitation of Virtual Assets for ML/TF Purposes', and 'Addressing Challenges with Investigations and Confiscation'. Projects have started on methods and instruments for confiscation in cross-border cases (Cross-Border Conviction-Based Asset Recovery) and on the carrying out of illicit trade-based financial activities. Work is also continuing through interaction with the private sector.

The fight against the financing of terrorism has continued in Europe, in line with the Action Plan adopted by the Commission in 2016. The lines of action set out include strengthening the cooperation between the competent authorities (especially the FIUs) and the prevention of anonymity in financial transactions.

As part of the work of the Egmont Group, the third phase of the ISIL Project (see *Annual Report for 2017*, section 5.4), currently under way, focuses on the financing of subjects (both lone wolves and small cells) that act in isolation or in any case without the support of organized structures. The analyses focus on suspicious transaction reports relating to persons involved in terrorist attacks, whose informative contribution is particularly important for reconstructing terrorist networks and identifying enablers.

The UIF took part in the ministerial conference entitled 'No Money for Terror', organized in Paris on 25 and 26 April 2018 by the Presidency of the French Republic. In line with the indications given by the G20, the conclusions of the Ministers from the 70 participating countries reiterate above all the need to adequately criminalize the financing of terrorism, to strengthen cooperation between authorities, and to increase liaison with the private sector.

4.5. International exchanges

As part of the Egmont Group's ISIL Project, now also geared to studying the financial support for foreign fighters, a group of FIUs, including the UIF, are engaged in a multilateral exchange of information on entities and activities potentially of interest, based on indicators that are broader compared with the actual elements of suspicion.

In 2018, the UIF received 124 requests and communications from foreign FIUs on financing of terrorism phenomena, of which 29 related to cross-border reports received from a European FIU and 22 were spontaneous communications relating to remittance networks created by potential terrorist facilitators: particular attention has been paid to remittances sent via the internet. In a very few cases, communications received from abroad also covered entities connected with internal terrorism of a subversive nature. The UIF made 49 requests with regard to the financing of terrorism, most of which were 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 has promoted a joint analysis exercise on transnational remittance networks linked to the financing of terrorism.

5. CONTROLS

5.1. Inspections

The UIF contributes to preventing and combating money laundering and the financing of terrorism, in part through on-site inspections of entities subject to reporting requirements.

An on-site inspection is a non-routine prevention tool used in conjunction with off-site assessments to verify compliance with the active cooperation obligations and to obtain important information on operations and phenomena. By means of on-site inspections, the UIF's objective is to strengthen active cooperation among reporting entities and to improve the quality of their contribution.

The Unit conducts general inspections to examine at-risk sectors and operations more closely, and to check that the procedures for reporting suspicious transactions are adequate and that the active cooperation obligations are being fulfilled. It also carries out targeted inspections to reconstruct financial flows relating to specific operations, supplementing the information acquired during the analysis of STRs or received from foreign FIUs, or arising from cooperation with the judicial authorities, investigative bodies and the sectoral supervisory authorities.

The UIF carries out inspections by means of a risk-based planning, which takes account of the degree of exposure to the risks of money laundering and financing of terrorism of the various categories of obliged entities and of the control measures of other authorities.

In 2018, the UIF carried out 20 on-site inspections, of which 18 were general and 2 were targeted; the latter were carried out in connection with irregularities arising from specific operational points and with the involvement of intermediaries' clients in judicial proceedings (Table 5.1).

Table 5.1

Inspections

	2014	2015	2016	2017	2018
Total	**24**	**24**	**23**	**20**	**20**
Banks	12	4	8	4	8
Trust companies	3	3	4	4	3
Payment Institutions and other financial intermediaries	-	9	3	3	2
Asset management companies and SICAVs	3	2	1	-	4
Insurance companies	-	2	-	6	-
Other entities (1)	6	4	7	3	3

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

On-site inspections were geared to detecting emerging risks in activities that are more vulnerable to money laundering and the financing of terrorism, or to those entities subject to the rules that are less aware of the operational aspects of active cooperation obligations.

The intermediaries to be inspected were chosen by taking several factors into account that could be indicative of possible shortcomings in active cooperation: the absence or small number or poor quality of the suspicious transaction reports; references in reports transmitted by other obliged entities; anomalies detected by analysing the aggregated data; the presence of detrimental information on the intermediary or on its customers; and specific information or requests from investigative bodies or sectoral supervisory authorities. As inspection activities cover extremely diverse contexts, an effective cooperation with the sectoral supervisory authorities, the Special Foreign Exchange Unit of the Finance Police and the Customs and Monopolies Agency has made it possible to fully exploit their respective expertise in a multidisciplinary way.

In 2018, controls on Italian branches of EU intermediaries were stepped up, also with a view to detecting anomalies arising from asymmetries in national regulatory frameworks, which favour arbitrage and elusive behaviour. In this context, financial flows relating to the operations of service providers involving the use of virtual currency were also examined.

In relation to the anomalies detected in operations with foreign countries and counterparties at high geographical risk, the UIF carried out inspections on intermediaries involved in foreign trade and correspondent banking. Areas of weakness emerged in these sectors as regards the ability to detect possible suspicious patterns, mainly due to the non-use of all the information available in the different departments, the adoption of a purely formal approach to counterparty verification activities, as well as the absence of appropriate anomaly indicators in the internal procedures. Integrated assessment processes need to be adopted in the letters of credit sector that take into account the specific characteristics of the countries involved, the standing of the counterparties and the appropriateness of the prices of goods for sale.

The monitoring of trust companies also continued, subject to the supervision of the Ministry of Economic Development. The inspections revealed weaknesses in active cooperation obligations due, among other things, to the lack of adequate information systems for properly assessing customer risk, to an excessive reliance on the information on the origin of the funds provided by the other intermediaries involved in the operation, and to a lack of attention to prevention issues.

The first round of general inspections was concluded on the main gaming and betting licensees, selected in cooperation with the Customs and Monopolies Agency. The inspections showed that, in a sector that is particularly vulnerable to the infiltration of funds of illicit origin, the AML function is often centralized and undersized, with inadequate tools for monitoring and controlling distribution networks. One of the main problems found was the lack of in-depth information on the subjective profile of customers and/or contracted entities, in particular as regards detecting connections between those responsible for the operational points and the activities carried out there.

As a result of the inspection activities, the UIF provided information to the supervisory authorities on their respective areas of competence, as well as to the judicial authorities on matters of a potentially criminal nature. The parties inspected were informed of the shortcomings identified and asked to take the necessary corrective measures. Action was also taken to sanction administrative violations in their spheres of competence.

5.2. Sanctions procedures

The anti-money laundering system envisages a complex system of administrative sanctions designed to punish violations of its obligations. The UIF ascertains whether there has been a violation of the obligation to report suspicious transactions and, depending on the violation, informs parties of the allegations against them and submits the alleged violation to the MEF or the sectoral supervisory authority so that they may impose the sanctions envisioned under the law.

The sanction measures for which the UIF is responsible have a significant enforcement and deterrence function, but it is only complementary to that deriving from the overall system of organizational safeguards imposed by legislation, from the controls performed by various authorities and from criminal penalties.

In 2016, a total of eight proceedings were initiated (all following on-site inspections) for the application of pecuniary administrative sanctions for failing to report suspicious transactions (Table 5.2). The proceedings involved suspicious transactions not reported, for a total amount of approximately €2.3 million.

Table 5.2

Administrative irregularities

	2014	2015	2016	2017	2018
Failure to report a suspicious transaction	11	32	17	17	8
Failure to transmit aggregate data	-	-	1	-	1
Failure to report a transaction in gold	8	7	5	5	26
Failure to freeze funds and financial resources	8	10	8	5	-

The marked decrease in this figure compared with previous years is mainly due to the reform of the sanctions system pursuant to Legislative Decree 90/2017, which introduced a dual competence for the MEF and for the supervisory authorities for violations of active cooperation committed by supervised entities. On the basis of the outcome of its controls and after having assessed whether the case in question falls under the competence of one or the other authority, the UIF informs the subjects concerned and sends the information to the MEF for any sanctions to be imposed, or submits the alleged violation to the sectoral supervisory authorities for it to be disputed or for sanctions to be imposed. The complex organization of sanctioning powers has made it necessary to strengthen cooperation between the authorities at operational level, including through reciprocal participation in the respective collegial bodies entrusted with assessing irregularities.

With reference to the law on gold trading (see Section 6.3 'Gold trade declarations'), the UIF runs the investigations for sanction procedures, also initiated by other authorities, and sends the relevant documents to the MEF, together with an explanatory report on its findings. In 2018, the Unit sent documents on 26 sanctions procedures to the MEF. Of these cases, 11 refer 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 attention of the

UIF by the Finance Police. The MEF agreed with the UIF's line of interpretation for these cases, according to which operations of this kind, irrespective of the delivery of gold to the purchaser, must be regarded as non-financial transactions subject to the declaratory obligation under Law 7/2000.

6. STRATEGIC ANALYSIS

International standards place strategic analysis among the official duties of the FIUs together with operational analysis. In line with these principles 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 by examining suspicious transaction reports, by analysing aggregate reports (SARA), from operational activity, from collaboration with national and international authorities and from the 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 the priority objectives to be pursued. Strategic analysis also uses quantitative methods, such as econometric techniques and data mining tools, in order to identify trends and anomalies on a statistical basis.

The purpose of strategic analysis includes the assessment of the risk of involvement in money laundering and financing of terrorism operations in the financial system as a whole, or of geographical areas, means of payment and specific economic sectors, as well as the identification of situations and contexts that may be subject to further targeted studies.

6.1. Aggregated data

SARA reports are submitted monthly by financial intermediaries and are derived from an aggregation of data on their operations in accordance with criteria laid down by the UIF in its *Measure*. They cover all transactions initiated by customers for amounts (also split up) of €15,000 or more.

The data are aggregated and anonymous and cover the full range of payment instruments and financial transactions. The aggregation criteria for SARA data are mainly related to the means of payment used, the location of the reporting branch, the business sector and the residence of the customer, and the location of the counterparty and its intermediary (in the case of wire transfers). Data refer to both incoming and outgoing transactions and report separately the amount, if any, of cash transactions.

SARA data

The amount of SARA aggregated data received by the UIF remained broadly stable at about 100 million in 2018, representing a total of more than 330 million individual underlying transactions; there was a slight increase in the total amounts reported (€30 trillion; +4 per cent). The number of reporting intermediaries decreased further compared with the previous year, mainly owing to mergers and acquisitions (-4 per cent). The banking sector continues to account for 95 per cent of the data records submitted and 97 per cent of the amounts reported (Table 6.1).

As of this year, trust companies set up pursuant to Article 106 of the Consolidated Law on Banking (TUB) are presented as a separate category, owing to the importance they have

achieved in terms of number of intermediaries and of reported volumes. The category of electronic money institutions reported the greatest increase in terms of amounts (€8 billion) and transactions (more than 670,000). This increase, mainly recorded in the second half of 2018, is attributable in particular to specific operators.

Table 6.1

Aggregate anti-money laundering reports (SARA data)

TYPE OF INTERMEDIARIES	**Number of reporting entities in the year**	**Number of aggregated reports sent** (1)	**Total aggregated reports sent** (*billions of euros*)	**Number of transactions underlying the aggregated reports**
Banks, Poste Italiane and CDP	571	97,624,486	29,098	305,595,629
Trust companies under Law 966/1939	218	49,913	28	153,303
Asset management companies	193	1,419,283	208	6,447,402
Financial intermediaries under Article 106 of the TUB	205	1,363,156	314	4,802,629
Investment firms	121	170,180	97	4,339,569
Insurance companies	75	1,358,070	130	2,599,976
Payment institutions	54	701,956	38	7,690,457
Electronic money institutions	8	54,882	8	670,920
Trusts, pursuant to Article 106 of the TUB	39	111,597	85	444,194
Total	**1,484**	**102,853,523**	**30,006**	**332,744,079**

(1) The individual data item of SARA is calculated by the reporting agency by grouping single transactions according to precise criteria. SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 7 March 2019.

The UIF provides administrative and technical support for reporting entities: in 2018, it received around 1,500 requests for assistance.

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

Cash transactions have been decreasing for several years and in 2018, they stood at €204 billion, marking a 3 per cent decrease compared with 2017. This reflects both the increasing diffusion of alternative means of payment and the effectiveness of the monitoring by financial intermediaries and control authorities of possible illegal uses.

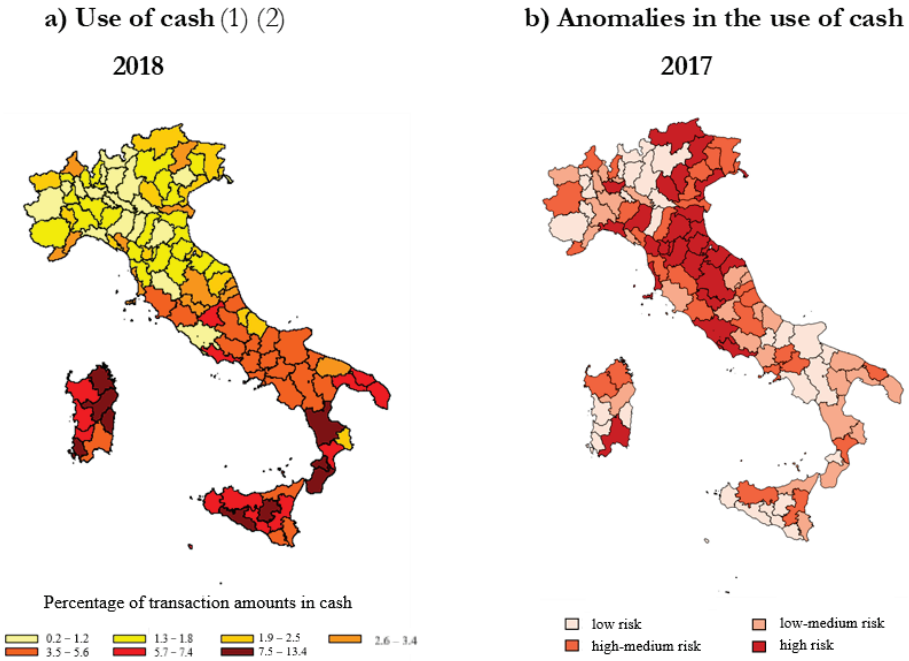
The amounts of withdrawals and cash deposits remain asymmetrical due to the intrinsic characteristics of the data: withdrawals, which are usually more fragmented and thus fall under the SARA reporting threshold, recorded a total volume of €12 billion (€14 billion in 2017), while the total for deposits stood at €192 billion (from €196 billion).

Anomalies in the use of cash

The geographical distribution of cash use remains highly uneven (Figure 6.1a), primarily owing to differences in the local economies, in people's habits, and in the availability and supply of financial services. By using econometric models, it is possible to exclude structural determinants from transactions; the remaining transactions, potentially abnormal as they cannot be attributed to a physiological use, may be symptomatic of unlawful conduct. Risk indicators are defined based on the importance of these anomalies at provincial level (Figure 6.1b; see the box 'Anomalous use of cash').

Figure 6.1

Use of cash and anomalies, by province



(1) Share of cash transactions in total transactions. — (2) The SARA data used do not include transactions carried out by general government or by financial and banking intermediaries resident in Italy, in the European community or in countries considered equivalent by the Ministerial Decree of 10 April 2015, in line with 2017 data. The SARA data are subject to correction by the reporting agents; the data used in this chapter are updated to 7 March 2019.

Although the two maps in Figure 6.1 refer to successive years, a comparison can be made.[19] As is well known, the use of cash is higher in the South (left-hand map); in contrast, when account is taken of the economic and financial fundamentals to exclude the effects of physiological uses from the data, the territorial distribution of unexpected and abnormal uses – estimated for 2017 – actually shows a concentration of high-risk provinces in the North

[19] The chart shows the 2017 map, since it is the most recent year for which all the data needed to estimate the model are available. Moreover, the preliminary results on the anomalies identified in 2018 show a provincial risk map that does not differ markedly from that shown in Figure 6.1.

and Centre, whose rich economies lend themselves to a growing criminal infiltration (right-hand map).

Credit transfers are another payment instrument recorded in the SARA data, which are of particular importance in the effort to counter financial crime. The information content of credit transfer reports is extensive, and includes details of the municipality (or foreign country) of residence of the counterparty and of the bank involved. This wealth of information makes it possible to produce statistics and correlations based on the geographical origin and source 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 connected to the opacity of their fiscal and financial systems.

Credit transfers to and from foreign countries

The total value of credit transfers to and from foreign countries exceeded €2,700 billion, with an increase of 6 per cent compared with 2017. Specifically, outflows reached €1,300 billion, compared with almost €1,400 billion for inflows (Table 6.2).

Table 6.2

Outgoing and incoming credit transfers, by country of destination and origin (1)

Credit transfers abroad	**Amounts** (billions of euros)	**Inward credit transfers**	**Amounts** (billions of euros)
Total	1,325	**Total**	1,396
to EU countries	999	**from EU countries**	1,035
United Kingdom	306	United Kingdom	322
Germany	229	Germany	215
France	190	France	213
Belgium	68	Belgium	67
to non-EU countries	326	**from non-EU countries**	361
United States	133	United States	133
Turkey	49	Turkey	49
China	17	Japan	21
Japan	5	China	10
***of which*: tax havens**	81	***of which*: tax havens**	86
Switzerland	38	Switzerland	41
Hong Kong	13	Serbian	13
Serbia	13	Hong Kong	9
Singapore	4	Abu Dhabi	6

(1) See footnote 2 to Figure 6.1.

In 2018, there was once again a high concentration of flows with EU countries, which are Italy's main trading partners. In addition, there are non-EU countries, including the

United States and Turkey, with which the volumes of trade increased by more than 40 per cent in both directions.

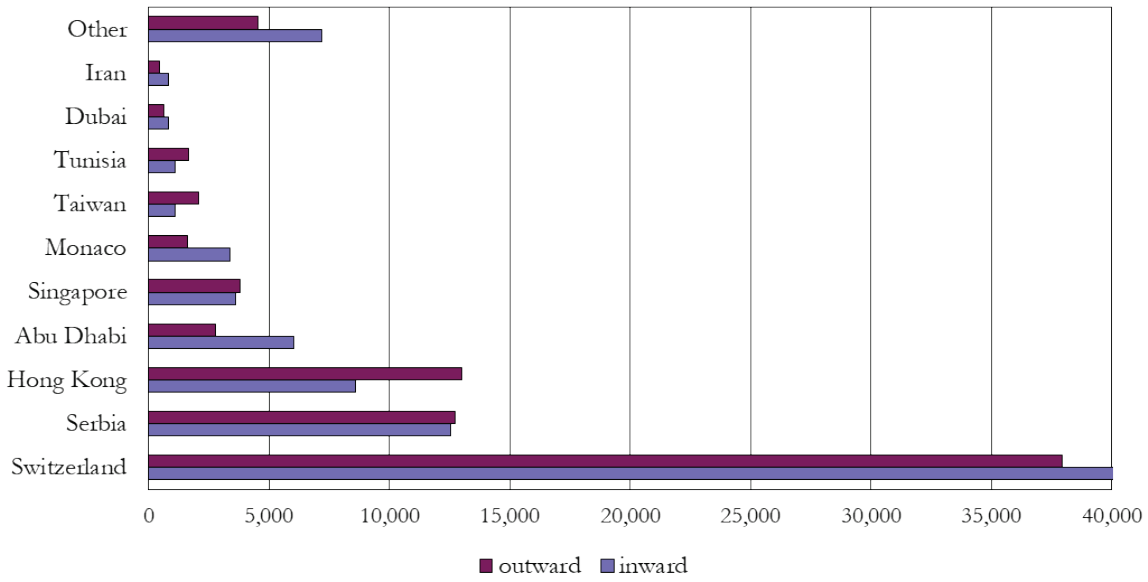
Flows with tax havens

The volume of financial flows with tax havens or non-cooperative jurisdictions increased, having been significantly affected by the changes made to the reference lists for 2018.[20] Inflows and outflows increased by 21 and 30 per cent respectively compared with 2017, mainly owing to Serbia and Tunisia joining the main counterparty countries (Figure 6.2). In contrast with last year, financial flows to and from Iran fell sharply to €850 and €480 million (-10 and -13 per cent respectively), probably due to new international political tensions with this country.

Figure 6.2

Credit transfers to/from tax havens and non-cooperative jurisdictions (1)

(millions of euros)



(1) See footnote 2 to Figure 6.1.

Anomalies in financial flows

The provincial distribution of flows with tax havens or non-cooperative jurisdictions continued to be uneven both for outward and inward credit transfers: provinces with peaks in the share of these flows are found all over Italy (Figure 6.3a). As with the use of cash, it is possible to identify the component explained by the economic and financial fundamentals for foreign credit transfers as well (in this case, those of the provinces in Italy and in the foreign countries affected by the various flows). The differences between observed and expected credit transfers based on econometric models can be used as anomaly indicators (see *Annual Report for 2017*, pp. 85-86). The share of anomalous flows at provincial level (corre-

[20] The list of non-cooperative countries and/or tax havens included in the Glossary is taken from the ministerial decrees implementing the Consolidated Law on Income Tax (TUIR) that came into force on 31 August 2018, and from the list of high-risk and non-cooperative jurisdictions published by the FATF in February 2018, alongside the publication of the statistics for 2018 in the UIF's *Quaderni Antiriciclaggio*, Dati statistici. Serbia, Tunisia, Sri Lanka and Trinidad and Tobago have been added to the list since 2017.

sponding to the biggest differences estimated for 2017) is shown in Figure 6.3 for both inward and outward flows for Italy: it represents the distribution of the risk of money laundering associated with financial flows abroad.

Figure 6.3

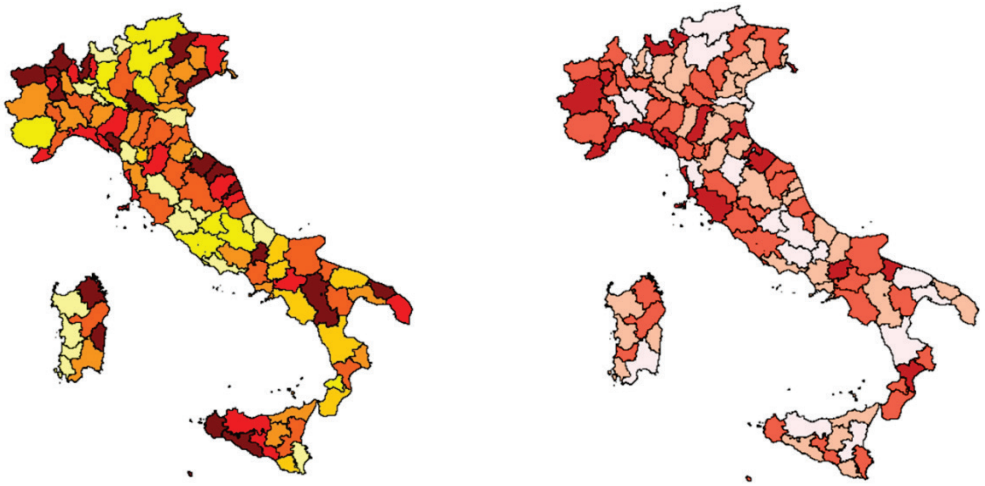
Credit transfers at risk

a) Share of credit transfers with countries at risk on total foreign credit transfers (1)

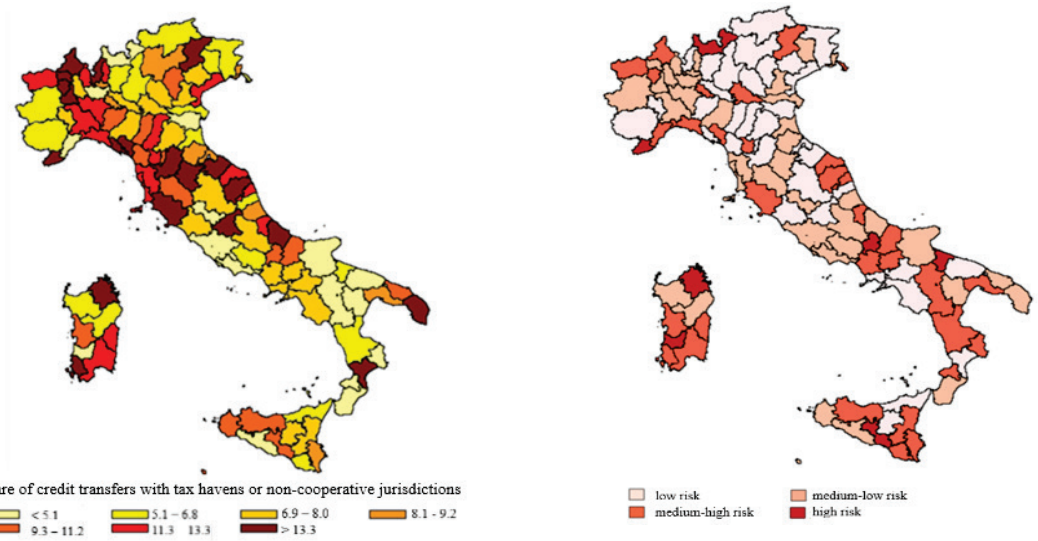
b) Anomalies in foreign credit transfers

2018 **2017**

Outward credit transfers



Inward credit transfers



(1) See footnote 2 in Figure 6.1. The countries at risk used in the left-hand maps are tax havens or non-cooperative jurisdictions.

The anomalies in outgoing flows are concentrated in economically advanced provinces in the North and Centre, those in incoming flows in the South and the Islands; in both cases, the incidence of anomalies is also high in provinces bordering countries at risk (Monaco and Switzerland). In line with this situation, the correlation between anomalous flows and reports of specific crimes shows that anomalous outgoing flows are more frequent in provinces with bigger illicit goods and services markets (e.g. the drugs trade and prostitution), while incoming anomalous flows are more frequent in provinces that are more under criminal control (e.g. extortion crimes).

6.2. Analysis of aggregated data and study activities

Data quality is essential for ensuring the reliability of the 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 further investigation 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 against their own reporting patterns over the previous 12 months.

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

The UIF continues to work on the study of phenomena and financial conduct of interest based on econometric techniques, with the twofold aim of increasing knowledge of specific phenomena and of providing operational guidelines for preventing and combating money laundering. These findings are used internally to identify sectors and geographical areas at risk and cases in need of closer scrutiny. The evidence is also shared with other AML authorities in accordance with their respective functions. The methodology and the general findings are published in the 'Analisi e studi' collection of the *Quaderni Antiriciclaggio*.

Statistical checks on data accuracy

The statistical checks carried out in 2018 identified around 25,000 potentially anomalous aggregated data (27,000 in the previous year). Some 844 reporting entities (of which 526 were banks) were requested to verify these data: errors were only found in 5 per cent of the data and the necessary corrections were made. In 260 cases (around 1 per cent of the total), the verified data were found to be related to STRs already sent to the UIF; in a further 190 cases, the reporting entities reviewed the related transactions to decide whether to submit a suspicious transaction report.

Anomalous use of cash

The updating of the model for analysing anomalous uses of cash was recently completed. A new econometric methodology produced ML risk indicators, taking into account the operations of each financial intermediary within each Italian municipality.[21] This makes it possible to obtain more detailed operational guidance for the prevention and combating

[21] The previous version of this study enabled ML risk indicators to be defined, but only up to the highest level of territorial detail in the municipalities: see Ardizzi G., P. De Franceschis and M. Giammatteo (2018), 'Cash payment anomalies: An econometric analysis of Italian municipalities', *International Review of Law and Economics*, 56, pp. 105-121.

of money laundering, above all by the Unit, but also by the other authorities and the reporting entities.

Anomalous use of cash

The study updates and refines the work published in 2016, which enables the identification of cash flows that are not consistent with socio-economic and financial fundamentals and are therefore potentially linked to illegal activities. A new methodology is proposed to detect anomalies in the use of cash at a higher level of detail, i.e. for each bank in each municipality. The ML risk indicators obtained are thus even more detailed tools for guiding the action of the authorities and the intermediaries involved in preventing and combating money laundering.

The variable that the new model seeks to explain is the ratio between cash deposits and total deposits other than cash (cheques and credit transfers), as observed at bank counters. This 'propensity to use cash' measure is linked to various explanatory variables. Compared with the previous model, an indicator of the overall amount of the financial transactions of each branch has been added to the economic and financial fundamentals observed locally, namely the taxable income, the value of deposits other than cash deposits and the number of bank branches. Among the other explanatory variables, the bank classification of individual intermediaries (defined based on the operational scale, type of activity and geographical location) has been added to the variables representing the shadow economy and the geographical connotation of the municipalities. The specification of the model was initially selected based on the 2015 data; the model thus obtained was then estimated on the 2017 data, using the updated information.

Hence, the model allows us to estimate, at the level of each individual bank in each municipality, the share of 'propensity to use cash', which is explained by the structural factors and as such is physiological. It is therefore possible to identify — using the difference compared with the observed cash use — the anomalous or non-justifiable component based on the fundamentals, and potentially deriving from the proceeds of illegal activities.

By aggregating the new results, it is possible to derive risk indicators for individual intermediaries, as well as to update and refine the indicators at municipal and provincial level that were obtained with the old methodology.

The measures thus obtained were validated by crossing independent ML and crime indicators: specifically, the risk indicator derived from the study is related at provincial level to: (i) measures of ML activities, such as the number of suspicious transactions reported to the UIF; and (ii) territorial indicators of criminal activities such as reports of selected crimes (drug trafficking, money laundering, exploitation of prostitution, extortion and mafia-type criminal association).

In addition, the provincial map of ML risk drawn up on the basis of the study is consistent with the investigative and judicial evidence available: the most anomalous provinces are largely the same as those with a greater mafia presence, both in the traditional territories of origin of Italy's criminal organizations and in the other areas of the country where they have subsequently extended their influence.

A second econometric study, developed in collaboration with the Bank of Italy's Directorate General for Economics, Statistics and Research, is the first empirical verification

Impact of inspections

of the effect on the reporting activity of banks stemming from the inspections by the anti-money laundering authorities.[22] The data on the number of STRs received by the Unit were used, as were the SARA data on the financial transactions of banks and information on anti-money laundering inspections carried out by the Bank of Italy's supervisory directorates and by the UIF and on the relative results for the two years 2012-13. The results show that the inspections lead to an increase in the number of STRs and in the probability of a suspicious transaction being reported. The increase in reports is not at the expense of their quality or importance, with equal measure given not only to those with a low information content but also to those at high risk (as measured by the UIF rating; see Chapter 2 'Operational analysis'). The impact of the inspections was observed mainly in conjunction with the implementation of some form of intervention by the authorities (from a warning letter to starting a sanctions procedure).

Analysis of the balance sheets of infiltrated companies

The initial results of the study that the Unit is completing on the balance sheets of firms infiltrated by organized crime are available. Starting with the various judicial proceedings (preventive seizures and confiscation orders) conducted in the decade 2007-2017, a sample of companies controlled by organized crime was defined: the balance sheet data make it possible to identify recurring factors in the financial position and management of these companies.

The various ways that organized crime infiltrates companies are identified. Firstly, companies can be identified that have a predominant position in their market achieved by using the mafia method to the detriment of competitors; these companies typically show a higher turnover than the corresponding healthy firms, but also higher labour and intermediate goods costs. Against this background, it can be assumed that the remuneration of labour and suppliers is inflated to pay the criminal workers and to distribute the profits surreptitiously, thereby reducing balance sheet profits and the payment of the relative taxes. A second category of companies is the one that the mafia runs for the sole purpose of investment, abandoning violence and intimidation and almost completely camouflaging itself in the legal economy: the fiscal indicators of these companies are therefore more or less similar to those of other companies. There has also been a dynamic analysis of balance sheets, which has shown that the attack on the part of organized crime focuses on companies in economic and financial difficulty: the decrease in turnover and capital typically recorded before infiltration is followed by a rapid recovery in the following years, with a concomitant increase in labour costs.

Risk indicators for non-bank intermediaries

As part of the work on drawing up synthetic money laundering risk indicators and in collaboration with the Bank of Italy's supervisory directorates, the UIF launched a project to expand the set of indicators already in use for anti-money laundering controls on banks. The project will extend the calculation of the synthetic risk measures to non-bank intermediaries as a whole. The results will help to enrich the information already used to support the assessments of money laundering and financing of terrorism risks in the financial sector, with a view to increasing the effectiveness of the authorities' controls by adopting a risk-based approach.

Big data

The Unit continued to take part in the Bank of Italy's trial on the opportunities for using analysis methodologies based on big data. In particular, it consolidated the exploitation

[22] Gara M., Manaresi F., Marchetti D.J. and Marinucci M. (2019), 'The impact of anti-money laundering oversight on banks' suspicious transaction reporting: Evidence from Italy', UIF, *Quaderni dell'Antiriciclaggio, Analisi e studi* No. 12.

of the dedicated platform set up by the Bank's Directorate General for Information Technology, which enables big data methods to be applied to the most recent SARA reports for identification for AML purposes of any peaks, anomalies and correlations of interest at territorial or sectoral level.

Some trials have shown that the adoption of new technologies and methodologies in the search for anomalies saves up to two thirds of processing time compared with the use of traditional techniques and software.

Other activities

The UIF once again participated actively in national and international academic debates on topics related to its activities. The organization, together with the British research centre RUSI (Royal United Services Institute for Defence and Security Studies), of the Workshop on the 'Contribution of advanced analytics to AML supervision and enforcement' was particularly important.

In June 2018, together with the British think-tank RUSI, the UIF organized an international Workshop in London on the application of advanced quantitative methods in the anti-money laundering field by the authorities and reporting entities (SupTech and RegTech). The conference brought together central banks and financial authorities (including the Bank of England and the FCA), British government institutions (including the Treasury, the Home Office and Customs) and European Union institutions (the European Commission and Europol), as well as FBI representatives, universities (such as University College London, Bocconi University and the Max Planck Institute), and some of the main international intermediaries. The opportunities that technological and scientific progress offers to authorities and the private sector in the field of compliance and anti-money laundering controls were debated, and the use of new techniques for analysing financial transaction data on a large scale was discussed further. Some of the participants made presentations on their experience and contributed different points of view to the subject under discussion at the meeting. The UIF presented the ML risk indicators developed for the banking sector in cooperation with the Bank of Italy's supervisory authority.

Again in 2018, the UIF was invited to present its analysis and study work at national and international scientific conferences. Some works were selected for presentation at the fourth international conference on 'Governance, Crime and Justice Statistics' (UNODC), at the sixth international Workshop on 'Computational Economics and Econometrics' (IRCrES-CNR), at the annual conference of the 'European Association of Law & Economics' (EALE) and at the Workshop on 'Harnessing big data & machine learning technologies for Central Banks' (Bank of Italy). The UIF was invited for the second time to take part in the meeting of experts – organized in Geneva by the UNCTAD and the UNODC – to define the 'Indicators of illicit financial flows', which is one of the areas for action set out in the UN's 2030 Sustainable Development Agenda.

Cooperation has recently started between the UIF and the BIS's Financial Stability Institute on the application of big data analysis techniques in the fight against money laundering and financing of terrorism. To this end, a representative of the UIF was invited in the role of fellow to carry out a joint research project to produce an international review of the use of these methodologies.

6.3. Gold declarations

The law governing the gold market in Italy provides that transactions involving investment in gold or gold materials for mainly industrial uses (other than jewellery) should be declared to the UIF. This requirement applies to the cross-border trade or transfer of gold for amounts of €12,500 or more. There are two types of declaration: monthly declarations, submitted for all transactions made in the reference period; and 'advance declarations, submitted prior to a physical transfer of gold out of the country. Advance declarations are only for physical transfers of gold abroad, which must be submitted to the UIF before any gold crosses the border. If the gold is not being transferred to a new owner, the advance declaration is the only source of information for such transfers.

The competent authorities have access to these declarations not only for anti-money laundering purposes, but also to counter tax evasion and for reasons of public order and public safety.

In 2018, the value of gold sales transactions remained stable at €13 billion. The fall in prices (-4 per cent on average, in line with market prices) and in the number of transactions was offset by a sharp increase in the average amount per transaction (Table 6.3).

Table 6.3

Declarations of monthly gold transactions

TYPE OF TRANSACTION	**Number of reports**	**Number of transactions**	**Declared value** (millions of euros)
Sales	33,250	89,506	13,174
Gold loan (concession)	1,330	3,118	893
Gold loan (restitution)	312	411	53
Other non-financial transactions	53	53	27
Personal imports of gold	105	155	181
Delivery services for investments in gold	486	490	129
Total	**35,536**	**93,733**	**14,457**

This year too, physical transfers of gold out of the country remained heavily concentrated among a few entities, with a further increase in the value of the declared gold (+8 per cent).

Types of declaring entities

Despite the increase in the number of entities registered in the system, the group of those actually active shrank further, from 443 in 2017 to 419 in 2018 (Table 6.4). Most of the new registrations involved professional operators and natural persons. The assistance provided by the UIF to reporting entities remained constant at around 600 requests. Investment gold was the type of gold most traded in 2018 as well, at 51 per cent, followed by industrial gold at 41 per cent; in the remaining 8 per cent of cases, it was not possible to identify a unique purpose for the exchange. Professional gold operators continue to be the main category of registrants, with a share of 75 per cent of the total value exchanged; banks account for 24 per cent, while the private share remains low at 1 per cent.

Counterparties

With reference to the geographical distribution of Italian counterparties, the marked concentration in the traditional gold working areas continued: apart from Vicenza and Alessandria, the growth of a macro district in Tuscany appears to have consolidated including, together with the province of Arezzo (which alone represents almost half the market), those of Florence and Siena. Just under one third (€4 billion) of the amounts declared continue to refer to foreign counterparties; the high concentration in a few countries persists: more than 70 per cent of the amounts refer to just five countries (Figure 6.4).

Table 6.4

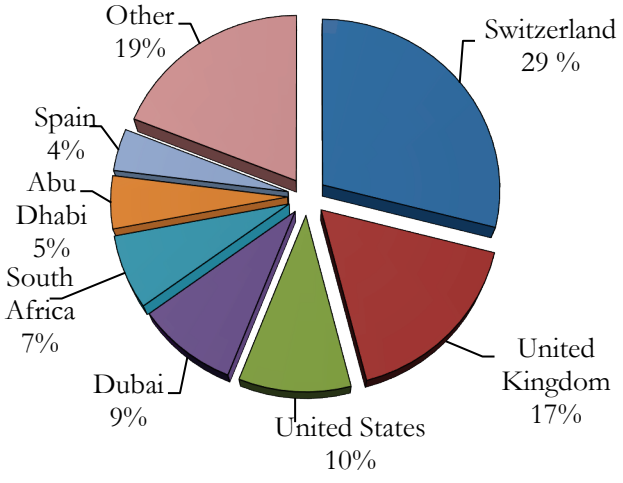
Categories of reporting entities engaged in total gold transactions

TYPE OF REPORTING ENTITY	**Number of reporting entities registered**	**Number of reporting entities active in the year**	**Number of declarations**
Banks	78	39	5,632
Professional gold dealers	423	341	30,474
Private natural persons	107	14	19
Private legal persons	81	25	262
Total	**689**	**419**	**36,387**

The weights of the largest foreign countries have changed significantly: specifically, Dubai's share has fallen from 15 to 9 per cent, while Switzerland's share has risen from 26 to 29 per cent. The top five countries included South Africa this year, which had a share of 7 per cent; only a few entities had transactions with this country.

Figure 6.4

Gold transactions with foreign counterparties



Advance declaration statistics for the gold trade

Over the year, the total value of physical transfers of gold abroad increased markedly (+19 per cent; Table 6.5), in contrast to a significant fall in the number of transactions (-12 per cent).

Analysis of the GOLD database

As well as providing useful information for the analysis of STRs (see the section 'Financial anomalies in the gold sector' in Chapter 3), cross-checking the data contained in gold

declarations with other databases and analysing some operational practices led to the identification of anomalous conduct and operations and to the creation of risk indicators. The resulting evidence was forwarded to the investigating bodies.

Discrepancies were found between the volume of activity of professional operators based on statements made in their gold declarations and that recorded in the balance sheet data, which could be symptomatic of tax evasion.

Table 6.5

Advance declarations of transfers of gold abroad (1)

TYPE OF TRANSACTION	**Number of declarations/ transactions**	**Declared value** (millions of euros)
Sales	831	818
No operation (mere transfer)	18	3
Other non-financial transactions	2	0.4
Total	**851**	**821**

(1) The advance declarations are included in the monthly declarations when they relate to commercial or financial transactions.

There are also companies that systematically carry out gold transactions without making the required declaration and without being registered in the Bank of Italy's special register, which could give rise to cases of abusive exercise of the activity that would then be investigated. The differences between advance declarations and monthly ones are symptomatic of an anomalous transfer to and from abroad, considering that some of the countries receiving transfers with the most significant differences are also opaque financial centres. Some additional indicators of anomalous operations in gold have also been defined, for example with reference to: (1) 'mirror' operations that two operators carry out in the same month at prices that are very different from market prices; and (2) the extremely high concentration among a few operators of purchases from private counterparties registered in specific provinces. In several cases, the identified anomalies are reflected in the STRs analysed by the Unit. Finally, the analysis of recent judicial cases involving major players has resulted in the drawing up of some anomalous behaviour patterns for the detection of shell companies and illegal networks operating in the market.

7. COOPERATION WITH OTHER AUTHORITIES

7.1. Cooperation with the judicial authorities

International and European principles and rules pursue the broadest possible cooperation between the 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 of information exchanges. By means of ever more efficient and advanced forms of interaction and channels for exchanging information, national legislation capitalizes on fruitful opportunities for coordinating prevention and enforcement action, giving rise to various forms of cooperation between the UIF, the investigative bodies and the judiciary, in compliance with the limits and the distinction of roles provided for by law.

While the UIF fulfils its reporting obligations pursuant to Article 331 of the Code of Criminal Procedure and concerning offences detected in the performance of its duties, at the request of investigating magistrates, it also provides information obtained in the course of its in-depth analyses and inspections 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 their turn, the judiciary and the investigative bodies forward information to the UIF. The National Anti-Mafia and Anti-Terrorism Directorate (DNA) regularly provides feedback to the UIF on the usefulness of the information received.

These information exchanges help the Unit to carry out its functions more effectively by expanding its knowledge of criminal typologies and practices and by making a greater contribution to preventing and combating crime.

The data for 2018 show that cooperation with the judicial authorities and the investigative bodies is increasing. Some 265 requests were received from the judicial authority, to which the UIF sent 488 responses, (including follow-ups to the first exchange, with subsequent STRs and information received from foreign counterparties concerning subjects of interest to the judicial authorities (Table 7.1).

Requests from the judicial authorities to the Unit are generally made to obtain information gathered by the UIF in its analysis of STRs and as part of international cooperation, or to make requests to foreign FIUs. The purpose of specific requests is to obtain financial analyses that help with ongoing investigations.

Table 7.1

Cooperation with the judicial authorities

	2014	2015	2016	2017	2018
Information requests from the judicial authorities	265	259	241	226	265
Responses	393	432	473	429	488

The UIF cooperated on investigations into organized crime, drug trafficking, corruption, unauthorized financial activities, fraud and money laundering. There were also several requests for cooperation in combating financial cybercrime (mainly involving cases of unauthorized financial activities on IT platforms and of cyber fraud) and illegal online gambling.

The judicial authorities are increasingly being assisted by the UIF in carrying out investigations concerning criminal activities of a cross-border nature, with a view to acquiring useful information in a timely manner for investigation purposes. Transmission of information from foreign counterparts to the judicial authorities takes place with the prior consent of the counterparts concerned and with the adoption of special precautions to safeguard confidentiality and to limit the use of this information.

Information exchanges with foreign counterparts made it possible to identify the account holders used to convey the proceeds of criminal activities, to have a clearer idea of the persons connected to ongoing investigations, and to facilitate the adoption of preventive seizures of funds, including of large amounts, which can be traced to members of organized crime groups.

The requests for activation on behalf of the judicial authorities mainly involved the FIUs of the United Kingdom, Denmark, Malta, the Czech Republic, Slovakia, Slovenia and Romania. There are also many information exchanges with the FIUs of Switzerland and Luxembourg. From an operational point of view, the Finance Police's use of the SAFE Portal (see the UIF's *Annual Report for 2017*, p. 98) as part of the investigations delegated by the judicial authorities contributed to increasing the cooperation provided by the Unit, especially at international level, as it made information exchanges more fluid and rapid.

In 2018, the effects of the decriminalization of some of the offences included in the anti-money laundering legislation established by law in 2016 continued to be felt,[23] with a steady reduction in the number of reports under Article 331 of the Civil Code. The number of informative reports made for investigative purposes also decreased (Table 7.2).

Table 7.2

Reports to the judicial authorities

	2014	2015	2016	2017	2018
Reports per Article 331 of the Civil Code	85	233	157	115	87
of which: submitted to judicial authorities	7	5	2	3	-
made in connection with technical reports sent to investigative bodies	78	228	155	112	87
Informative reports for investigative purposes	23	17	16	26	16

The UIF made its expertise and technical competence available to the Public Prosecutors' Offices in 2018 as well, in accordance with the respective roles established by the legal system. On 5 April and 25 July 2018, memorandums of understanding were signed with the Public Prosecutors' Offices of Naples and Florence.

In implementing the envisaged legislation, the agreements regulate the exchange of information of mutual interest and provide for the identification of areas for joint analysis of facts and information. The memorandums regulate the use of documentation and indicate

[23] Law 8/2016.

the need for reciprocal training programmes.

Cooperation with the National Anti-Mafia and Anti-Terrorism Directorate (DNA)

The reform introduced by Legislative Decree 90/2017 emphasized the role of the DNA in the anti-money laundering prevention system, introducing among other things new forms of cooperation with the UIF (Article 8 of Legislative Decree 231/2007). The new provisions incorporate and enrich the fruitful relationships established over the years between the Unit, the DNA and the Anti-Mafia District Directorate (DDA).

On 7 May 2018, the technical and operational protocol for implementing these forms of cooperation was drawn up with the DNA. The protocol follows up on the one signed on 5 October 2017 between the UIF, the DNA and the investigative authorities for the implementation of the reform. (See the *Annual Report for 2017*, pp. 15-16) and sets out precisely how to exchange data and information in order to ensure a more immediate use by the DNA of the elements in STRs and better guidelines for the Unit's financial analysis (see the section 'The methodology' in Chapter 2).

Based on the protocols, the Unit communicates the personal data of the persons reported and of the persons connected to them to the DNA, ensuring that they are processed anonymously and in order to verify their connections with ongoing criminal proceedings; the DNA may request additional information and analyses from the UIF in cases of interest. In turn, the UIF receives feedback on the importance of the information provided. The National Anti-Mafia and Anti-Terrorism Directorate's feedback concerns the presence of the persons reported in its databases and contains a risk rating based on the level of involvement of the subjects in investigative activities.

The first months' experience of applying the protocols showed that the information exchanged for the stimulus and coordination activity assigned to the DNA was extremely useful. For the UIF, the information obtained constitutes a valuable additional element for analyses and contributes to better defining the priorities and refining the methodologies.

Exchanges are carried out using cryptographic techniques that ensure data confidentiality, in line with the provisions of the legislation (see the sections 'The methodology' and 'IT resources' in Chapters 2 and 10 respectively). The automation of the information exchange process with the DNA is under way as well as the gradual integration within the RADAR system of information flows returned to the UIF.

The UIF continued to take part in the panel of technical experts set up at the National Anti-Mafia Directorate that also includes the Customs and Monopolies Agency by means of a constant exchange of information.

In 2018, the SAFE portal was further enhanced; the new IT system makes it possible to manage the information exchanges with the judicial authorities in a completely automatic way. The UIF launched specific training initiatives at many Prosecutors' Offices to explain the functionalities of this IT system and to communicate the relative operational instructions. SAFE

To this end, specific training meetings were organized with the Prosecutor's Offices in Brescia, Naples and Ancona: contacts were established with other Prosecutor's Offices to set up similar initiatives.

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. In this context, the UIF participates in the work of the Financial Security Committee (FSC), set up at the Ministry of Economy and Finance to carry out analyses and coordination activities for preventing the use of the financial and economic system for the purpose of money laundering and the financing of terrorism. All the authorities involved in the prevention and law enforcement system are represented in the Committee, which serves as a focal point for developing strategies and is responsible for implementing international sanctions.

The UIF takes part in the work of the experts that is used 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 based on European regulations and helps to consolidate the interpretative guidelines and draw up operational practices for sanctions.

The activity of the working group that led to the adoption of a document updating the National Risk Assessment approved by the FSC in March 2019 continued. As regards secondary legislation, the FSC expressed a favourable opinion on the UIF's *Guidelines* for threshold-based communications (see the section 'Secondary legislation and self-regulation' in Chapter 9).

7.2.1. List of designated persons and measures to freeze funds

The UIF monitors the implementation of asset freezing measures[24] as part of the financial sanctions adopted at national or EU level, which are essentially part of countering the financing of terrorism and the activities of countries that threaten international peace and security.

The UIF also collects information and financial data 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 European Union, also in accordance with some UN Security Council resolutions, further tightened the framework for financial sanctions against North Korea by issuing Regulation (EU) 2017/1509. In 2018, the European Union adopted 16 amendments to the aforementioned regulation on North Korea concerning, among other things, the extension of the lists of persons subject to the freezing of funds and the introduction of new categories of goods (including oil) for which export is prohibited, as is the relative provision of financial assistance by European financial intermediaries. The requirement to send suspicious transaction reports to the FIUs in the event of suspicion of financing for proliferation (Article 23) and a specific authorization regime for transfers of funds for amounts that exceed certain thresholds were both confirmed.

[24] Article 10(1) of Legislative Decree 109/2007.

The amount of frozen funds and financial resources remained the same as in 2017. Two accounts were closed due to the charging of costs and commissions and three new accounts were frozen (Table 7.3).

Table 7.3

Measures to freeze funds at 31/12/2018					
COUNTRIES AND ENTITIES	Accounts and transactions frozen	Persons subject to freezing	Amounts frozen		
			EUR	USD	CHF
ISIL and Al-Qaeda	32	26	39,268	114	50
Iran	17	4	1,086,120	158,453	37,593
Libya	4	3	125,334	132,357	-
Syria	28	5	18,564,736	240,825	149,872
Ukraine/Russia	2	1	93,781	-	-
DPR of Korea	3	4	8,000	-	-
Total	**86**	**43**	**19,917,239**	**531,749**	**187,516**

In this context, current accounts and financial resources traceable to four entities recently listed by the UN and the European Union were frozen. As part of its participation in the work of the FSC, the UIF contributed to carrying out the assessments under its jurisdiction regarding compliance with the relevant legislation, specifically upon request of the UN panel 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 2018, the UIF received six freezing notices against entities included in the lists of those subject to financial sanctions. In most cases, these are updates of transactions on accounts held by designated Syrian banks, which were specifically authorized by the FSC under certain conditions provided for by European Union law.

7.3. Cooperation with supervisory authorities and other institutions

The legislation promotes cooperation between the various competent authorities and institutions at national level by providing that, notwithstanding official secrecy, the Ministry, the supervisory authorities, the UIF, the Anti-Mafia Investigation Department (DIA), the Finance Police and the government agencies and entities concerned work together to identify circumstances that may point to facts and situations, knowledge of which can be used to prevent the financial and economic system from being used for money laundering or the financing of terrorism.

Exchanges with the Bank of Italy's supervisory directorates

The exchange of information between the UIF and the Bank of Italy's supervisory directorates remained constant. The supervisory department submitted information to the UIF discovered during inspection activities, concerning possible shortcomings in the field of active cooperation on the part of obliged entities. In turn, the UIF brought to the attention of

the department the anomalies found at the intermediaries with regard to organizational structure and the fulfilment of the department's obligations (with regard to sanctions procedures, see the paragraph: 'Sanctions procedures' in Chapter 5).

... with CONSOB

Collaboration continued with Consob, with the usual exchange of information flows on failures to submit STRs uncovered in the course of supervisory inspections and analyses of market abuse. In 2018, meetings aimed at further refining the general criteria for selecting the information to send were held in order to optimize the process of information exchanges.

... with IVASS

In 2018, the main purpose of information exchanges with IVASS was to check the absence of links between events relating to the governance of insurance companies and money-laundering or terrorism-financing activities.

The requests for information sent by IVASS often required the involvement of foreign supervisory authorities. In view of the particular confidentiality regime for the data held by the UIF, such requests were processed by providing the FIUs of the countries concerned with the information available for possible AML analysis purposes and giving consent to inform the local insurance supervisory authorities, in compliance with the restrictions imposed by national and international law. IVASS was notified of such cooperation with the foreign authorities concerned. The uncertainties found led the UIF to propose a specific legislative intervention as part of the initiatives under way, designed to make amendments to Legislative Decree 231/2007 and to transpose the Fifth Directive.

MED and Customs and Monopolies Agency

The results of the analysis carried out by the UIF on trust companies and gaming operators were sent to the relevant departments of the Ministry of Economic Development (MED) and the Customs and Monopolies Agency. The Agency sent several information reports to the UIF, which enabled specific investigations to be carried out on anomalous financial flows, which in some cases were found to be linked to illegal activities of investigative interest.

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 or charitable donations for significant amounts in Italy (see the *Annual Report for 2017*, p. 22).

In 2018, the Operations Manual governing the procedure for obtaining visas was updated and specific FAQs were published.[25] It was specified that, among the documents that foreigners must produce for assessing compliance with the requirements, there must be a statement from the intermediary with which the funds are deposited, in which the intermediary declares that its client is effectively compliant with the national anti-money laundering and anti-terrorism legislation, in accordance with the FATF's international standards.

Ministry of Justice

As provided for by Legislative Decree 231/2001, in 2018 the UIF continued to act as advisor to the Ministry of Justice, taking part in the review of the codes of conduct drawn up by representative associations for the purpose of preventing the commission of offences.

In this context, work continued on preparing guidelines for the associations as an ancillary tool for drawing up codes of conduct, to facilitate the subsequent approval on the part of the authorities concerned.

[25] See *Investor Visa for Italy*.

Anti-corruption coordinating Committee

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 encourage dialogue between all the institutions concerned, to define the positions to be held by each technical panel and to promote policy coordination. The Committee also encourages the gathering and sharing of issues and proposals to ensure the active participation of the delegations representing Italy in international forums.

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 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).

8. INTERNATIONAL COOPERATION

8.1. Exchange of information with foreign FIUs

Within the system of international anti-money laundering rules, the FIUs are given centralized responsibility for the tasks connected with receiving and analysing suspicious transaction reports and the related exchange of information with their foreign counterparts. The latter function is 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 ability of FIUs 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 another FIU.

In accordance with the principle of multidisciplinarity, FIUs must have 'financial, investigative and administrative' information for domestic and reciprocal analysis. 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.

Europol has hosted the FIU.NET network since 1 January 2016. Based on a Common Understanding with European FIUs, Europol must ensure full functional equivalence with the previous system and the development of more sophisticated forms of cooperation. The European FIUs continue to participate in the governance and decision-making processes relating to FIU.NET through an Advisory Group appointed by the FIU Platform and called upon to issue opinions and proposals to the competent Europol decision-making bodies.

The range of international cooperation is continually increasing: the UIF has exchanged information with all the EU FIUs and with 125 counterparties overall at global level (against 101 in 2017 and 87 in 2016). The types of suspicious transactions dealt with in their exchanges mainly concern the most common criminal phenomena in Italy: organized crime, corruption and tax offences. As part of the analysis of STRs, the UIF sends requests for information to foreign FIUs if there are objective or subjective links to other countries. Requests are generally aimed at reconstructing the origin or use of funds transferred from or to other jurisdictions, identifying movable or immovable assets abroad, and detecting ongoing inquiries or investigations in other jurisdictions or the beneficial ownership of companies or entities in other countries.

Moreover, the exchange of information enables the UIF to provide the investigative bodies and the judicial authority with additional information to support their criminal investigations and proceedings. (See the Section 'Cooperation with the judicial authorities' in Chapter 7).

Requests sent to foreign FIUs

In 2018, the UIF sent 1,082 requests for information to foreign FIUs, 41.8 per cent more than in 2017. This confirms the trend in recent years of a growing reliance on international cooperation, in line with the FATF recommendations that followed the 2015 Mutual Evaluation of Italy (Table 8.1). The increase relates both to requests sent for the analysis of suspicious transactions with foreign links (+21 per cent), and to requests made on behalf of the judicial authorities (+113.4 per cent).

Table 8.1

Requests sent to FIUs in other countries

	2014	2015	2016	2017	2018
Information required by the judicial authority	146	217	204	172	367
Information required for internal analysis	242	323	340	591	715
Total	**388**	**540**	**544**	**763**	**1,082**

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 do not emerge from the analysis of a case.

Requests received from foreign FIUs

The UIF received 2,228 requests and spontaneous communications from other FIUs (Table 8.2). The slight decrease compared with 2017 does not alter the trend towards steady growth in information exchanges in recent years.

Table 8.2

Requests/spontaneous communications received and responses provided

	2014	2015	2016	2017	2018
Egmont network	486	1,078	1,259	668	594
Requests/spontaneous communications	*486*	*695*	*723*	*504*	*577*
Exchanges on ISIL		*383*	*536*	*164*	*17*
FIU.NET	453	1,075	2,055	1,578	1,634
Requests/spontaneous communications	*453*	*518*	*580*	*524*	*602*
Cross-border reports		*557*	*1,475*	*1,054*	*1,032*
Total	**939**	**2,153**	**3,314**	**2,246**	**2,228**
Responses provided (1)	**1,144**	**1,223**	**1,568**	**1,232**	**1,681**
Communications to investigative bodies	**713**	**868**	**1,430**	**2,031**	**3,070**

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

The highest volumes recorded mainly in 2016 were due to the start of suspicious cross-border transaction reports, the numbers of which became more moderate in the following years, pending the definition of appropriate uniform criteria. On the other hand, requests and spontaneous communications, both through the Egmont network and the FIU.NET, are increasing.

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 counterparties that are not members of the Organization.

At European level, the automatic exchanges of cross-border reports that, under the Fourth ML/CFT Directive, 'concern another Member State' and are forwarded to the FIU of that Member State, are an important source of information.

In 2018, 1,032 reports of this kind were received. They contained several communications, amounting to 6,718 altogether. The reports received are assessed, analysed and disseminated according to their priority level. They are also used for cross-checks in the analysis of suspicious transactions reported to the UIF.

The cooperation for analysing international money laundering schemes or the possible financing of terrorism is particularly frequent and fruitful. The most common types of suspicious activities brought to the attention of foreign counterparties relate to the use of cash, the transfer of funds by persons involved in investigations in Italy, and the use of trusts and foreign trust companies to disguise beneficial ownership or for tax evasion purposes. Transactions linked to cyber frauds and unlawful access to IT systems for the misappropriation and transfer of funds are also increasing substantially. The purpose of cooperation in such cases is to intercept and halt the fraudulent transfers as soon as possible in order to make their recovery possible.

Exchanges with FIUs in Eastern Europe have brought to light a widespread and large-scale tax fraud scheme, which is also linked to Italian organized crime. It is characterized by the opening of foreign accounts, often held by companies, to which large sums of money are transferred, also in cash; these sums are then withdrawn or transferred onwards with no particular economic rationale and in a way that hampers traceability. Another important line of in-depth analysis launched on a multilateral basis examines the widespread occurrence of trade-based money laundering, which involves various jurisdictions and movements of significant sums, over- and under-invoicing and the participation of several companies from the electronic goods sector, used for laundering the proceeds of drug trafficking.

The UIF provides cooperation to foreign counterparts in accordance with European rules and international standards. Specifically, data relating to STRs, relevant information from external archives or from obliged entities, and investigative elements from the competent authorities are sent to the FIUs. The UIF provided 1,681 responses to foreign FIUs in response to requests or information received (+ 36 per cent compared with the previous year). This includes both responses to requests for cooperation and feedback on the use of information received in spontaneous communications. In many cases, feedback is also given on the quality and usefulness of the assistance received.

In 2018, there were a significant number of exchanges with foreign FIUs on the suspension of transactions or on freezing funds in Italy or abroad (a total of 66 cases).

Cooperation for the suspension of transactions

Cooperation between the UIF and its foreign counterparts makes it possible to suspend transactions, thereby preventing the diverting of funds of illicit origin, pending the application of the necessary seizure or confiscation procedures.

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, upon request by foreign FIUs to suspend transactions or accounts in Italy where suspicious activities are detected or for precautionary purposes.

In 44 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 many cases were under investigation. The UIF was asked to provide feedback on Italy's interest in continuing to freeze assets for the possible application of precautionary measures through cooperation with investigative bodies. In these cases, the UIF informed the Italian investigative bodies in a timely manner, making it possible to identify, block and seize the assets of subjects under investigation that had not emerged during domestic investigations.

Further interventions involved freezing assets in Italy at the request of FIUs in other countries. Some 22 requests of this kind arrived in 2018, mainly relating to fraud, often cyber fraud, identity theft, and the transfer of the related proceeds to Italy for immediate cash withdrawals or further transfers. In these cases too, it was often possible to take prompt action to avoid funds being dispersed, allowing the foreign authorities concerned to assess and initiate the necessary seizure request procedures. Of particular importance was the cooperation of the Italian intermediaries involved, which often applied constraints on the accounts to which illicit proceeds were transferred.

Exchange of information with investigative bodies

Article 13(1) of Legislative Decree 231/2007 provides that the UIF can also use the investigative information obtained specifically by the Special Foreign Exchange Unit of the Finance Police and by the Anti-Mafia Investigation Department in its information exchanges with foreign counterparties, derogating from data confidentiality, 'without prejudice to the provisions on the secrecy of investigations.

The explicit reference to respect for the confidentiality of investigations, though not entailing any important changes compared with the previous system, has made necessary, according to the interpretation of the investigative bodies, a close review of the system and of the procedures for providing the UIF with investigative data. This has resulted in a delay in applying the law that risks undermining and limiting how international information exchanges operate.

The UIF sends information from foreign sources to the investigative bodies on its own initiative, after obtaining the necessary consent of the FIUs concerned. The figure (3,070 communications) increased compared with the previous year; this reflects both changes in the way information is collected and the widening of this form of dissemination. Dissemination is addressed not only to the Special Foreign Exchange Unit of the Finance Police and the Anti-Mafia Investigation Department, but also to other investigative bodies dealing with particular crimes, in compliance with specific confidentiality safeguards and with the conditions of use posed by foreign counterparts.

In 2018, the UIF adapted its working processes for exchanging information with the investigative bodies to which the identifying data of the persons named in foreign FIU's communications are sent, in order to allow timely feedback and to obtain the investigative information required for international collaboration. In addition, the underlying information is then made available, with the prior consent of the FIUs concerned, taking account of the relevance of the cases and the links with Italy.

This dissemination of information is based on selective criteria of an objective and subjective nature, referring to elements such as the probability of committing a crime, organized crime activities, tax crimes, the presence of foreign assets, cross-checks with suspicious transaction reports, and references to ongoing investigations or to politically exposed persons. This information is also shared with the investigative bodies for the cases reported by the Special Foreign Exchange Unit of the Finance Police and the Anti-Mafia Investigation Department as being of specific interest.

An essential component of the new work process is the use of the SAFE portal to send communications securely and in real time. An important advantage of the new communication system is the possibility to export in a structured way the names of persons in the requests sent by the UIF, pursuant to Article 13 of Legislative Decree 231/2007, so that the investigative bodies can then feed this information into the SIVA system.

Cross-border reports

Work continued in 2018 on implementing the automatic exchanges of cross-border STRs between the FIUs of the European Union, under Article 53 of the Fourth Directive. As part of a project in which the UIF participates, the EU FIUs Platform approved an initial set of criteria of a subjective and objective nature, aimed at focusing exchanges on cases of real interest, thus avoiding excessive flows.

The most important reports in automatic exchanges are those sent by entities working under the freedom to provide services. Moreover, the subjective criteria refer, for example, to the place of residence of individuals or entities involved or to the existence of investigations in other countries. Objective elements relate to the origin or destination abroad of financial flows or to accounts or financial activities held abroad. Reference is also made to links with illegal activities carried out in another country and to the importance of the case for other countries, based on elements derived from specialized databases or from discretionary assessments.

Taking into consideration the wide range of reports falling under these criteria, a further selection based on FIU.NET matching is planned for the extraction of significant cross-checks between countries.

The sending of cross-border reports is still intermittent and extremely varied. Only a few FIUs have adopted a systematic exchange of cross-border reports; some continue to make use of manual procedures and only partially apply the agreed criteria.

The commitment to European works continues, refining the criteria for increasing the quality of information through an appropriate selection process and limiting the impact on FIUs' resources.

8.2. Cooperation between FIUs

The quality of cooperation between FIUs has improved. The requests and information received from some counterparties, especially European ones, are more focused on the description of the case and the elements of suspicion. There seems to be a greater ability to exchange financial information, often obtained from obliged entities, in order to process the information requests. These improvements stem from legislative reforms made in European countries for transposing the Fourth AML Directive and from the subsequent initiatives taken at national and European level to increase the capacity of FIUs to access information for their own analysis and for working with foreign counterparts.

However, the effectiveness of the information exchanges continues to be hampered by the differences in the institutional nature and organization of each FIU, which affects their independence and powers. Informative capabilities are not uniform, there are still constraints on the use of information for subsequent investigations, and the dividing line between financial analysis and investigations is not always clear-cut.

Further progress is needed to expand the FIUs' ability to access information, especially of a financial and corporate nature, to share it for analysis and to allow it to be used for subsequent investigations when necessary. A boost for greater operational integration and a progressive development of common practices and approaches could come from the consolidation of joint analysis methodologies for cross-border related phenomena. The European Commission, in compliance with Article 65 of the Fourth Directive, began an analysis of the cooperation between the FIUs in the European Union and at global level, in order to identify any obstacles as well as opportunities to further strengthen it, so as to establish a support and coordination mechanism (see the *Annual Report for 2017*, p. 10).

The nature of European FIUs. Administrative and investigative models

EU anti-money laundering rules set out the minimum requirements and provisions focusing on general aspects, which leaves it to national lawmakers to define the respective regulatory scopes. Within a framework of flexible rules, European FIUs display significant institutional and organizational differences. This variety directly affects the characteristics of the activities carried out, the information available, and the ability to cooperate.

In the European Union, the largest group of FIUs are administrative ones: there are 13 of them, while a further 10 are of a law enforcement or judicial nature and 5 have mixed characteristics.

In order to meet the requirements of autonomy and independence, the administrative FIUs are usually established inside public institutions, supervisory authorities or central banks, as is the case in Italy. Law enforcement FIUs are part of their countries' national police administration and have different levels of hierarchical dependence and organization: some units are separate and have their own governance systems, others are offices set up within departments or structures for combating economic or other serious crimes. Because of the presence of administrative and law enforcement elements, FIUs of a mixed nature are set up within administrative authorities, police agencies or judicial bodies; they specialize in analysing suspicious transactions and are kept separate from the other sectors of the organizations to which they belong.

The administrative model allows for greater compliance with the typical role of the FIUs, which is to carry out financial analyses, separate from investigative activities, and to

dialogue with the private sector, in particular with banking and financial intermediaries.

The advantages of the administrative model lie both in the effectiveness of actions and cooperation and in the requirements of autonomy and independence. The administrative FIUs are placed between the reporting entities and the investigative bodies, facilitating dialogue based on common technical and financial expertise. In addition, administrative FIUs develop independent methods of financial analysis, specialized and distinct from investigative activities and thus capable of providing investigative bodies with added value for the reconstruction and interpretation of complex economic phenomena.

The empirical evidence at the heart of the Mapping Exercise on the characteristics, powers and cooperation of the European FIUs, conducted by the EU FIUs Platform under the aegis of the Commission, together with the results of the FATF's evaluations, show that the necessary distinction between analyses and investigations tends to become blurred in law enforcement FIUs, with the two tasks overlapping into a single activity (see the *UIF's Annual Report for 2016*, p. 107). Access to financial information is often considered as part of an investigation and requires the relevant powers to be activated, generally subject to authorization from third parties (for example, the competent public prosecutor).

8.3. Developments in the FIU.NET

The debate on the functioning and use of the FIU.NET system in Europol's IT infrastructure has continued both on the EU FIU.NET Platform and in the FIU.NET's Advisory Group. The 2017 Roadmap for the integration of FIU.NET into Europol's IT systems was the subject of a comprehensive review by a working group, in which the UIF participated. Among other things, a number of guiding principles have been drawn up on which the new platform for cooperation between European FIUs should be based.

The FIU.NET system is intended to provide support for the cooperation and exchange of information between European FIUs, with Europol acting as the service provider. The system is therefore geared to fostering FIU-to-FIU cooperation, and the FIUs are the exclusive owners of the exchanged data; it does not include any cross-checks or mixing with the data in Europol's databases. The Working Group's analyses also focus on the data protection issues arising from the centralized configuration of the system. An opinion was requested from the European Data Protection Supervisor on the compatibility of the centralized solution with the necessary data protection safeguards for information exchanged between FIUs.

8.4. The EU FIUs Platform

The Platform, which has been active since 2006 and was formally recognized by the Fourth Directive, has confirmed its role in coordinating the European FIUs for the implementation of European Union rules through the development of common practices and forms 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 the use of innovative forms of automatic exchange and joint analysis. The implementation 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. A comprehensive work plan, divided into five thematic areas, is being implemented through multiple operational projects.

The conclusions on how to use the information exchanged have been updated, specifying the information and investigation purposes that can be pursued by means of dissemination. The project to establish the application criteria for the correct functioning of automatic exchanges between the European FIUs of STRs with elements of common interest is still ongoing (see the section 'Exchange of information with foreign FIUs').

The FIUs identify and analyse threats and vulnerabilities of common importance on the Platform in depth, comparing the types of behaviour that emerge from the transactions and contributing to the draft of the Supranational Risk Assessment (see the section 'Further European and international initiatives', in Chapter 9). The Platform is also where the FIUs draw up analyses and proposals on the European policies that concern them. In recent months, there has been work on the numerous legislative measures under discussion (see the section 'The evolution of European legislation' in Chapter 9), in particular the Proposal for a directive on the sharing and use of financial information, and on further analysis for the design of a European coordination and support mechanism. The UIF has promoted the development of common analyses and positions in support of the European Commission and of European and national policymakers.

The discussion on the evolution of FIU.NET and on the use of the network for exchanging information has also continued on the Platform. The focus was on the difficulty in ensuring the necessary levels of functionality and effectiveness, the development of the Roadmap for the creation of a more robust system, the lack of involvement of FIUs in the network governance, and the data protection regime.

From an operational point of view, innovative activities for cooperation between FIUs are promoted by the Platform through joint analyses of cases of cross-border importance.

Joint Analyses - Projects coordinated by the UIF

While the traditional means of cooperation are based on the request for and transmission of information for the analysis of cases focused on by the individual FIUs concerned, in joint analyses, both the necessary information and the very process of analysing the suspicious activities that the FIUs have in common are shared.

This is necessary for dealing with cases that have links with many different countries and which cannot be dealt with effectively by analysis at national level. The sharing of the information available or that can be acquired at national level goes together with the analysis of such information by international teams of analysts designated by the FIUs concerned. In this way, it is possible to share the entire analysis process, thereby gradually enriching the joint database, to compare the characteristics of the case and to reach shared conclusions that take account of the transactions in different countries and the different methods, tools and sensitivity of the analysis. The UIF launched and coordinated two of the three joint analysis exercises, completed in 2018.

The UIF, together with the FIUs of the Netherlands (in the role of co-lead), Belgium, France and Spain conducted in-depth analyses on activities linked to terrorist financing,

carried out through complex and stratified transactions for international money remittances.

A second exercise (carried out with the FIUs of Bulgaria, Croatia, Germany and the Czech Republic) focused on the possibility of developing an analytical methodology with which European FIUs can converge, while maintaining their specificities also to enable effective cooperation and joint analysis.

The exercise was conducted following a bottom-up approach: the team started with a joint analysis of a complex intra-EU VAT fraud scheme ('carousel fraud'); the information tools and methodologies applied by the FIUs involved in the analysis were isolated and clarified. It was therefore possible to set out the reconstruction of the phenomenon examined (for every further follow-up via national dissemination) in the final report and to establish a common initial methodology for carrying out analyses.

By testing innovative methods and instruments, the multinational teams of analysts worked closely through video and audio-conferences, and face-to-face meetings took place in Italy at the UIF. The experience gained in the joint analysis exercises has shown that there are possibilities for developing this new form of cooperation. The outcomes of the exercises were gathered in a report, endorsed by the Platform, and useful for the progress of the European FIUs' system towards the creation of a common mechanism to facilitate joint cooperation and analysis.

8.5. Relations with foreign counterparties and technical assistance

International cooperation activities at operational level are part of wider relationships with foreign counterparts; in this context, the UIF shares experiences, develops activities of common interest and participates in technical assistance interventions. In 2018, the most frequent contacts were with the geographically closest FIUs (San Marino, the Holy See and Switzerland), to deal with cases of mutual interest and to compare risk factors, regulatory innovations and organizational changes.

For the analysis of the large-scale trade-based money laundering that is based in Italy but is also found in many other countries, the UIF organized a multilateral round table. The evidence from the information exchanges was assessed with the competent FIUs and investigative bodies of the United States and Spain, and financial analysis and investigation activities were developed at the same time.

The UIF also continued in its commitment to international technical assistance in its areas of competence, mainly addressed to its counterparts, through bilateral initiatives and participation in multilateral projects.

The requests for interventions or contributions continued, in part thanks to the positive assessments in Italy's Mutual Evaluation on the UIF's operational practices and the results achieved.

In 2018, the Unit organized a study visit for Albania's FIU to illustrate the tools and methodologies developed to support the activities of receiving, analysing and international cooperation. There was a particular focus on the experience as regards the financing of terrorism and crypto-assets.

The question of STRs relating to virtual currencies was also the subject of a meeting in the Unit with representatives from South Korea's FIU. In the meeting, the Unit also explained the features of the tools and working processes for managing and further analysing large amounts of information of a heterogeneous nature.

The UIF hosted a delegation from Bulgaria's FIU at a workshop focusing on the tools and work processes for receiving and analysing STRs, and on the relative analysis, dissemination and cooperation activities. The visit took place as part of a project funded by the European Union, aimed at strengthening analytical and cooperation capacities in the context of the new European regulations.

As in the past, the UIF's representatives participated as speakers in training courses for police officers and officials from the Caribbean Community countries (CARICOM) organized by the Scuola di Polizia Tributaria of the Finance Police. There were also training activities dedicated to police officers from other European countries at this school with the support of the Unit, which form part of the projects planned by the European Union Agency for Law Enforcement Training (CEPOL).

A large number of FIUs in countries currently undergoing a review of their institutional anti-money laundering systems — also in connection with the transposition of the new European rules — requested help from the UIF to further examine the regulatory aspects, characteristics, organization and activities of the Italian AML system.

The UIF also continues to contribute to the technical assistance carried out by the Egmont Group's working groups (especially the Training and Technical Assistance Working Group). These initiatives are generally for FIUs in the process of being set up or that need training and capacity building programmes to develop their analytical, operational procedures and IT tools, as well as international cooperation activities. These initiatives, carried out by the Egmont Group in sensitive geographic areas, support the establishment of new FIUs and their membership of the organization.

8.6. Participation in the FATF

Given the importance of international cooperation for combating money laundering and terrorism effectively, several governmental and technical bodies have been set up over time, whose scope varies 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 to the need to adapt and harmonize prevention and law enforcement measures.

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

In 2018, the UIF continued to participate in the work of the FATF within the Italian delegation coordinated by the MEF. 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.

This contribution covered all the various stages of the procedure: identifying the risks posed by each country involved and the quality of the collaboration with the local authorities, the analysis when drawing up the reports and participation in the discussion for their approval.

The UIF also continued to involve its own experts in the processes for evaluating individual countries' AML systems, with a view to facilitating the correct implementation of the standards and the effectiveness of the relevant measures.

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

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 of the countries concerned. As well as contributing to the current in-depth analyses of the risks linked to technological innovation and to the possible specific measures for compliance in relation to operators and innovative instruments (such as FinTech/RegTech), the UIF took a direct part in the recognition and analysis of the crypto-asset sector and in drawing up AML standards that take account of its particular risks.

Virtual asset standards

In line with the recommendations drafted by the G20 countries, the FATF extended the provision of safeguards to virtual asset operators and transactions. The approach adopted is based on the amendment to Recommendation 15 and contains the following main elements.

Definition of a virtual asset. This refers to assets that can be transferred as well as to exchanges between different entities: 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes'.

Definition of a virtual-asset service provider (VASP). This concept centres on the reference to specific activities and determines the scope for applying anti-money laundering measures. This means operators engaged in the following activities can be identified: conversion of asset and fiat currencies to virtual currency; conversion between different types of virtual asset; transfer of virtual assets between different accounts or addresses (not necessarily between different entities); the safekeeping or administration of virtual assets or their credentials; and carrying out activities relating to the issue or placement virtual assets (Initial Coin Offerings).

Determination of obligations and of the related control regime. With regard to the former, they include all ordinary due diligence processes, data storage and the reporting of suspicious transactions. With regard to controls, countries can choose between a system of authorization and supervision, based on subjective and capital requirements and in-depth checks, and a system of registration and monitoring based on simplified requirements and controls. In any case, there is still a need to ensure compliance with anti-money laundering obligations (the FATF does not intervene in sectoral controls, for reasons of stability, transparency or correctness, the nature and intensity of which are left to the competent international bodies and national authorities).

The solutions identified are conditioned by the need to detect trade-offs between national positions that are often divergent and also extremely vague. The content of the

applicable rules and of certain application details, which are essential for adapting the traditional institutions to the innovative activities and methods in question, is set out in a separate Interpretative Note in Recommendation 15.

The intangible nature of the activity makes it particularly difficult to identify suitable criteria for determining which country must regulate and control VASPs. The traditional territorial criterion applied until now in international standards and European rules, which use the physical location to identify the standards and competent authorities, has been adapted and completed. The FATF has accepted an approach based on the importance of both the 'institution' or the place of business and the place where the activity is provided: VASPs should be obliged entities in the country where they are established or otherwise based; in addition, countries where VASPs operate (without being physically present) may extend their anti-money laundering regime to such entities. This approach seems destined to raise application issues for the controls, enforcement, reporting and analysis of suspicious transactions. Further details will be set out in dedicated guidelines, which will take into account the initial practical experience and dialogue with the private sector.

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 the section 'Interventions by international bodies' in Chapter 4).

FATF's Forum of FIU heads

For the FIUs, the FATF's Forum of FIU heads is an opportunity to further explore and make useful suggestions for policy and standard-setting activities. However, the Forum does not have a stable role in the FATF's organization and it carries out its work based on the renewal decided each time by the rotating Presidency, which proposes the priorities to be pursued. The conclusions reached and the documents produced are taken into account in the FATF's work and inform the initiatives involving the FIUs.

The Forum recently drew up two documents on partnership models between the public and private sectors in order to facilitate active cooperation and the procedures for detecting and reporting suspicious transactions. The US Presidency has promoted new projects on themes identified as priorities.

The project on 'Countering Proliferation Finance. FIUs' Roles' is designed to recognize national experiences in detecting risks of financing of proliferation, in identifying and reporting suspicious transactions, and in applying adequate countermeasures via financial sanctions and targeted investigations.

Further consideration is given to the existence of significant differences between national approaches and to the role played by FIUs, in a framework of standards focusing mainly on the application of freezing measures. The aim is to contribute to broadening the standards on countering proliferation, for example by introducing specific criminal offences and obligations for reporting suspicious transactions.

The project launched by the Forum on 'Enhancing FIU Strategic Analysis' aims to further analyse the main characteristics of this function (which differs significantly from FIU to FIU in its methods, information sources and output), to identify the effectiveness factors and the main difficulties, and to further examine the tools available to support the FIUs.

The goal is to make available to the FIUs a series of practices and guidelines that can help converge towards shared methods and objectives and increase the effectiveness of strategic analysis. The UIF contributes actively to the project and provides expertise developed through recent studies, based in particular on quantitative analysis methodologies.

A third project is dedicated to the role of the intermediaries and the FIUs in reporting and mainly aims to further examine the existing limits to the anti-money laundering arrangements in place for monitoring and detecting criminal activities in crypto-assets.

8.7. Participation in other international organizations

The UIF contributes to the activities of the Egmont Group by promoting the policies and the lines of action in relation to the activities of the FIUs. Of particular relevance in the Group's activities are the support and compliance procedures launched when insufficient ratings are assigned in the Mutual Evaluation on issues relating to FIUs' activities and competences. The Egmont Group's verifications 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 remove the limits on the capacity of FIUs to cooperate, for example through the acquisition of additional information from obliged entities. In 2018, the Egmont Group concluded the preliminary analysis of reports on the FIUs in ten countries. The UIF actively contributed, in particular by finalizing the reviews for the FIUs of Switzerland and Austria.

The Support and Compliance procedure, currently limited to technical compliance, will be extended to review the effectiveness of the activities of the FIUs, with particular regard to analytical work (Immediate Outcome 6 of the FATF methodology) and international cooperation (Immediate Outcome 2). The Egmont Group's work on adjusting procedures is intended to avoid duplication with FATF assessments and to identify the most important aspects for the work of the FIUs.

The work of the Egmont Group continued with the identification and analysis of the typologies of money laundering and financing of terrorism. Work on the ISIL Project also continued, focusing on the project dedicated to 'Lone Actors and Small Cells' (see the section 'Interventions by international bodies' in Chapter 4).

Further ongoing projects deal with the laundering of proceeds from corruption and the development of effective forms of cooperation between FIUs and customs authorities.

The UIF was awarded the 'Best Egmont Case Award of Excellence' as part of the World Bank's 'STAR — Stolen Asset Recovery' initiative. The winning case, which operated through analysis and information exchanges with other FIUs, concerns the misappropriation of public funds submitted to insolvency proceedings.[26]

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 the Republic of Malta. In addition, one of the UIF's scientific experts 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.

[26] *Casistiche di riciclaggio e di finanziamento del terrorismo*, Quaderni dell'antiriciclaggio, No. 11, 2018.

9. THE LEGISLATIVE FRAMEWORK

9.1. The international and European context

9.1.1. The evolution of European legislation

The Fifth Directive

The Fifth Anti-Money Laundering Directive[27] was published on 19 June 2018. It provides the EU regulatory framework with targeted amendments on specific subjects and requires measures to update the national legislations shortly after the transposition of the Fourth AML Directive,[28] which has not yet been completed in some countries.

In detail, the Fifth Directive extends the range of obliged entities to include virtual currency providers; includes more detailed rules on due diligence, especially given the risks linked to the use of prepaid payment cards and to counterparties in 'high risk' countries (identified on a specific European list); extends the transparency measures for the beneficial ownership of companies and trusts via accessible and interconnected national registers; and strengthens the powers of the FIUs for domestic analysis and to provide active cooperation. The European Commission is tasked with assessing the effectiveness of the cooperation between EU FIUs and proposing a 'coordination and support mechanism'.

Cooperation between FIUs

In order to implement the European provisions, the European Commission is currently preparing a report on the activities of and cooperation between the FIUs and setting up a 'coordination and support mechanism'.[29] The analysis focuses on four main themes: 1) cooperation between European FIUs and FIUs in third countries; 2) cooperation between EU FIUs; 3) the tasks of the European mechanism; and 4) the possible role of the FIUs and the mechanism in carrying out controls. There has been extensive consultation on these issues with Member States and in particular with the FIUs. They have produced joint analyses and positions to contribute to the ongoing reflections based on their experience and the relative operational needs.

The European Coordination and Support Mechanism for the FIUs

The European mechanism should acquire the competences currently assigned to the FIUs' Platform, such as for the uniform implementation of the common rules and for participation in the functioning of FIU.NET.

The mechanism should focus on the problematic areas found in the recent Mapping Exercise and on the conclusions and proposals set out in the relative Report. It would specifically cover working methods and practices, analytical activities that cannot be carried out effectively at national level only, and cooperation between European FIUs. However, the tasks entrusted to the mechanism should not include the core functions of the FIUs; therefore, the receipt of suspicious transactions reports from obliged entities would remain at national level, as well as their financial analysis and the subsequent dissemination.

A first step could be the definition of common practices or guidelines on the content

[27] Directive (EU) 2018/843.

[28] Directive (EU) 2015/849.

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

of STRs, and on the nature and processing of the analyses. Given the generic nature of the European rules on this issue, greater uniformity in reporting and analysis would facilitate both domestic effectiveness and mutual cooperation.

Further operational alignment could be carried out specifically on the instruments and methods for joint analysis; this process, which is already found in the list of the Platform's competences,[30] concerns the examination of cases that, owing to their transnational nature, even if enriched by the exchange of information between the authorities, cannot be handled effectively by the single FIUs involved.

The mechanism could be the appropriate forum for defining uniform patterns and methods for the cooperation activities that European FIUs must undertake at bilateral or multilateral level. This may include measures relating to the content and format of exchanges, the use of the information provided, and the difficulties in relationships with FIUs in third countries.

In any case, the organizational solution chosen will have to ensure the governance and management of the information in order to guarantee independence (both of the mechanism and of every FIU involved), confidentiality and the appropriate handling of the information.

Other European legislation measures

Other European legislative measures, whether recently adopted or still being defined, even if not closely connected to anti-money laundering rules, require corresponding changes at national level. Such initiatives have closely related motivations and objectives: the strengthening of the safeguards against the risks of terrorism; the problems found in the compliance control system; and the need to expand cooperation and exchanges of information of a financial and investigative nature with supervisory authorities, including beyond the scope of the fight against money laundering and financing of terrorism. The impact on FIUs' activities, powers and cooperation is significant.

Cooperation between FIUs, investigative authorities and Europol

A draft directive[31] on information exchanges between FIUs, national investigative bodies and Europol provides for flows of financial information from FIUs to the said authorities, in compliance with the FIUs' independence, both at operational level and for analysis activities. The draft confirms and reinforces the need for FIUs to access appropriate investigative information.

The aim of the intervention is to use the FIUs' information as much as possible to support investigations into serious crimes,[32] in addition to money laundering, predicate crimes and the financing of terrorism.

Cooperation between FIUs and supervisory authorities

Given the significant cases of European banks' involvement in illegal activities, more direct forms of cooperation between FIUs and supervisory authorities are outlined.

[30] Article 51 of the Fourth Directive provides for 'joint analyses of cross-border cases'.

[31] The draft directive was drawn up on the basis of the Proposal of the European Parliament and of the Council, laying down provisions to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and it repeals Council Decision 2000/642/GAI.COM/2018/213 final — 2018/0105 (COD).

[32] Identified by referring to the list of cases in Regulation (EU) 2016/794 on Europol's powers.

Against this backdrop, amendments have been included in the revision of the 'CRD IV' Directive[33] providing for both enhanced cooperation between supervisory and anti-money laundering authorities and forms of information sharing between them and the FIUs.

In accordance with these guidelines, FIUs will cooperate more widely with the prudential and anti-money laundering authorities at national and European level. In particular, information on STRs may be used for compliance and internal organization controls more broadly, though also more selectively. At the same time, information on anomalies detected during supervisory checks and communicated to the FIUs will make it possible to identify and analyse possible illegal economic activities.

The changes currently being adopted[34] to Regulation (EU) 2010/1093 on the EBA are part of the same context. Though confirming national competence in anti-money laundering controls, the EBA is entrusted with new responsibilities for conducting reviews of national supervisory authorities, regarding the exercise of enforcement and sanctions, the application of binding mediation powers, the use of substitute powers in the event of inaction by national supervisors, and the drawing up of guidelines to encourage checks and develop cooperation. The EBA will have the power to acquire the necessary information for its new tasks from the competent national supervisory authorities; there is also a need for close coordination between the EBA and the FIUs, in accordance with their status and obligations.

The coordination work centralized at European level, made necessary by the recent emergence of local crises, should be preceded by a mapping of the various national systems with a view to achieving greater convergence among them, thereby preventing this centralization from lowering the efficiency levels achieved by the best legal systems, as the UIF has pointed out on several occasions.

Cash controls

Regulation (EU) 2018/1672 extends the measures for monitoring cross-border transfers of cash and for sharing and using the relevant information. The new rules require the competent authorities (usually customs agencies) to transmit all the declarations to the FIU of their country concerning the transport of values of an amount of €10,000 or more twice a month; the declarations also include instruments other than cash, such as payment cards and other means connected to liquidity. In addition to the declarations, information on cases of suspected money laundering or financing of terrorism detected by the customs authorities should be sent to the FIU, with no threshold limits, as well as allegations of breaches of the obligation to declare that emerged during the checks.

The information flows between the Customs and the FIUs will go through the Customs Information System, to which the FIUs will have to be connected according to the technical standards established by the European Commission with the help of the Cash Control Working Group, in which the customs administrations of the Member States participate. The Regulation also requires FIUs to submit declarations containing elements of interest or cross-border relevance to their European counterparts.

Criminal justice rules

As regards criminal justice rules, following the extension of the terrorist financing offence under Directive 2017/541/EU, a new, more comprehensive and harmonized

[33] See the European Parliament's legislative resolution of 16 April 2019 on the proposal for a directive of the European Parliament and of the Council amending Directive 2013/36/EU as regards exempted entities, financial holding companies, mixed financial holding companies, remuneration, supervisory measures and powers, and capital conservation measures (COM (2016) 0854 - C8-0474/2016-2016/0364 (COD)).

[34] See COM (2018) 646 final.

definition of money laundering was introduced, based on international sources (Directive 2018/1673/EU).

This intervention deals with both the configuration of money laundering conduct and of predicate offences. The former is defined and outlined in accordance with international rules; the latter are defined in broad terms, by reference to both specific cases and the size of the sanction laid down in national law; the importance of offences committed abroad is foreseen, provided that they constitute criminal offences within the national territory as well. The need to determine all the facts and circumstances relating to predicate offences is excluded from a money laundering prosecution. The new definition goes together with and does not replace the administrative one, which is the basis for preventive measures under the Fourth Anti-Money Laundering Directive.

OLAF

The Regulation[35] on the establishment of a European Public Prosecutor's Office (EPPO), which is in charge of prosecuting offences affecting the financial interests of the Union, assigns the task of supporting the related investigations to OLAF (European Anti-Fraud Office). In this context, in May 2018, the Commission presented a proposal for a regulation to adapt OLAF's competences and powers accordingly, through amendments to Regulation (EU) 2013/883.

The Proposal includes the possibility for OLAF to acquire information from national bank account archives, made obligatory by the Fifth AML Directive, and sees the FIUs as the national access point for information on bank accounts. The negotiation in Council and Parliament envisages a more general reference to the authorities competent to serve as national access points, which can include FIUs, as identified by the Member States.

EPPO

A Communication presented by the Commission to the Parliament and Council in September 2018[36] foresees extending the competences of the European Public Prosecutor's Office to include coordinating and carrying out investigations into terrorism.

The scope of the action is determined by a reference to the recent Directive 2017/541/EU on criminal matters and includes a broad list of cases, including financial support for terrorism. With this in mind, the Communication specifically refers to the necessary forms of cooperation between the European Public Prosecutor and the FIUs to be set out in the provisions for their implementation.

9.1.2. Further European and international initiatives

The Supranational Risk Assessment

When implementing the European provisions in 2018, the European Commission started work on updating the first supranational risk assessment (SNRA), which was published on 26 June 2017.

The assessment, to be updated every two years, is envisaged by the Fourth Directive as an integral part of the risk-based approach, which is the basis of the AML system. The 2017 SNRA contained recommendations with which Member States were obliged to comply under the 'comply or explain' principle.

Some mitigation measures were introduced by the Fifth Directive, with particular regard to the completion of the risk-based approach, to the establishment of beneficial owners' registries, and to strengthening cooperation between FIUs. The new supranational

[35] Regulation EU/2017/1939.

[36] COM (2018) 641 final.

assessment, published in the second half of 2019, reviews the risks identified in the first supranational assessment in order to assess whether they persist, in light of the Commission's recommendations and the measures applied by the Member States; the assessment identifies new risk factors of a supranational nature.

The European FIUs are directly involved in the in-depth analyses and contribute by providing the results of their operational activities. The UIF participated actively and cooperated with the other Italian organizations concerned.

The work at European level covered various aspects: recognizing the measures adopted by member states to deal with the risks that emerged in the first assessment; seeing to what extent the relative recommendations have been implemented; collecting and assessing the data on the activities carried out in the various fields of interest (reporting suspicious transactions, international exchanges, investigations and confiscations); and describing newly emerged risks.

High-risk third countries

The European Commission published the updated list of third countries that, because of strategic shortfalls in their prevention systems, put the EU at high risk of money laundering or financing of terrorism;[37] they were identified using a specific methodology drawn up on 22 June 2018 with the help of the Member States.

The document was drawn up using a different approach from that based on the passive alignment with the FATF's black list (often criticized by the European Parliament), and defines the procedure and criteria used by the European Union to autonomously identify those jurisdictions with significant weaknesses as far as the EU is concerned. The elements on which to focus evaluations are identified with regard to the safeguards envisaged by the Fourth Directive, as supplemented by the fifth Directive; they include the legal and institutional framework, money laundering and financing of terrorism cases, reporting obligations, the powers of competent authorities, preventive measures, the degree of corporate and tax transparency, the sanctioning system and international cooperation.

The objective of identifying high-risk third countries is, on the one hand, to protect the integrity of the European Union's financial system through the application by obliged entities of enhanced due diligence measures commensurate with the risks, and on the other hand, to encourage high-risk countries to take the necessary corrective measures to overcome the shortcomings identified.

The assessment takes into account both the evidence gathered by the FATF and by other competent bodies, and issues of particular importance from a European perspective, also based on evidence from Member States and other institutions. The procedure provides that the Commission can request data contributions from European organizations such as the EU FIUs Platform, European supervisory authorities, Europol and the European External Action Service.

Based on the analyses carried out, the Commission identified 23 countries with strategic shortcomings in their systems for combating money laundering and the financing of terrorism. A list was published on 13 February 2019, compiled in line with the indications of the European Parliament and more wide-ranging than that of the FATF.

[37]Article 9 of the Fourth Directive, as amended by the Fifth Directive, assigned the task of forming a list of countries at risk for Europe to the Commission, thereby allowing the criterion based on the inclusion of 'equivalent' anti-money laundering regimes on a list of third countries to be dropped.

The Commission identified 23 countries: Afghanistan, American Samoa, the Bahamas, Botswana, the Democratic People's Republic of Korea, Ethiopia, Ghana, Guam, Iran, Iraq, Libya, Nigeria, Pakistan, Panama, Puerto Rico, Samoa, Saudi Arabia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, the US Virgin Islands and Yemen.

However, the list drawn up by the Commission was strongly opposed by the Member States in the Council. They felt it was inappropriate to depart from the FATF's approach and from the reference to countries identified by the FATF as having 'strategic deficiencies'. The Council therefore rejected the adoption of the relative delegated act, which had actually been approved by the European Parliament.

In February 2019, the FATF discussed and approved the first evaluation report on the follow-up to the Mutual Evaluation of Italy.

The FATF's follow-up assessment of Italy

Two years after the evaluation of Italy carried out in 2015-16, this Report concerns the Technical Compliance sector (analysis of compliance of the rules with FATF standards). The evaluation was positive for this sector, also in light of the rules introduced with the transposition of the Fourth Directive. The rating related to the eight Recommendations, including those concerning the UIF's activity, was raised to the maximum level (Compliant); at the same time, there is still evidence of the limits that remain in the new regulatory framework.

For cases of specific interest to the UIF, there is a recognition of the explicit extension of the reporting obligation and of the Unit's field of activity to include cases of suspected predicate offences, as well as of money laundering and the financing of terrorism (Recommendations 20 and 29). The new provisions are acknowledged, which envisage forms of access for the UIF to investigative information to support analyses (Article 12(4) of Legislative Decree 231/2007). As regards international cooperation, the extension of the UIF's field of activity to include predicate offences for money laundering also resolves the observation made previously in Recommendation 40, by making explicit the Unit's full capacity to exchange information (see Article 13 of Legislative Decree 231/2007).

The assessment of the real applicative effectiveness of the new provisions will be the subject of a subsequent follow-up on aspects of Effectiveness that, according to the rules governing the assessment process, is expected to occur five years later, also based on information to be obtained in a new on-site visit. In other respects, the report shows progress in regulating the risk-based approach (Recommendation 1), in AML supervision as regards the assessment of specific risks (Recommendation 26) and in the range of sanction measures (Recommendation 27). In these cases too, it was proposed that the ratings be raised from Largely Compliant to Compliant. Given the absence of adequate developments, the non-fully positive assessments of compliance with the due diligence standards for 'politically exposed persons' (Recommendation 12) and for correspondent banking (Recommendation 13) are confirmed for the time being.

UNCAC Assessment

The second cycle of the review of Italy's implementation of the United Nations Convention against Corruption (UNCAC) was concluded. This exercise, conducted by an international team selected by the United Nations Office for Drugs and Crime (UNODC),

focuses on the implementation of the Convention chapters relating to prevention (Articles 5-14) and asset recovery (Articles 51-59).

The UIF, together with ANAC, CONSIP and the Ministry of the Interior, were members of a small group that, between 2017 and 2018, followed the various stages of the peer review process, providing written contributions and participating in a dialogue with the evaluators.

The Executive Summary of the UNCAC Report devotes a great deal of attention to AML prevention measures, taking account of the recent legislative developments for implementing the Fourth European Directive and transposing the FATF's recommendations for Italy after its Mutual Evaluation. The document reviews the UIF's functions, highlighting their variety and pointing out that other institutional stakeholders of the UIF have been introduced in the context of domestic cooperation, but that there are also limits affecting the UIF's access to investigative information. One of the recommendations addressed to Italy is to further strengthen cooperation between the UIF and other competent authorities.

The UIF regularly participates in the Table for inter-institutional coordination established by the Ministry of Foreign Affairs to create a unified approach to corruption, stimulate dialogue between the entities concerned, define positions, and promote coordination in the various relevant forums, especially at international level.[38]

9.2. National legislation

In 2018, Italy's AML legislation was subject, at primary level, to limited amendments and, at the secondary regulatory level, to various initiatives of the competent authorities aimed mainly at implementing the reform made by Legislative Decree 90/2017.

New regulatory measures are now needed to transpose the Fifth Directive into Italy's legal system.

9.2.1. Legislative measures

The work to transpose the Fifth Directive

Work began recently at the MEF to make amendments to Legislative Decree 231/2007 aimed both at implementing the Fifth Directive[39] (see the section 'The evolution of European legislation') and at correcting certain problems that emerged when applying the provisions introduced by the 2017 reform.[40]

On 22 March 2019, the Ministry of Economy and Finance held a public consultation on a draft legislative decree to serve these purposes.

In brief, the draft envisages: i) extending AML obligations to digital portfolio service providers and a more precise configuration of subjects trading works of art or that act as

[38] The Table includes various institutions, including the Department of Public Administration, the ANAC, the Ministry of Justice, CONSIP, the Ministry of Economy and Finance, CONI, the Ministry of the Interior, the Finance Police, the Customs and Monopolies Agency, ISTAT and the AGCM.

[39] The parliamentary procedure to issue the delegation law, including the transposition of the Fifth AML Directive, is ongoing.

[40] Pursuant to Article 31(5) of Law 234/2012, within 24 months of the entry into force of the legislative decrees adopted in relation to the legislative delegations conferred by the European delegation law for transposing directives, the Government can adopt supplementary and corrective measures. The expiry date for Legislative Decree 90/2017 was 4 July 2019.

intermediaries in such trade (also in free ports); ii) implementing the specific EU provisions that regulate international cooperation between authorities; iii) some interventions on institutional cooperation between the UIF, the DNA and investigative bodies; iv) a review of some customer due diligence profiles (with particular reference to 'enhanced' ones for transactions and relationships involving high-risk third countries); v) updating the provisions concerning the list of entities that can access information on the beneficial ownership of legal entities and trusts; and vi) some amendments to the provisions for administrative sanctions.

Legislative adaptation

In 2018, Legislative Decree 231/2007 underwent two technical adaptation procedures. The crime of 'misusing and falsifying credit and payment cards' was removed from Legislative Decree 231/2007,[41] following its insertion into Article 493-ter of the penal code as a result of Legislative Decree 21/2018,[42] which moved some offences already present in special laws to the penal code.

In addition, with regard to bank and postal cheques issued for sums equal to or above €1,000, in the event that a cheque is not marked as non-transferable or if the name or business name of the payee is missing, the minimum sanction applicable has been changed from €3,000 to ten per cent for violations involving amounts of less than €30,000, if less serious circumstances pursuant to Article 67 of Legislative Decree 231/2007 are established.

On 1 January 2019, the limit on cash transfers for purchasing goods and services relating to tourism by natural persons of nationalities other than Italian and not resident in Italy was changed back to €15,000. The requirements of the law are without prejudice to the transferor of the good or the service provider.[43]

9.2.2. Secondary discipline and self-regulation

The reporting of STRs by general government offices

In April 2018, the *Guidelines and anomaly indicators drawn up by the UIF for the general government offices* were issued,[44] which are required to send the UIF data and information concerning suspicious transactions.[45] In its meeting of 27 March 2018, the Financial Security Committee (FSC) gave a favourable opinion on the Unit's measure and also approved the guidelines for the mapping and assessment of risks by the general government entities concerned (see the *Annual Report for 2017*, section 1.3.1).

The Guidelines regulate, with a view to continuity with the rules previously applicable on this matter, the conditions, methods and content of communications sent by general government entities. The anomaly indicators are designed to facilitate assessments linked to communications of suspicious transactions, to reduce burdens and to facilitate the homogeneity of such communications. The indicators refer to the 'subject with which the transaction is connected', i.e. to the natural person or legal entity entering into a relationship with general government entities, in respect of which elements of suspicion can emerge. The general indicators concern the identity or behaviour of the abovementioned subject and how

[41] Article 55(5) of Legislative Decree 231/2007.

[42] Article 7 of Legislative Decree 21/2018, issued to implement the delegation contained pursuant to Article 1(85) letter q) of Law 103/2017.

[43] Article 1(245) of Law 145/2018, which amends Article 3 of Decree Law 16/2012, converted with amendments into Law 44/2012. The limit under Article 3 had been set at €10,000 by Legislative Decree 90/2017.

[44] The provisions were published on the UIF's website and in the Gazzetta Ufficiale, General Series, No. 269, 19 November 2018.

[45] Article 10(4) of Legislative Decree 231/2007.

the transactions are requested or carried out; the specific ones for types of activity refer to active administration or control tasks, pursuant to Article 10(1) of Legislative Decree 231/2007, and specifically identify the anomalies inherent in the public tender and contracts and public funding sectors, and relating to the 'real estate and trade' sector.

The diffusion of the Unit's indications has helped to increase the focus on active cooperation on the part of the category of entities connected with general government, as shown by the requests sent to the UIF by various regional and municipal authorities and by important government-owned companies (see the box 'The active cooperation of general government' in Chapter 1).

Threshold-based communications

Legislative Decree 90/2017 introduced into Legislative Decree 231/2007[46] the obligation for operators to periodically send communications to the UIF that refer to data and information identified on the basis of objective criteria linked to money laundering or terrorist financing risks. Threshold-based communications are used for investigating suspicious transactions and analysing phenomena or typologies of money laundering and financing of terrorism. The UIF is responsible for identifying, by means of instructions and after consulting the FSC, the transactions and their content and how they were sent.

Instructions for sending threshold-based communications

The Instructions provided by the UIF identify, in accordance with national and international risk assessments, the categories of transactions concerned and the parties to which the Measure is addressed.

Cash transactions are subject to new reporting obligations as a category at high risk of money laundering and financing of terrorism; a criterion for recording transactions has been established, based on exceeding a threshold of €10,000 or more, calculated on a monthly basis and also taking into account any 'cumulated' operations during the same period, individually equal to or above €1,000 and carried out by the same client or executor.

In view of the type of operations targeted, the list of recipients is composed of banks, Poste Italiane, EMIs, PIs, branches of such intermediaries from EU and third countries, as well as banks, PIs and EMIs from EU countries that have to designate a central contact point.

Recipients must forward the data requested on a monthly basis. Due to the confidential nature of the information handled and in line with the other reporting requirements, the information will be collected by the UIF via its Infostat portal.

In accordance with a precise legislative indication, hypotheses in which threshold-based communications exclude the obligation to report a transaction as suspect are expressly identified; in particular, this exclusion is linked to two criteria, an objective one (the failure to connect cash transactions with other different types of operations that lead to conclusions of a complex suspected activity) and a subjective one (cash transactions are not made by customers at high risk of money laundering).

In July 2018, the Unit submitted the 'Instructions for threshold-based communications' for public consultation This was the first public consultation carried out on a measure falling within the competence of the Unit which, although not requested, was deemed appropriate

[46] Article 47 of Legislative Decree 231/2007.

given the importance of the requirements, also in order to ensure the transparency of the Unit's regulatory choices. The consultation, which ended on 10 August 2018, recorded a broad and fruitful involvement on the part of operators, which gave rise to explanations and limited further clarifications and corrections of the regulatory text and its technical appendix.

On 14 November 2018, the Measure was submitted for the approval of the Financial Security Committee that, following a written exchange with the various authorities concerned, expressed a positive opinion on 20 March 2019. The Instructions were published on 28 March 2019 on the UIF's website (together with the results of the consultation) and on 15 April in the Gazzetta Ufficiale.

Since it took a long time for approval to be given, the obligation to send threshold-based communications dated from April 2019; however, for the first application, the Measure envisaged that data for April, May, June and July could be sent by 15 September 2019.

Virtual assets

As regards virtual currencies, on 28 May 2019, the UIF issued a specific *Communication* (see the box 'Reports on suspicious transactions and virtual asset transactions' in Chapter 3).

Consob

On 4 June 2018, Consob issued a communication[47] on the criteria and methodologies for the self-assessment of the money laundering and financing of terrorism risks[48] to which auditors and auditing firms are exposed in the course of their activities.

The methodology for risk self-assessment is divided into the phases of identifying 'inherent risk', analysing the vulnerabilities of the risk mitigation safeguards actually adopted, and determining the residual risk. Once the residual risk has been determined, any corrective actions or adjustments have to be described in the risk self-assessment document.

In September, the Commission adopted the single implementing Regulation of Legislative Decree 231/2007 for supervised auditors and auditing firms, regarding organization, procedures and controls, as well as due diligence and keeping records.[49]

The Regulation envisages that auditors and auditing firms must provide themselves with organizational and procedural safeguards and adequate internal checks to prevent, mitigate and manage money laundering and financing of terrorism risks. Clearly identified and appropriately specialized resources, procedures and organizational functions are required; instructions are provided for risk assessment and customer due diligence. The requirements and procedures for identifying the person responsible for reporting suspicious transactions, as well as the activities required of those involved in the signposting procedure, are indicated as part of active cooperation. Arrangements for storing documents, data and information in paper or electronic format are acceptable; however, some data and information need to be recorded in computer files to ensure that it is quick and easy to consult them.

IVASS

On 12 February 2019, IVASS issued a Regulation on organization, procedures and internal checks and on customer due diligence for the insurance sector.

The provisions strengthen the anti-money laundering safeguards, further enhancing the adoption of a risk-based approach by companies and insurance intermediaries. In terms of active collaboration, the STR manager is responsible, among other things, for checking

[47] Communication No. 0186002 of 4 June 2018.

[48] Pursuant to Article 15(1) of Legislative Decree 231/2007.

[49] Consob Decision No. 20570 of 4 September 2018.

suspicious transactions, also on a sample basis and together with the AML and the audit offices, for the appropriateness of the first level assessments.

It was established that if it is not possible to identify a firm, brokers can inform the UIF directly about suspicious transactions. In the area of due diligence, it was expressly confirmed that the constant monitoring of customer behaviour also refers to cases where several insurance contracts are distributed to the same entity, albeit on behalf of other firms. In addition, in the event of a discrepancy between the executor and the person who pays the premium, although there has been no equivalence between the two, an obligation was established to identify the latter and obtain information about the relationship with the contractor.

Bank of Italy

The Bank of Italy has submitted for consultation the arrangements of the provisions relating to: (i) anti-money laundering organization, procedures and controls; (ii) customer due diligence; (iii) record-keeping requirements; and (iv) administrative sanctions and procedures.[50] The UIF has also contributed to the development of these regulatory schemes.

The provisions on anti-money laundering organization, procedures and internal controls were issued on 26 March 2019.

These provisions identify the general principles of the risk self-assessment methodology introduced by the AML Decree. Particular attention is paid to the role of the contact points and to the relationship between them, foreign intermediaries and the network of distributors and agents. In the field of active cooperation, the requirements and tasks for the STR manager are regulated; the manager's independence and confidentiality requirements are strengthened, as is the role. The STR manager should assess suspicious transactions, including in the absence of communications from the first level of control, and verify on a sample basis the appropriateness of the performance of the latter. In addition, more detailed rules are introduced for groups, conferring a prominent role on the parent company's management, checking and coordination activities and including the obligation to set up a joint database that allows all firms to make a homogeneous assessment of their customers (see the *UIF's Annual Report for 2017*, section 1.3.1).

The due diligence provisions further optimize the risk-based approach; they give additional guidance in respect of the Decree for identifying beneficial owners; they contain examples of the high risk factors set out in the Decree and identify the enhanced measures that can be taken. Some technologically advanced instruments are included among the checking mechanisms for remote due diligence; third party intermediaries can be used for due diligence, in line with the provisions of the AML decree, also where the latter have carried it out remotely (see the *UIF's Annual Report for 2017*, section 1.3.1).

The draft provisions for keeping and using data and information for anti-money laundering and financing of terrorism purposes, taking into account that the AML Decree no longer provides for the mandatory institution of the single electronic archive (AUI), are intended to ensure that the competent authorities can obtain all the necessary information in a timely and complete manner in order to carry out their AML tasks. Specifically, intermediaries may extract data for these purposes from a chosen storage system based on the technical specifications and standards included in the provisions or use standardized archives, including those already established on the date of entry into force of the reform. In order to reduce the burden on the obliged entities, the provisions confirm the exemption

[50] The new sanctions provisions were issued on 15 January 2019; for their content, see below.

from the obligation to make available, in a standardized way, data relating to relationships and/or transactions considered to be less important for AML supervisory purposes.

Bank of Italy Communication on PEPs

On 23 January 2018, the Bank of Italy issued a Communication on enhanced due diligence procedures for Politically Exposed Persons,[51] in order to disseminate good practices and examples that can improve intermediaries' management of their relationships.

Based on the problems found following some thematic inspections by the Bank of Italy, the following areas for improvement were identified: i) management of relationships with PEPs; ii) identification of such subjects; iii) risk classification; iv) setting out clear internal procedures and effective safeguards both in setting up and renewing relationships, as well as systems for monitoring transactions that can intercept any anomalies; and v) the appropriate organization of the internal checks system.

The Bank of Italy's Measure on sanctions

On 15 January 2019, the Bank of Italy reviewed the supervisory provisions for sanctions in order to take account of the new elements introduced by Legislative Decree 90/2017 with regard to AML violations.[52] The Measure governs the phases of the sanctions procedure and identifies the elements that may indicate the existence of serious, repeated, systematic and multiple violations.

Emphasis is placed on: (i) the possibility of exposing the intermediary to significant money laundering, financing of terrorism or, more generally, significant legal or reputational risks; (ii) recurrent infringements of the same provision in a significant number of cases, taking into account the size, organizational complexity and operations of the intermediary; (iii) the widespread and non-occasional nature of infringements, such that they can be attributed to the intermediary's normal mode of operations or are symptomatic of weaknesses in the operational procedures, and in the organizational and control arrangements adopted by the intermediary; and (iv) the existence of violations of a number of anti-money laundering provisions.

The Measure also takes account of the opinion of 3 August 2018, in which the Council of State clarified that the Bank of Italy has the power to impose sanctions on holders of administrative, management or supervisory functions in supervised intermediaries for AML infringements, with the exception of those concerning the reporting of suspicious transactions that, as expressly provided for by law, fall under the competence of the Ministry of Economy and Finance.[53]

As regards the time sequence for sanctions provisions and the resulting need to apply the most favourable law to the person responsible for the violations, as part of the sanctions system amended in the wake of the Fourth AML Directive, the Supreme Court of Cassation established that Article 69(1) of Legislative Decree 231/2007 is also applicable to pending proceedings for opposing an administrative penalty that has already been paid. This is the case if the application of Article 69 of Legislative Decree 231/2007, 'No one shall be punished for any act that, on the date of entry into force of the provisions laid down in this Title, is no longer illicit', is not affected by the failure to conclude the sanctions procedure,

[51] Articles 1(2) letter dd) and 24(5) letter c), of Legislative Decree 231/2007.

[52] On this occasion, the provisions were aligned with what is laid down at the level of sanctions to implement Directive 2014/65/EU (MiFID II) and Directive 2014/91/EU (UCITS V).

[53] Article 62(9) of Legislative Decree 231/2007.

but only by the definitive nature of the Measure.[54]

The Bank of Italy's provisions for cash handlers

On 23 April 2019, the Bank of Italy issued the provisions for registering on and managing the list of professional non-financial operators in the transport and safe custody sector pursuant to Article 134 of the TULPS (Consolidated Law on Public Security), limited to cash handling.[55] The same measure contains provisions for these operators in the field of anti-money laundering organization, procedures and controls.

The provisions identify the requirements for registration; specific anti-money laundering organizational units are also established, making things simpler for smaller operators, and regular reporting for the purposes of preventing money laundering and financing of terrorism is regulated.

Provisions of the Customs and Monopolies Agency

For the gaming sector, on 15 February 2019 and after submitting them to the FSC, the Customs and Monopolies Agency issued provisions to support operators, for the implementation of Legislative Decree 231/2007.[56] These are guidelines to help gaming licensees in the field of anti-money laundering, with specific provisions for the bingo, remote gaming, fixed-odds horse racing and sports bets, and video lottery terminal sectors.

The guidelines envisage minimum measures for carrying out preventive activities, allowing the licensee to adopt additional measures. They also identify behaviour to be monitored in order to detect any anomalies, without prejudice to what is set out by the anomaly indicators and patterns drawn up by the UIF. Gaming licensees are required to adopt adequate procedures and control systems to mitigate and manage the risks of money laundering and financing of terrorism. These procedures and systems must make it possible to verify that activities are also carried out correctly by distributors and operators and must be appropriate to the risks involved: types of game; the geographical areas in which the gaming is provided; the specific customers of sales points; and the impossibility of or difficulty in identifying customers. The licensees ensure the training and updating of the staff responsible for activities relating to compliance with anti-money laundering obligations.

Technical rules for self-regulatory bodies

To implement the provisions of the reformed Legislative Decree 231/2007,[57] in 2018, some self-regulatory bodies drew up technical rules for risk analysis and assessment, internal checks, due diligence and data storage for the benefit of the respective professional categories.

The objective of self-regulation is to formulate operational rules that adequately exploit the specificities of each professional category, in accordance with the risk-based approach. The texts proposed by these bodies were submitted for examination to the FSC for the purpose of issuing the opinion as provided for by law. The FSC held that the technical rules, if appropriate to the content of and applied in compliance with the opinion, are an appropriate and simplified way of meeting the customer due diligence and record-keeping requirements prescribed by the legislation in force.

The Committee's first opinion (18 September 2018) dealt with the technical rules of the National Council of Notaries (CNN). These rules identify some notarial activities from which due diligence obligations are excluded and pay particular attention to the rules applicable

[54] Cassation II Section CIV, Judgments No. 20647 and No. 20648 of 8 August 2018.

[55] Article 8 of Decree Law 350/2001, converted with amendments into Law 409/2001.

[56] Article 52(4) of Legislative Decree 231/2007.

[57] Article 11(2) of Legislative Decree 231/2007.

following the 2017 reform. Guidance is provided on the simplified due diligence, especially with regard to low risk factors relating to types of customers, as well as on how information is acquired for the purpose and nature of the service. Further rules concern the identification of the customer or the effective holder and the beneficial owner, the due diligence timeframe and how data and information are to be stored.

The second act issued by the FSC (6 December 2018) concerns the rules drawn up by the National Council of the Order of Accountants and Bookkeepers (CNDCEC), definitively approved by the Council on 16 January 2019. These rules provide indications for fulfilling the obligations in relation to risk assessment, customer due diligence and record, data and information storage. The CNDCEC specifically classified the main services provided by accountants and bookkeepers based on their inherent risk by providing explanations in this respect. Implementation details are also explained for ordinary, simplified and enhanced customer due diligence and for the fulfilment of record-keeping obligations. The adoption of this approach aims to encourage abandoning bureaucratic approaches to the fulfilment of obligations, while promoting a focus on the situations most exposed to risk. It is to be hoped that this is beneficial for active cooperation in terms of the significance of the suspicions identified as worth reporting to the UIF. In light of the technical rules, on 16 May 2019, the National Council approved the guidelines for risk assessment, due diligence, and the storage of documents, data and information pursuant to Legislative Decree 231/2007.

As far as the category of lawyers is concerned, the technical rules drafted by the National Lawyers' Council (CNF) are being considered by the FSC. The CNF's indications aim to exclude the application of the preventive regulations to some activities carried out by lawyers, to provide clarification on the rules applicable following the 2017 reform, and guidelines on risk assessment, due diligence, data conservation and reporting suspicious transactions; moreover, this last area is not included among those that Legislative Decree 231/2007 leaves to the self-regulatory bodies.

The Association of Employment Consultants is currently drawing up the technical rules on anti-money laundering.

10. RESOURCES AND ORGANIZATION

10.1. Organization

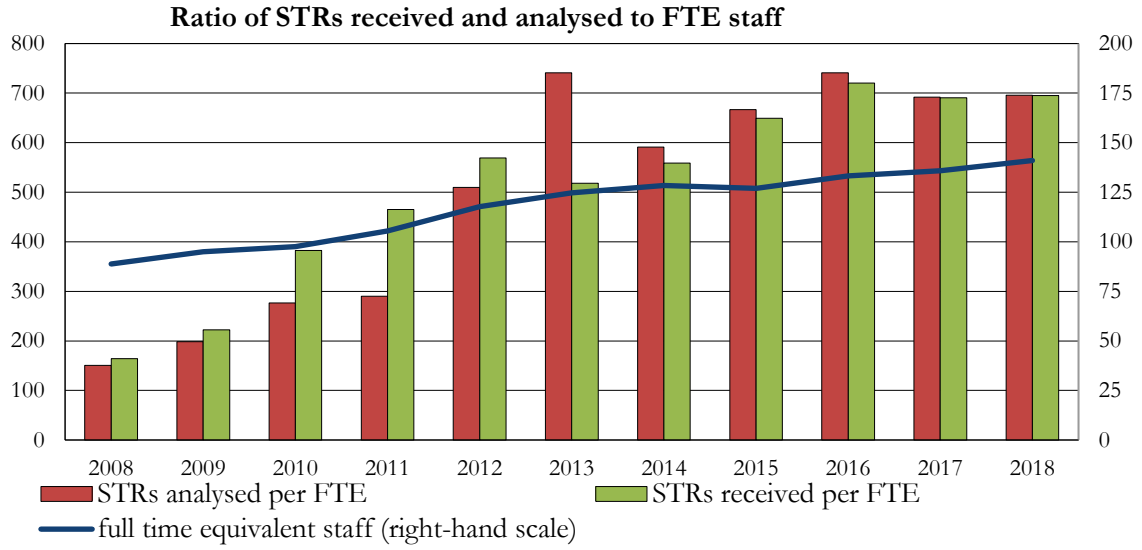
The UIF is headed by the Director, who is assisted by the Deputy Director, a number of staff managers and two Directorates. The Suspicious Transactions Directorate is in charge of the financial analysis of suspicious transaction reports and the Analysis and Institutional Relations Directorate is responsible for legislation, analysing financial flows and cooperating with the judicial authorities and other domestic and foreign authorities.

In February 2019, an organizational reform was approved that, owing to the Unit's greater operational needs, includes the role of Deputy Head of Directorate in line with the Bank of Italy's current system,[58] the creation of three new divisions and the elimination of two operating sectors. The Director is also assisted by the Advisory Committee for the Review of Irregularities (COCEI), which is a collegiate body with the tasks of analysing anomalies and suspected irregularities uncovered by the UIF in order to initiate sanction procedures, forwarding reports to judicial and sectoral supervisory authorities, and taking any other action deemed necessary. A committee of experts has been established as required by law, 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 a valuable forum for discussion, providing constant support for the UIF's activities and insights into the most important issues.

10.2. Performance indicators and strategic plan

In 2018, the performance indicator stood at 696 STRs analysed per full-time equivalent (FTE) employee, with a further slight improvement compared with 2017 (Figure 10.1).

Figure 10.1



[58] See Bank of Italy Resolution 66/2019.

The variation in the indicator reflects an increase in analysed reports that is higher than the number of human resources used, which reduced the backlog: at the end of the year, the number of reports still being processed was 54 per cent of the monthly average flow.

The indicator tends to underestimate the real increase in productivity because it does not take into account the activities carried out by the UIF that are not directly or indirectly linked to the processing of STRs, which are increasing significantly.

Definition of the strategic lines

The UIF draws up its strategic action plan every three years (Figure 10.2). The 2017-19 Action Plan envisages that the Unit will seek to improve the efficiency and quality of its analyses by developing methodologies and IT tools that support a risk-based approach and allow for a more in-depth analysis of STRs.

The commitment to increasing cooperation with reporting entities, investigative and judicial bodies, the DNA, other competent authorities and foreign FIUs, also through the impetus given to new communication tools, is confirmed.

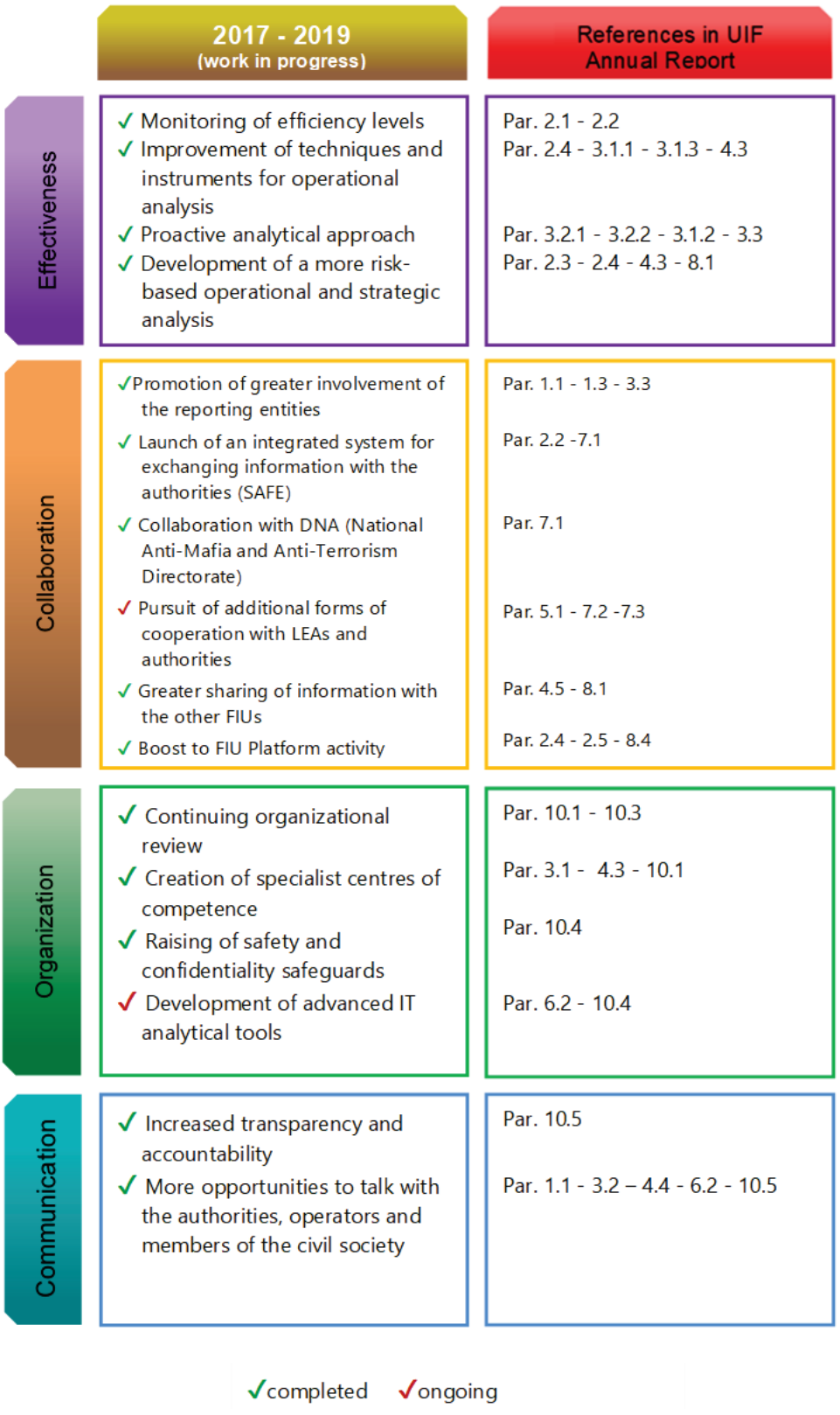
The organizational objective focuses on the development of specialized centres and IT analysis tools, and on improving security and privacy safeguards. In terms of communication, the UIF seeks to enhance transparency and accountability, including by promoting dialogue with the reporting entities, the institutions and civil society.

In 2018, the UIF's strategic planning was updated to take account of the effects of the implementation of the regulatory reform of 2017, which includes new operational tasks (such as those connected with the introduction of threshold-based communications and with the increase in the number of institutional partners) and regulatory tasks (in particular, guidelines for public administrations and threshold-based communications).

Further developments will result from the advance of FinTech, which is leading to changes in financial products and services, and from the transposition of the Fifth Anti-Money Laundering Directive, which will further extend the scope of obliged entities and the information powers of FIUs. Other European measures in the pipeline will introduce new forms of cooperation between FIUs and Europol, national investigation bodies, and tax and customs agencies.

Figure 10.2

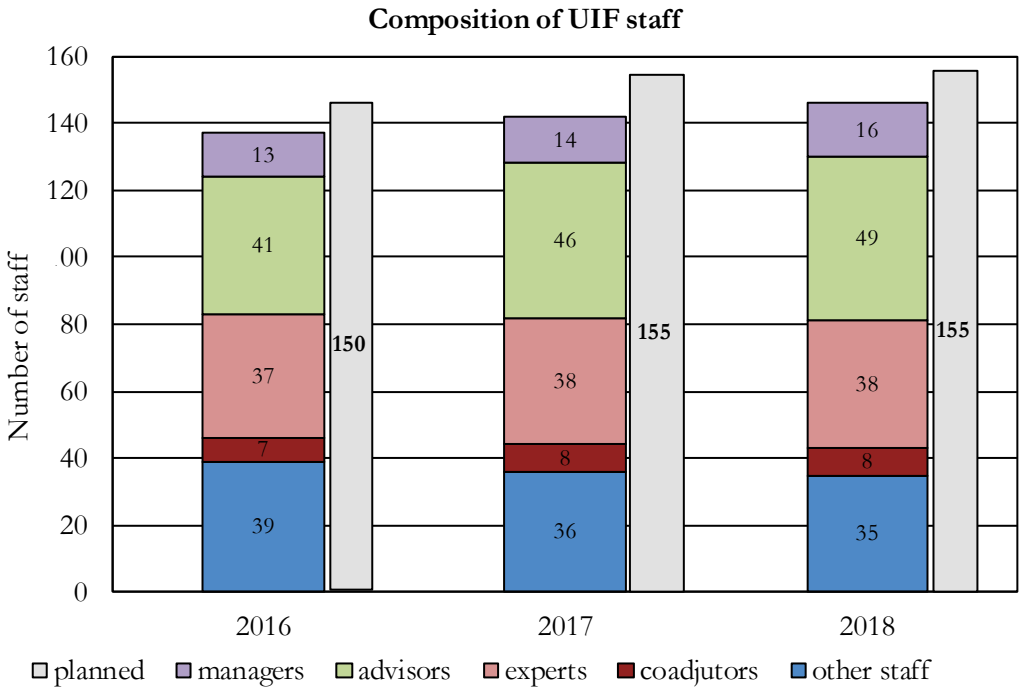
Strategic objectives of the UIF and results achieved



10.3. Human resources

In 2018, the number of UIF staff members increased from 142 to 146, following the exit of six units and the addition of ten members, of which four new hires and six from other Bank of Italy areas through internal mobility procedures (Figure 10.3). Nonetheless, the number of staff is still below the planned number of 155. As at 31 December, 88 members of staff were assigned to the Suspicious Transactions Directorate while 54 were assigned to the Analysis and Institutional Relations Directorate.

Figure 10.3



The growth in the number of STRs received, the new tasks relating to threshold-based communications, increased regulatory competences, the objectives of stepping up activities to counter terrorism and preside over certain special sectors (money transfers, payment cards, gaming services and FinTech services) and the strengthening of cooperation and scrutiny all required a reform of how the UIF's work is organized that, together with the increase in the dedicated human resources, could properly address the new commitments. The reform will be implemented at the end of 2019 and includes: (i) the establishment of a third Division for analysing reports alongside the two existing ones, as a means to improve supervision of the activities and balance the workload distribution; (ii) the creation of a new Division for special sectors and for combating the financing of terrorism, which will also work on the analysis of money transfer reports and those linked to payment cards and gaming services that, where transactions are split up, require specific analysis techniques; (iii) the allocation of threshold-based communications to the information management Division; and (iv) the creation of a specific division for the examination of irregularities and the planning, support for and co-ordination of inspections.

These organizational changes are accompanied by a significant commitment to the professional training of staff, both through the organization of internal seminars (9 in 2018) and participation in external training on specific topics of interest to the Unit (20 courses and 24 enrolments of UIF staff), such as cybercrime, the use of big data and the potential of machine learning for analysis and study. Remote initiatives have been taken, in particular on FinTech and the relationships between crime and political power. Participation in in-house training activities at the Bank of Italy or the ESCB (74 courses and 133 participations) has also led to the professional growth of the Unit's staff.

10.4. IT Resources

In 2018, work relating to the evolution of the Unit's IT infrastructure continued in three key areas: raising safety and security standards, enriching the information available, and increasing efficiency through the automation, digitalization and integration of the analysis processes.

A number of steps have been taken to further strengthen security and the mechanisms for traceability available to the Unit's management. In October 2018, the new two-factor authentication mechanism[59] (strong authentication) was made available on the UIF's Infostat portal, while the technological update of the portal interface was launched and completed at the end of 2018.

Information exchanges

A new version of the SAFE application has been issued, which makes electronic channels available for information exchanges with judicial authorities, investigative bodies and foreign FIUs. Internal working processes have been refined and additional monitoring functions have been introduced, leading to an enhanced quality of data through new controls.

Threshold-based communications

An IT system for collecting data on threshold-based communications is being developed (see the box 'Instructions for threshold-based communications' in Chapter 9), which will deal, at least initially, with cash transactions for amounts above a certain threshold.

Return data flows

A project has been launched to automate the process of transmitting information flows to the reporting entities. The first phase of the project focused on creating functions for automatically forwarding the list of STRs that do not have sufficient elements to support suspicions of money laundering or the financing of terrorism (negative results). The next phases of this project will focus on the automatic forwarding of other kinds of communications, such as information on the reports for which the analyses yielded positive results, as well as feedback forms (see the section 'The quality of active collaboration' in Chapter 1).

Exchange of confidential information

Another project aims to increase the security safeguards for the information flows exchanged between the UIF and obliged entities. The first phase of the project will make it possible to channel information requests and their responses through the platform used by reporting entities to send STRs. The second phase, to be launched in the second half of 2019, will focus on defining a new layout allowing data to be exchanged in a structured format. To this end, cooperation began with the Revenue Agency to assess the use of a data scheme derived from that currently used in the context of financial investigations.

[59] To access the portal, the user must provide, in addition to a user name and a password, a One-Time Password (OTP) received by SMS on a specifically communicated mobile phone number.

Automatic classification of reports

The project for using machine learning and deep learning algorithms continued, which are designed to construct forecasting models capable of making choices based on the data and not on static IT instructions. It was launched by the UIF together with the Bank of Italy's IT Directorate General.

Management of the reporting entities' registry

Work is under way to finish a project to improve the management features of the reporting entities' registry to make it easier to update some important information for data flow exchanges (for example, those referring to the delegate for suspicious transactions). The project aims to find solutions that apply to all the UIF application users that already use that registry (RADAR, SARA and ORO). It also seeks to manage events that influence the reporting entity's history (e.g. mergers, takeovers and closures) and are useful for processing reports properly.

Improving personal data matching

The personal data matching of names found in the various databases used by the UIF has been improved. To this end, a study of a more advanced system for comparing names has also been launched, aimed at improving the processing of the names of foreign persons with specific characteristics with respect to western ones,[60] and more generally the ability of the Unit to link different operational contexts by identifying recurrent entities in the registry.

Cards, games and exchangers

At the end of 2018, a project was launched to create new ways for operators in the payment card and gaming sectors to send reports. The objective of the project is to acquire the information details of the reports by means of a new standardized data plot that the reporting entities in the relevant sectors will be able to use to send STRs more easily using the data entry mode. In light of the amendments to Legislative Decree 231/2007, which included exchangers of virtual currencies from/to currencies that are legal tender (exchangers) on the list of obliged entities, an extension of the data plot to allow new virtual currency operators to use it has also been examined.

Information exchanges with the DNA

Following the information exchange between the Unit and the DNA, the automation of the process of producing of and sending information to DNA is under way, as well as the gradual integration of the information flows returned by the DNA via the Unit's analysis platform (see the box 'Cooperation with the DNA' in Chapter 7).

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 *Unit's website*.

The *Hearing of the Director of the UIF* at the 6th Finance and Treasury Commission of the Senate of the Republic of the 18th legislature, held in September 2018, was an important opportunity to reaffirm accountability as an inherent component of the Unit's work and as a responsibility towards the general public.

[60] For example, Arabic and Chinese names, which require different matching criteria from those traditionally used.

The UIF's website, the layout of which was recently completely overhauled, explains the changes that have taken place, alongside a description of the work carried out and an overview of the overall Italian and international anti-money laundering and counter-terrorism system, with comprehensive and up-to-date information on regulatory and institutional aspects, initiatives and further research. In January 2019, the first issue of the *UIF Newsletter* was published, with a preview of the statistics for the second semester of 2018, of the 'Quaderni dell'antiriciclaggio – Dati statistici' and other information on the prevention of money laundering and the financing of terrorism. The second issue included the workshop on 'Quantitative methods and measures to combat economic crime', organized by the Baffi Centre, Bocconi University and the UIF in March 2019. The April edition presented the forthcoming threshold-based communications and in May, the Unit explained its activities in the field of virtual assets.

The Unit continues to encourage and foster dialogue and meetings with representatives and members of the main categories of reporting entities. The objective is to raise awareness of the purposes and uses of the various types of reports received. This is done by providing feedback (see the section 'The quality of the active cooperation' in Chapter 1), which is also useful for comparing contexts and best practices at the system level, and by facilitating the establishment of a more intensive dialogue to improve the standards of active cooperation.

This area also includes the initiatives for publication promoted by the UIF and the participation of members of the Unit in studying and extending the law and scenarios for combating economic crime in its various forms.

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', which are printed and also published on the Unit's website. The first series is issued every six months and contains statistics on reports received and 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. *Quaderno No. 9* 'Le linee di intervento della nuova regolamentazione antiriciclaggio nel settore del gioco' (only available in Italian) was published in the second series in January 2018, followed in June 2018, by *Quaderno No. 10* 'Come le statistiche bilaterali sul commercio estero possono aiutare a individuare i flussi finanziari illegali' (Magic mirror in my hand…How trade mirror statistics can help us detect illegal financial flows). In July 2018, *Quaderno No. 11* 'Casistiche di riciclaggio e di finanziamento del terrorismo' (only available in Italian) was published and *Quaderno No. 12* 'L'impatto delle ispezioni antiriciclaggio sulle segnalazioni di operazioni sospette delle banche: analisi empirica del caso italiano' (The impact of anti-money laundering oversight on banks' suspicious transaction reporting: evidence from Italy) in July 2019. Lastly, a study that had already appeared in this series was published in the International Review of Law and Economics (see the section 'Analysis of aggregated data and study activities' in Chapter 6).

In 2018, the FIU took part in conferences, seminars and meetings to increase awareness and understanding among the public and various types of operators, and to work further with other authorities on the topics of money laundering and the financing of terrorism. In particular, the UIF sent speakers to around 60 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 Scuola Superiore della Magistratura, the school for training officials at the Presidency of the Council of Ministers, the Istituto Superiore dei Carabinieri, 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 Tax Investigation School (for internal staff and foreign officials) and at the Naples Public Prosecutor's Office; cooperation continued with the universities as well, especially with La Sapienza University of Rome. Training initiatives were then launched, involving associations of professionals and representatives of local authorities (municipalities and regions).

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, licensees or other permits, of any kind, 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 Public Statement February 2019* and *Improving Global AML/CFT compliance: Ongoing process February 2019*), the following countries are not aligned with the legislation for combating anti-money laundering and terrorist financing: the Bahamas, Botswana, Cambodia, the Democratic Republic of Korea, Ethiopia, Ghana, Iran, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia and Yemen.

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.

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 Customs 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 weapons 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 programmes

Under Article 1(1)(e) of Legislative Decree 109/2007, the financing of weapons of mass destruction 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.

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 has taken up 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.

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 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); 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' can 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 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, and transferred, stored and traded electronically.

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 in 'fiat' currencies.

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
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