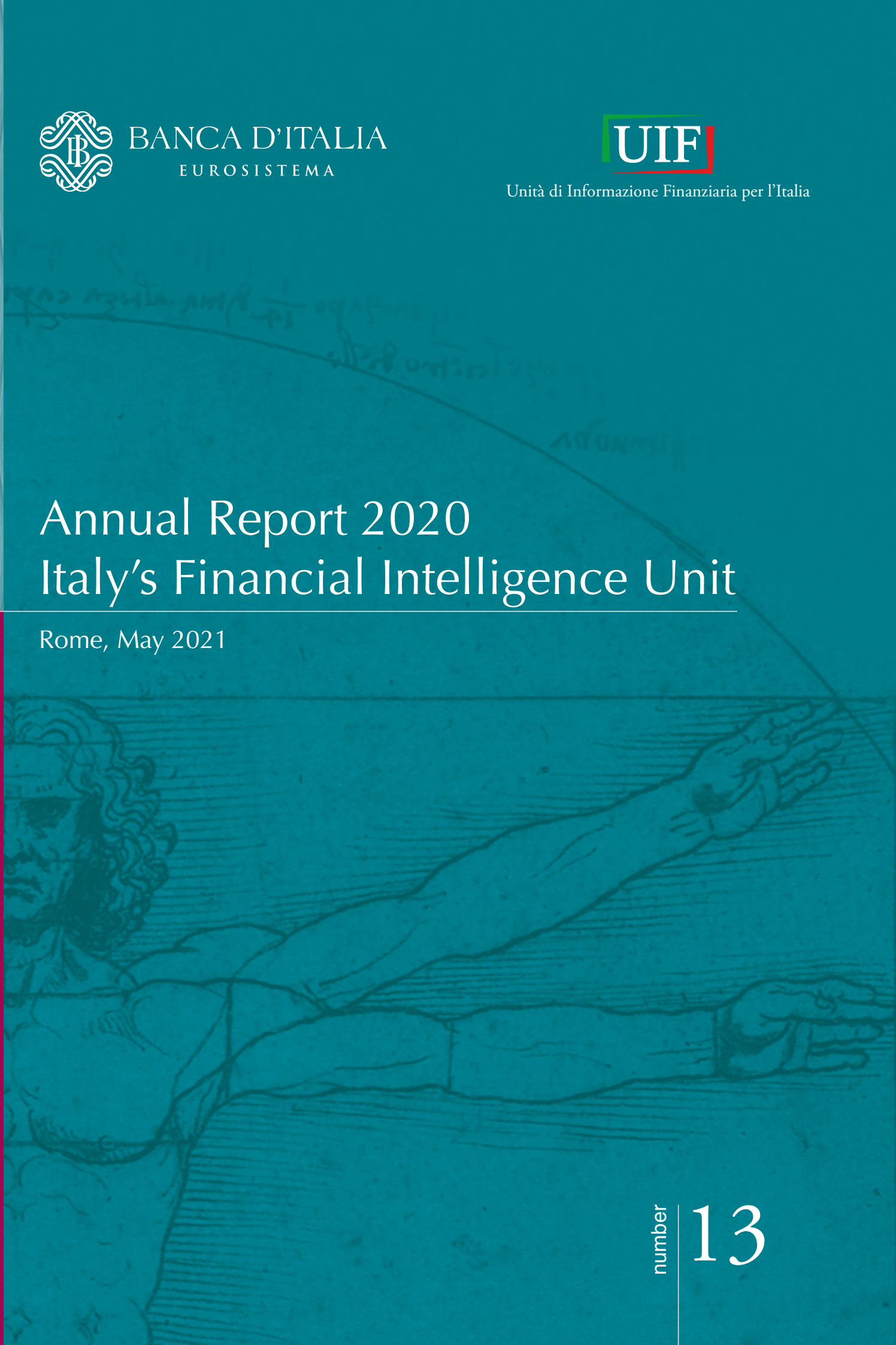
BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2020
Italy's Financial Intelligence Unit

Rome, May 2021



year 2020

number 13

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2020
Italy's Financial Intelligence Unit

Rome, May 2021

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

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

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

Bank of Italy, 2021

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

The year covered by this Report, 2020, was the year of the COVID-19 pandemic that disrupted lives, social dynamics and economies.

In a rapidly changing environment that created new opportunities for illegal activity, facilitated by social distancing and the state of emergency, the system for countering money laundering demonstrated its capacity for response and its organizational and operative flexibility. Working procedures and modes of interaction between the system's private and public components, and also between the UIF and the other competent authorities, necessarily had to change, but their efficacy of action remained unaltered and even increased.

Especially in the first months of the pandemic, the Unit helped obliged entities to fulfil their obligations to send suspicious transactions reports, SARA aggregate data and threshold-based communications, offering enhanced technical and methodological support.

The system did not fail to respond. In 2020, the number of STRs received again increased significantly, to over 113,000, of which 2,300 relating to risk contexts bound up with the health emergency. During the year, the Unit received threshold-based communications on 41 million transactions involving €215 billion worth of significant cash deposits and withdrawals, with a diminution in the average monthly amount compared with 2019 due to the pandemic's impact on behaviours and economic developments.

The principal contribution to the further growth in the number of STRs received came from banking and financial intermediaries, more highly structured and less severely affected than other reporting entities by the slump in economic activity or by operating difficulties. Most of the categories of professionals and non-financial operators, by contrast, sent fewer reports, even though the number of such entities registered with the STR reporting system increased.

The UIF continued its efforts to assist the obliged entities in improving their contribution and to monitor the quality of their reports, in order to avert the risk of a deterioration due to reliance on mere automatic reporting mechanisms or a strictly precautionary approach, also on the part of major intermediaries. The Unit launched a project to ease the reporting burden on operators in the payment card and gaming sectors, whose activity is characterized by very large numbers of customers, transactions and accounts.

To foster prompt and efficacious detection of criminal activities in connection with the health emergency, the Unit issued two Communications calling the reporting entities' attention to the main areas of risk and to some specific anomalies.

Contacts with general government entities were stepped up in the search for synergies to enable analysis to benefit from that sector's contribution of information, which is especially important during the current emergency in light of the risks connected with economic support programmes.

Again in 2020, the number of suspicious transaction reports analysed was slightly greater than that of those received in the same timeframe, confirming the Unit's ability to cope with the steady increase in the reporting flow in recent years and to continue shortening average processing times.

The persistence of the pandemic meant fewer inspections and prompted the adoption of new, alternative methods of control and of innovative procedures for interacting with the entities subject to the requirement of active cooperation.

The Unit reinforced its cooperation with the DNA, the Finance Police and the DIA by instituting weekly exchanges on the financial transactions relating to the COVID-19 emergency reported in cross-border STRs and spontaneous communications of foreign FIUs. The new memorandum of understanding signed with the DNA in early 2021 has further improved and automated the information sharing process, increasing the frequency of exchanges and their information content. There was a sharp increase in cooperation with the judicial authorities, whose requests rose by over 40 per cent compared with 2019.

Strategic analysis, ordinarily focused on the development of indicators of the risk of the infiltration of enterprises by organized crime, has now also been directed to picking up the signs of how this has been influenced by the pandemic.

More and more frequently, international cooperation has been activated in order to acquire from foreign FIUs elements pertinent to investigations of suspicious cross-border financial flows. The cooperation with other FIUs made it possible to detect suspicious cross-border transactions aimed at taking advantage of the health emergency and economic relief measures. There was an increment in information exchanges about on-line scams, favoured by the greater use of the Internet that has marked the pandemic period. Thanks to this cooperation, fraudulent transfers were traced and in some cases, the assets identified were promptly frozen, making their recovery possible.

The emergency has produced a sharp acceleration in the plan for reform of the European AML system. The Commission's Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing reaffirms the need for a European Support and Coordination Mechanism for FIUs. On the basis of the work of the UIF together with the Ministry of Economy and Finance, Italy has promoted a Common Position of EU Member States on the tasks and characteristics of the nascent Mechanism, in accordance with the subsidiarity principle and focusing on working methods and practices, international cooperation, and analyses that cannot be performed effectively at national level.

How long it will take for economic activity to recover, once the emergency has been overcome, is uncertain. The efforts to address the weaknesses that have pervaded the economy and society must be redoubled. It is essential that the recovery in demand and output not open up new avenues for criminal penetration of the country's economic and social life.

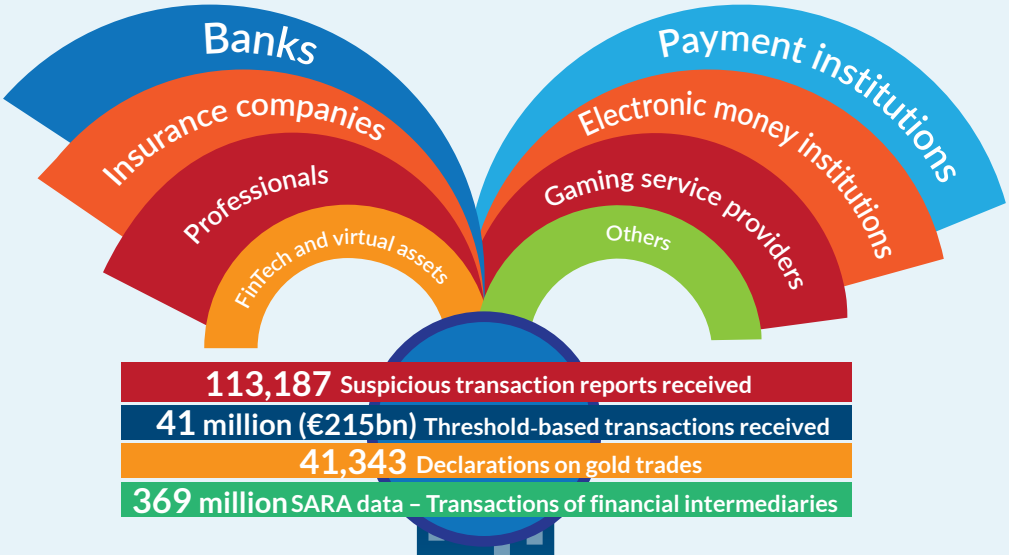
The challenges of this difficult historical period require stronger and more coordinated action. In combating money laundering, as in other areas, full advantage must be taken of the network of cooperation, the more effectively to prevent and counter the emerging risks. The UIF stands ready to make its contribution, marshalling its staff's resources of expertise, public spirit and flexibility.

The Director

Claudio Clemente

ACTIVITY AT A GLANCE

Financial analysis



113,187 Suspicious transaction reports received

41 million (€215bn) Threshold-based transactions received

41,343 Declarations on gold trades

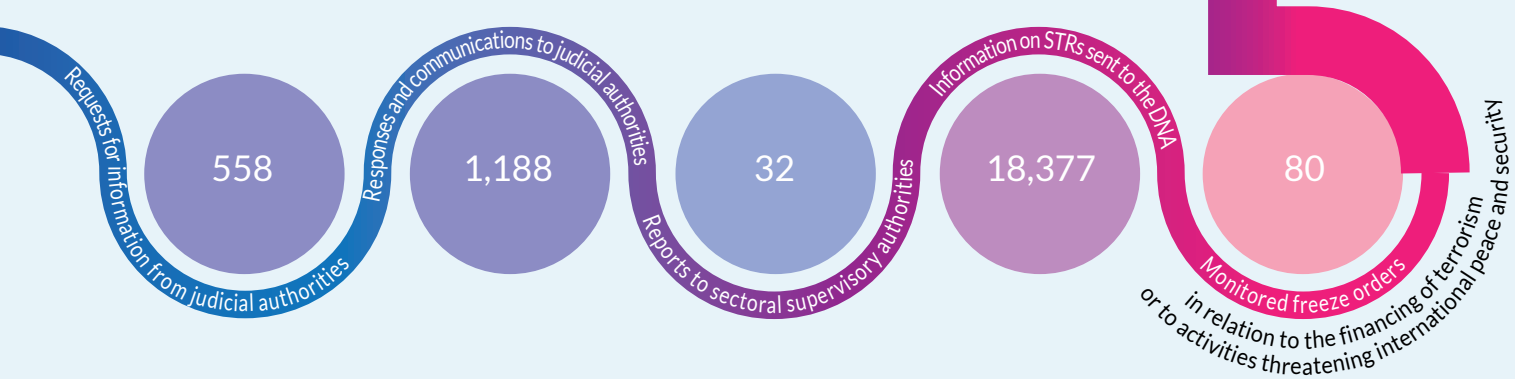
369 million SARA data – Transactions of financial intermediaries

Intelligence, dissemination and controls

UIF

- 113,643 Suspicious transaction reports analysed
- 32,055 STRs on payment card, gaming and money transfer transactions assessed using aggregate analysis
- 308 Suspicious transactions examined with a view to suspension
- 37 Suspension orders
- 3 Inspections
- 26 Sanction procedures

Cooperation with investigative bodies and national authorities



FOREIGN FIUs

1,546
Requests and spontaneous communication received

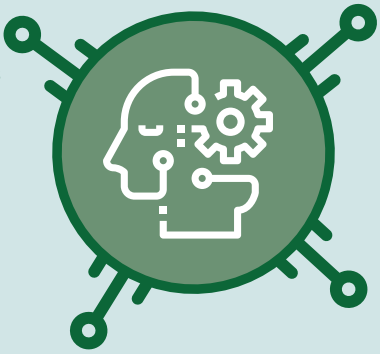
84
Exchanges on possible freezing of funds

1,050
Requests sent to other FIUs

3,296
Communications of foreign FIUs sent to investigative bodies

DISSEMINATION

of knowledge about money laundering



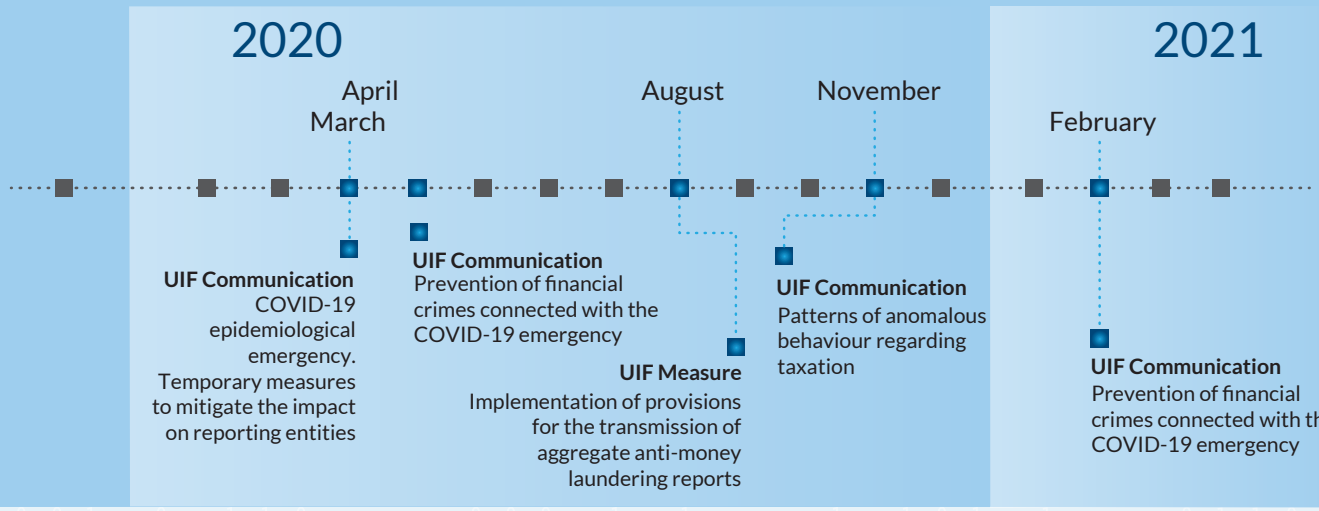
10
Speakers at international conferences and workshops

48
Speakers at conferences and workshops held by Italian institutions

17
Training interventions at regional bodies and other general government offices

9
Publications in *Quaderni dell'antiriciclaggio* and in scholarly journals

Secondary legislation and UIF communications



IT Infrastructure

Further controls on incoming STRs and introduction of non-blocking observations

Automatic transmission of feedback reports to major reporting entities

Identification and transmission of cross-border reports to European FIUs

Development and expansion of **data exchanges with the DNA**

Introduction of additional controls on the quality of aggregate AML reports and gold declarations

1. ACTIVE COOPERATION

The Unit is the institution appointed to receive suspicious transaction reports (STRs). These concern transactions which financial intermediaries, professionals and other qualified operators suspect may involve money laundering, financing of terrorism or financing of the proliferation of weapons of mass destruction, which they must identify, evaluate and promptly notify to the Unit in fulfilment of the requirement of active cooperation.

Centralizing the flow of reports at the Unit permits a homogeneous and integrated assessment that can pick up subjective and objective links, trace financial flows even beyond the nation's borders, with the contribution of information exchanged with the network of foreign FIUs, and identify innovative money laundering techniques and cases presenting high levels of risk.

The Unit sends the results of its analyses to the Special Foreign Exchange Unit of the Finance Police (NSPV) and the Anti-Mafia Investigation Department (DIA) for further investigation. It also sends reports and analyses to the judicial authorities in the event that information regarding crimes is found or upon their request. Where significant, the results of analyses may be transmitted to the supervisory authorities. The UIF sends data and information to the National Anti-Mafia Directorate (DNA) in order to check for possible links to criminal contexts and enable prompt action.

The body of information acquired is also used to develop anomaly indicators and identify patterns of anomalous behaviour serving to guide reporting entities and enhance their ability to detect suspicious transactions.

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

1.1. Reporting flows

In 2020, the Unit received 113,187 suspicious transaction reports, 7,398 more than in the previous year (+7.0 per cent; Table 1.1).[1]

Table 1.1

Reports received

	2016	2017	2018	2019	2020
Number of reports	101,065	93,820	98,030	105,789	113,187
Percentage change on previous year	*22.6*	*-7.2*	*4.5*	*7.9*	*7.0*

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

The increase compared with 2019 came chiefly from the growth in reports transmitted by banks and Poste Italiane SpA (+11.2 per cent) and in those received from intermediaries and other financial operators (+8.5 per cent), which more than offset the declines of 28.1, 10.8 and 14.4 per cent, respectively, in STRs from professionals, gaming service providers and non-financial operators (Table 1.2).

The share of reports transmitted by banks and Poste Italiane SpA rose to 67.0 per cent, from 64.5 per cent in 2019. Non-bank financial intermediaries ranked second among reporting entities by number of STRs filed, their share of the total edging up to 23.6 per cent.

The number of communications received from general government entities was again very small, and most of them (24) were submitted by public sector companies.[2] At local level, the contribution provided by chambers of commerce and by municipalities, with 5 and 4 communications respectively, is to be noted.

Table 1.2

STRs by type of reporting entity

	2019		2020		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2019)*
Total	**105,789**	**100.0**	**113,187**	**100.0**	**7.0**
Banks and Poste Italiane SpA	68,236	64.5	75,852	67.0	11.2
Non-bank financial intermediaries	24,648	23.3	26,735	23.6	8.5
Companies managing markets and financial instruments	11	0.0	17	0.0	54.5
Professionals	5,074	4.8	3,648	3.2	-28.1
Non-financial operators	1,303	1.2	1,116	1.0	-14.4
Gaming service providers	6,470	6.1	5,772	5.1	-10.8
General government entities	47	0.0	47	0.0	0.0

Financial intermediaries other than banks

In the non-bank financial sector, the number of reports by insurance companies continued to trend upwards (+23.8 per cent). The increase in STRs by electronic money institutions (+17.5 per cent, from 9,227 to 10,840; Table 1.3) was due to a sharp increase in the contribution of one reporting entity and, in part, to a corporate action carried out by a payment institution which gained the status of electronic money institution in the second half of 2020.

Despite this change, the number of reports received from payment institutions and from points of contact of EU payment institutions was about the same, as a result of the 0.3 per cent increase in those from other reporting entities (from 10,399 to 10,427). Among payment institutions and their points of contact, the flow of reports from money transfer agents, which had contracted in 2019, expanded to make up 89.4 per cent of the category's total, compared with 84.1 per cent in 2019. By contrast, the flow of reports from trust companies

[2] See 'Istruzioni sulle comunicazioni delle Pubbliche amministrazioni' (only in Italian), published by the UIF in 2018.

under Article 106 of the Consolidated Law on Banking fell by 49.6 per cent, from 546 to 275), with trust companies belonging to banking groups submitting more STRs than stand-alone operators (186 against 89).

Table 1.3

STRs by category of banking and financial intermediary

	2019		2020		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2019)*
Banks, intermediaries and other financial operators	**92,884**	**100.0**	**102,587**	**100.0**	**10.4**
Banks and Poste Italiane SpA	**68,236**	**73.5**	**75,852**	**73.9**	**11.2**
Non-bank financial intermediaries	**24,648**	**26.5**	**26,735**	**26.1**	**8.5**
Payment institutions and points of contact of EU payment institutions	10,399	11.2	10,427	10.2	0.3
Insurance companies	2,745	3.0	3,397	3.3	23.8
Electronic money institutions and points of contact of EU electronic money institutions	9,227	9.9	10,840	10.6	17.5
Trust companies - Article 106 of the Consolidated Law on Banking	546	0.6	275	0.3	-49.6
Financial intermediaries - Article 106 of the Consolidated Law on Banking	959	1.0	1,167	1.1	21.7
Asset management companies, SICAVs and SICAFs	448	0.5	368	0.4	-17.9
Investment firms	58	0.1	34	0.0	-41.4
Intermediaries and other financial operators not specified above(1)	266	0.3	227	0.2	-14.7

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

The effects of the COVID-19 pandemic on economic activity probably caused the 29.1 per cent drop in STRs received from professionals, and particularly from notaries, accountants and lawyers. The number of reports filed by law firms, law and accounting firms and law practices declined again, falling from 18 to 10 (Table 1.4). The overall decrease in reporting by professionals contrasts with the trend for the banking and financial sector and warrants careful consideration, given the crucial role that professionals are called on to play, in the current emergency situation, to safeguard the effectiveness of public measures in support of individuals and firms in difficulty.

The National Council of Notaries is by now practically the sole reporting channel for STRs by notaries (98.5 per cent of the total). Likewise, the National Council of the Order of Accountants and Bookkeepers transmitted most of the much smaller flow of reports by members of those professions (77.6 per cent).

The number of STRs sent by non-financial operators also contracted (down by 14.4 per cent, from 1,303 to 1,116) following the decline in those submitted by cash/valuables-in-

transit companies (down by 53.6 per cent, from 686 to 318). Although the number remained marginal, there was a marked increase, from 20 to 168, in reports coming from virtual asset service providers (entirely from virtual currency exchangers).

Table 1.4

STRs received from professionals and non-financial operators

	2019		2020		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2019)*
Non-financial obliged entities	**12,847**	**100.0**	**10,536**	**100.0**	**-18.0**
Professionals	**5,074**	**39.5**	**3,648**	**34.6**	**-28.1**
Notaries and National Council of Notaries	4,630	36.0	3,329	31.6	-28.1
Law firms, law and accounting firms and law practices	18	0.1	10	0.1	-44.4
Accountants, bookkeepers and employment consultants	327	2.5	223	2.1	-31.8
Lawyers	48	0.4	29	0.3	-39.6
Auditing firms and auditors	30	0.2	35	03	16.7
Other professional services providers (1)	21	0.2	22	0.2	4.8
Non-financial operators	**1,303**	**10.1**	**1,116**	**10.6**	**-14.4**
Gold traders and manufacturers and traders of precious stones and metals	536	4.2	533	5.1	-0.6
Cash/valuables-in-transit companies	686	5.3	318	3.0	-53.6
Virtual asset service providers (2)	20	0.2	168	1.6	740.0
Other non-financial operators (3)	61	0.5	97	0.9	59.0
Gaming service providers	**6,470**	**50.4**	**5,772**	**54.8**	**-10.8**

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

After growing by 27.7 per cent in 2019, the number of STRs sent by gaming service providers fell by 10.8 per cent, from 6,470 to 5,772. The reversal of trend is ascribable to the restrictive measures put in place to deal with the pandemic. In fact, the decline concerned STRs from physical network operators (down by 47.4 per cent, from 4,330 to 2,278) and casinos (down 58.8 per cent, from 68 to 28), while those received from online gaming operators rose by 67.3%, from 2,072 to 3,466.

STRs in the first five months of 2021

The growth in the number of suspicious transactions reported has intensified in 2021. In the first five months, the UIF received 58,586 reports, 30.8 per cent more than in the same period of 2020. The number of STRs transmitted to investigative bodies rose by 24.3 per cent.

New reporting entities

The number of reporting entities also continued to grow in 2020, rising to 7,167 thanks

to 459 new registrations (against 503 in 2019). In the course of the year, 14.8 per cent of newly registered entities sent at least one report, down from 22.7 per cent in 2019. The overall contribution of newly registered entities to the flow of reports for the year diminished, from 1,460 STRs to 864. The decrease is largely ascribable to newly registered electronic money institutions and their points of contact, which sent 589 STRs, and to newly registered EU payment institutions and the related contact points, which sent 162.

The largest share of new registrations for the year again came from professionals (292), mainly accountants, bookkeepers and employment consultants (189) and lawyers (34). There was also a significant number of new registrations among investment firms, asset management companies, SICAVs and SICAFs (37). The ranks of virtual asset service providers expanded with the addition of 4 virtual currency exchangers. Finally, there was a further rise in the number of general government entities registered in order to comply with the communication requirements of Article 10(4) of Legislative Decree 231/2007, although this was not accompanied by an increase in communications: with 23 new registrations, the number of communications received by the Unit remained unchanged at 47.

Initiatives vis-à-vis the general government sector

Contacts between the Unit and general government entities proceeded in 2020 in pursuit of synergies so that analysis can benefit from the information contribution of the public sector. That contribution is deemed even more valuable in the current emergency situation, given the risks associated with the measures to support the economy.

Contacts were undertaken with the Municipality of Rome with a view to obtaining information regarding the ownership of commercial establishments and the changes therein over time. The availability of such data is fundamental for establishing a method of analysis aimed at intercepting possible criminal infiltrations of businesses at local level.

In addition, the Unit engaged in exchanges with the municipal governments of Milan, Florence and Ragusa and with regional control bodies to detect risks of misappropriation of public funds and share this information, in the context of active cooperation against money laundering (see Chapter 7, 'Cooperation with other authorities').

The UIF and Cassa Depositi e Prestiti (CDP) initialed a memorandum of understanding to facilitate active cooperation by CDP in connection with its management of the so-called 'Patrimonio Rilancio' vehicle.[3] The memorandum will allow the UIF to acquire data on the interventions requested (names of the applicants, outcomes of the application examination procedures, etc.). At the same time, at-risk behaviour profiles will be developed to assist the transmission of suspicious transaction reports concerning both the examination phase and the implementation and monitoring of interventions (see Section 9.2.1, 'Legislative measures').

Together with the National Social Security Institute (INPS), the Unit launched an initiative to identify possible cases related to the Institute's activity that might be anomalous and warrant evaluation for suspicious transaction reporting purposes.

Training to assist general government entities in preventing money laundering continued. Following the measures taken to combat the pandemic, the Unit conducted its

[3] Although CDP does not fall within the perimeter of general government, Decree Law 34/2020 designated it as manager of the public subsidies to support the Italian economy during the COVID-19 emergency ('Patrimonio Rilancio').

training initiatives using remote procedures. This enabled it to augment its training activity and, by recording the training events, to reach a wider array of general government entities. Training again proved to be an essential part of AML awareness-raising, not least through thematic working groups capable of bringing out problematic aspects.

General government entities expressed a need to have more definite, precise indications for more effective implementation of AML controls and in particular the role of the AML manager.

It also emerged that even when the main preparatory steps for the launch of active cooperation have been completed, it often proves complicated for the offices to identify the elements of anomaly capable of triggering the reporting flow. This difficulty has to be overcome through the creation of training programmes by the responsible general government entities, as envisaged by the AML legislation.

The difficulties in implementing anti-money laundering controls and active cooperation are at the root of the need expressed by AML mangers to have opportunities for networking in order to share the good practices put in place by the offices that have initiated active cooperation most fruitfully, to the benefit of those that are encountering greater difficulty. In this perspective, a useful role could be performed by the numerous organizations that bring together the various entities, which could promote collective initiatives.

During 2020, the groundwork was laid for collaboration between the UIF and the National School of Administration. In 2021, this has resulted in an online course designed to stimulate reflection on anti-money laundering issues within general government (see Chapter 7, 'Cooperation with other authorities').

1.2. Suspicious transactions

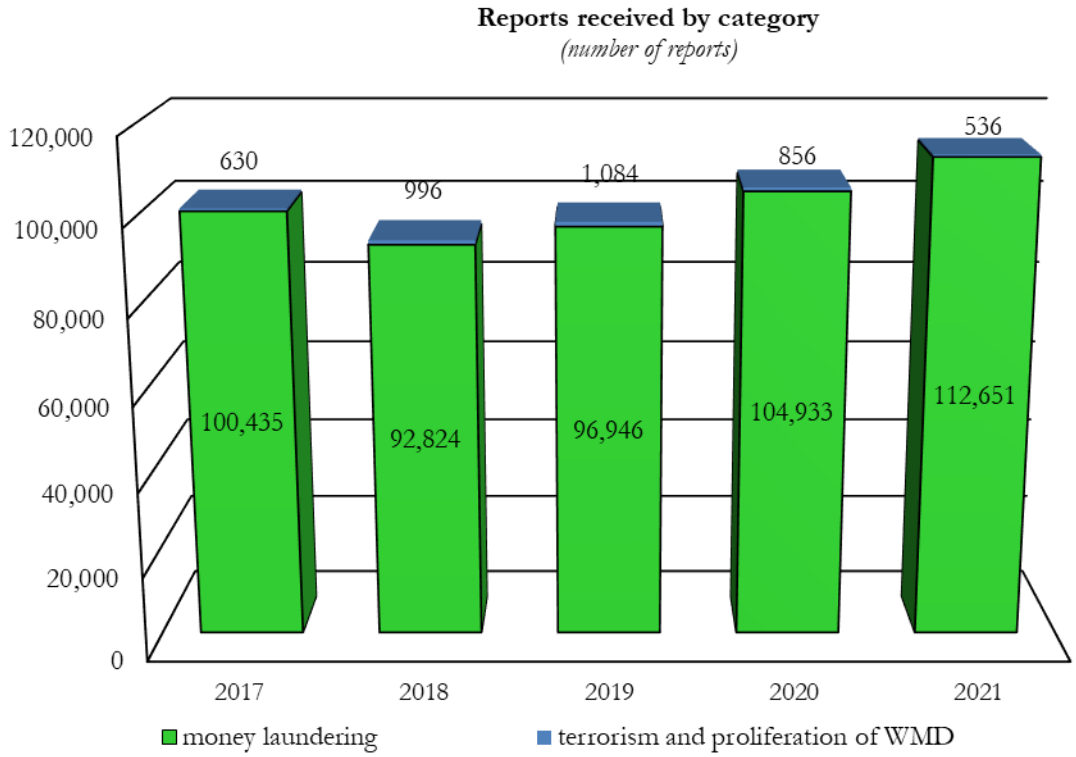
Nearly all of the suspicious transaction reports received in 2020 - 99 per cent of the total - again concerned money laundering. Reports linked to the voluntary disclosure measure dwindled to barely 387, or 0.3 per cent.

The skew in the distribution of STRs was reinforced by the 7.4 per cent increase in the number of reports of suspected money laundering (up from 104,933 to 112,651) and the simultaneous 33.4 per cent decline in those concerning terrorist financing, which fell again to 513 (see Chapter 4, 'Combating the financing of terrorism'). After spiking to 86 in 2019, the number of reports regarding financing of proliferation of weapons of mass destruction fell to a modest 23 (Table 1.5 and Figure 1.1).

Table 1.5

Distribution of STRs by category					
	2016	2017	2018	2019	2020
	(number of reports)				
Total	**101,065**	**93,820**	**98,030**	**105,789**	**113,187**
Money laundering	100,435	92,824	96,946	104,933	112,651
Financing of terrorism	619	981	1,066	770	513
Financing of proliferation of WMD	11	15	18	86	23

Figure 1.1



The distribution of reports by region largely duplicated that of 2019. Despite a 6.2 per cent decrease compared with the previous year, Lombardy was again the leading region for suspicious transactions, accounting for 17.3 per cent of the total reported, followed by Campania (13 per cent) and Lazio (12.7 per cent; Table 1.6). In terms of reports in relation to the resident population, the leading region was Campania, followed by Lazio and Lombardy.

Table 1.6

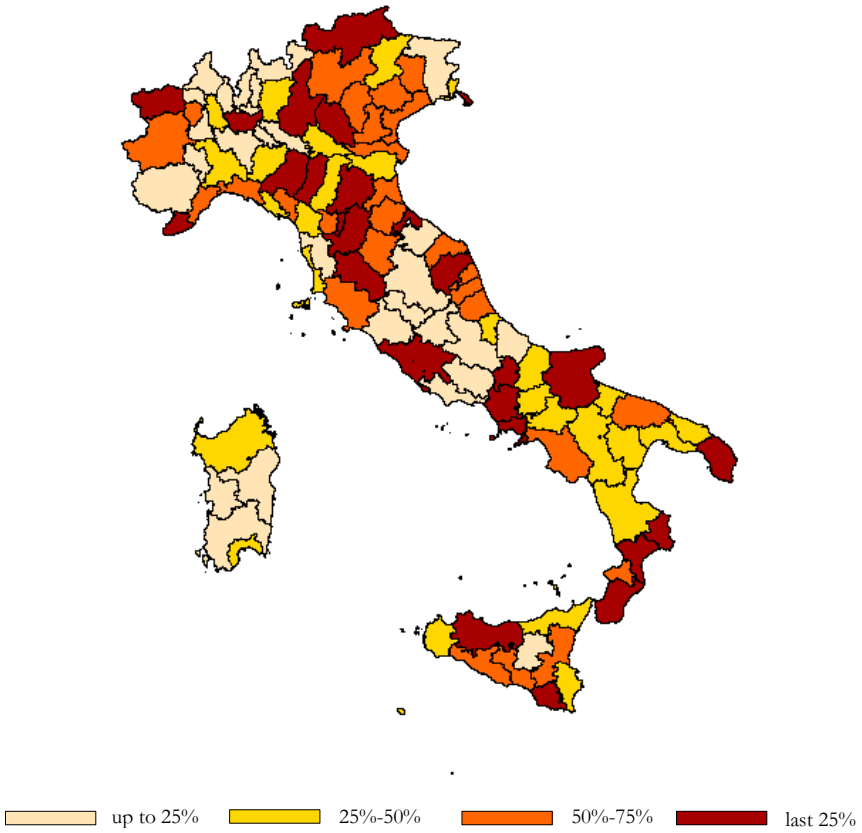
Distribution of STRs received by region of transaction					
	2019		2020		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2019)*
Lombardy	20,937	19.8	19,632	17.3	-6.2
Campania	12,929	12.2	14,715	13.0	13.8
Lazio	10,567	10.0	14,329	12.7	35.6
Veneto	8,791	8.3	8,374	7.4	-4.7
Sicily	7,399	7.0	8,005	7.1	8.2
Emilia-Romagna	7,632	7.2	7,810	6.9	2.3
Puglia	5,705	5.4	6,861	6.1	20.3
Tuscany	6,864	6.5	6,695	5.9	-2.5
Piedmont	6,317	6.0	6,398	5.7	1.3
Calabria	2,812	2.7	3,369	3.0	19.8
Liguria	2,873	2.7	2,574	2.3	-10.4
Marche	2,459	2.3	2,419	2.1	-1.6
Trentino-Alto Adige	1,513	1.4	1,869	1.7	23.5
Friuli Venezia Giulia	1,986	1.9	1,862	1.6	-6.2
Sardinia	1,420	1.3	1,757	1.6	23.7
Abruzzo	1,518	104	1,548	1.4	2.0
Umbria	973	0.9	1,032	0.9	6.1
Basilicata	695	0.7	786	0.7	13.1
Molise	452	0.4	468	0.4	3.5
Valle d'Aosta	198	0.2	229	0.2	15.7
Abroad	1,749	1.7	1,521	1.3	-13.0
Online	-	-	934	0.8	-
Total	**105,789**	**100.0**	**113,187**	**100.0**	**7.0**

Among the regions with the largest rises in the number of STRs, Lazio recorded the steepest increase (+35.6 per cent), followed by Puglia (+20.3 per cent), Calabria (+19.8 per cent) and Campania (+13.8 per cent). Although the numbers of STRs involved were lower, there were also sharp increases in Sardinia (+23.7 per cent), Trentino-Alto Adige (+23.5 per cent) and Basilicata (+13.1 per cent). The provinces of Prato and Milan again ranked first and second, respectively, by number of STRs per 100,000 inhabitants (Figure 1.2). The provinces of Naples, Rome and Caserta also placed high on the list, while Sud Sardegna and Nuoro, with the addition of Viterbo, were again those recording the lowest incidence of STRs, which ranged between 57 and 75 per 100,000 inhabitants.

During 2020, it became possible for reporting entities to mark transactions carried out via the Internet by indicating 'Online' as the place of execution, and 934 STRs were flagged this way.

Figure 1.2

Distribution in quartiles of STRs received per 100,000 inhabitants by province of transaction



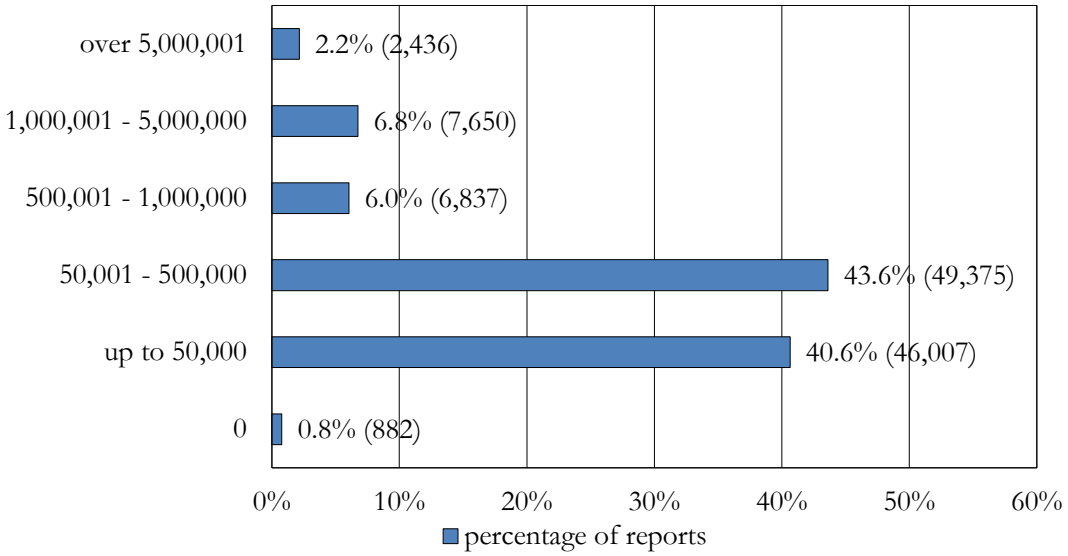
The total value of reported transactions that were actually executed totalled €85 billion, compared with €91 billion the previous year. Taking into account the STRs on transactions attempted but not executed, the total value of the year's reporting flow came to €98 billion, as against €97 billion in 2019, with the value of attempted but unexecuted transactions up from €6 billion to €13 billion. The increase in the latter component mainly reflected attempted fraud related to the COVID-19 emergency (see Chapter 3, 'Risk areas and typologies').

There were no significant changes in the distribution of STRs by transaction amount, with 43.6 per cent (44.4 per cent in 2019) falling in the intermediate range (€50,001 to €500,000; Figure 1.3).

Figure 1.3

Distribution of STRs received by amount

(in euros)



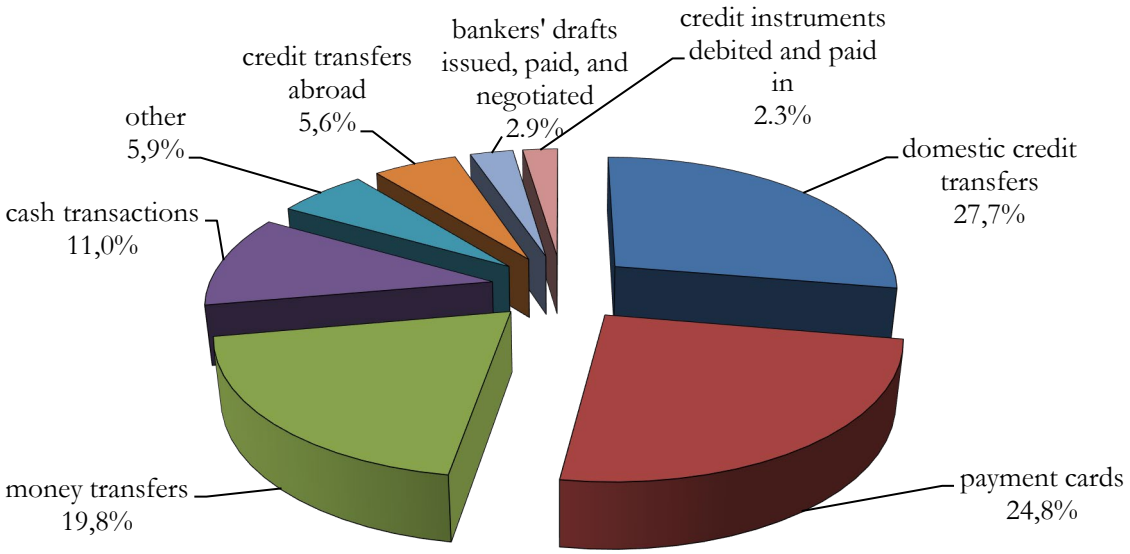
Types of transactions reported

The breakdown by type of transaction reported in 2020 displayed a sharp increase in transactions involving payment cards and electronic money, which accounted for 24.8 per cent of the total. This development was propitiated by the new automated reporting procedure introduced in January, which has afforded a more accurate representation of transactions (see Section 1.3, 'The quality of active cooperation'). Compared with 2019, the share of both domestic and cross-border credit transfers diminished, respectively, from 31.1 to 27.7 and from 7.0 to 5.6 per cent (Figure 1.4).

Figure 1.4

Main types of transactions reported

(per cent of total transactions reported)



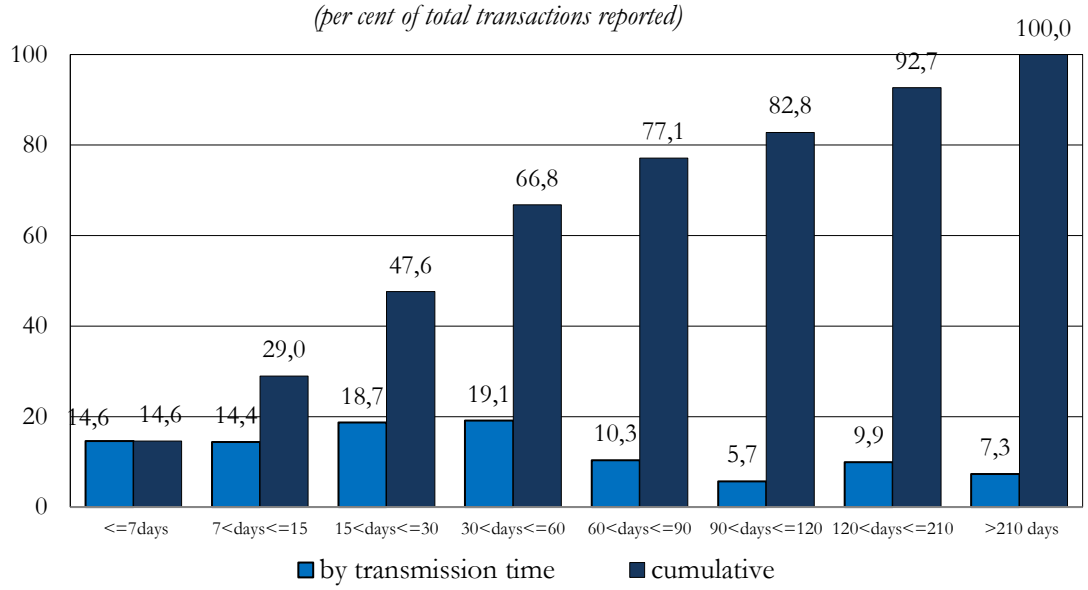
Report transmission times were slightly longer than in the previous year: 47.6 per cent of STRs were received within one month following the transaction (51.2 per cent in 2019), while 66.8 percent were received within two and 77.1 per cent within three months, compared with 71.4 and 79.6 per cent, respectively, in 2019 (Figure 1.5).

Transmission times for STRs

Figure 1.5

Distribution by transmission time of STRs received by the UIF

(per cent of total transactions reported)



The lengthening of transmission times, probably caused by the restrictive measures imposed to deal with the health emergency, mainly concerned banks, professionals and non-financial operators.

1.3. The quality of active cooperation

To raise the level of active cooperation, the Unit supplemented the customary dialogue with reporting entities with new formal controls on the contents of STRs and new functionalities to simplify the depiction of transactions in some sectors (payment cards, gaming and virtual assets).

New controls

The new controls were designed to permit a more accurate depiction of the transactions described in the reports and to improve the quality of the data tranmitted. Especially in the first half of the year, this innovation required intense consultation, which brought to light the need to envisage new specific cases (the insurance, gaming and virtual currency sectors). Reporting behaviour has yet to fully adapt to the new controls. The Unit has taken steps, on one side, to further refine the control logic, and, on the other, to reach out to those reporting entities that are behind in adapting to provisionally non-binding controls.

There was no lack of occasions for pointed discussion with reporting entities in 2020, conducted in various modes (meetings, formal and informal notes). Some of these again concerned the signs of deterioration in the quality of reports, which has called for recurrent follow-up.

For some medium-sized and large reporting entities, the Unit found: reporting flows

motivated chiefly by the fact that customers were under investigation; insufficient grounds for suspicion (e.g., transfers of modest amounts of cash); unsatisfactory response times to the UIF's requests for information. The measures taken succeeded in alleviating some of these problems.

The Unit's dialogue with operators of the payment cards and gaming sectors was directed at improving the completeness and enhancing the quality of reports. To this end, the Unit encouraged more attentive use of the new reporting procedure that allows these operators to use office automation programmes to enter a series of relevant data for the analysis of these types of transactions.

For now, using this report transmission procedure is optional for gaming operators, but it is strongly recommended. The Unit's help desk stands ready to assist operators in the transition to the new reporting procedures.

Feedback reports

The Unit provided the leading banks, Poste Italiane SpA and main money transfer agents with the customary summary feedback reports on their respective reporting activity. As of 2020, the feedback reports for banks and Poste Italiane SpA are transmitted with an automatic procedure and accompanied by a structured attachment for easier uploading to the reporting entities' IT systems.

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

- the extent of the cooperation, measured by the number of reports submitted by the reporting entity in the relevant time period in relation to the total number of reports sent by the reference group. This provides a parameter for quantitative evaluation of the operator's reporting activity;

- timeliness, shown by the percentage distribution of reports by time period and by median transmission time. This allows assessment of the reporting entity's speed of response to emergent suspicious elements;

- quality, measured by indicators that capture the importance of the reports (risk level, results of financial analyses and interest on the part of investigative bodies). This summarizes the ability of the reporting entity to intercept transactions that pose an effective money laundering risk compared with elements of objective risk;

- complexity, measured for reporting entities belonging to the 'banks and Poste' category, gauges the ability to depict suspicious activities adequately, completely and efficaciously. The indicator is based on the number of persons and significant transactions referred to in the reports and on the degree of structuring of the elements provided.

- emergence of anomalies, an indicator calculated for money transfer agents, which measures the ability to identify anomalies in multiple spheres (operations, customers' subjective profiles, conduct of the territorial sales network).

Evaluation of the quality and complexity of STRs controls

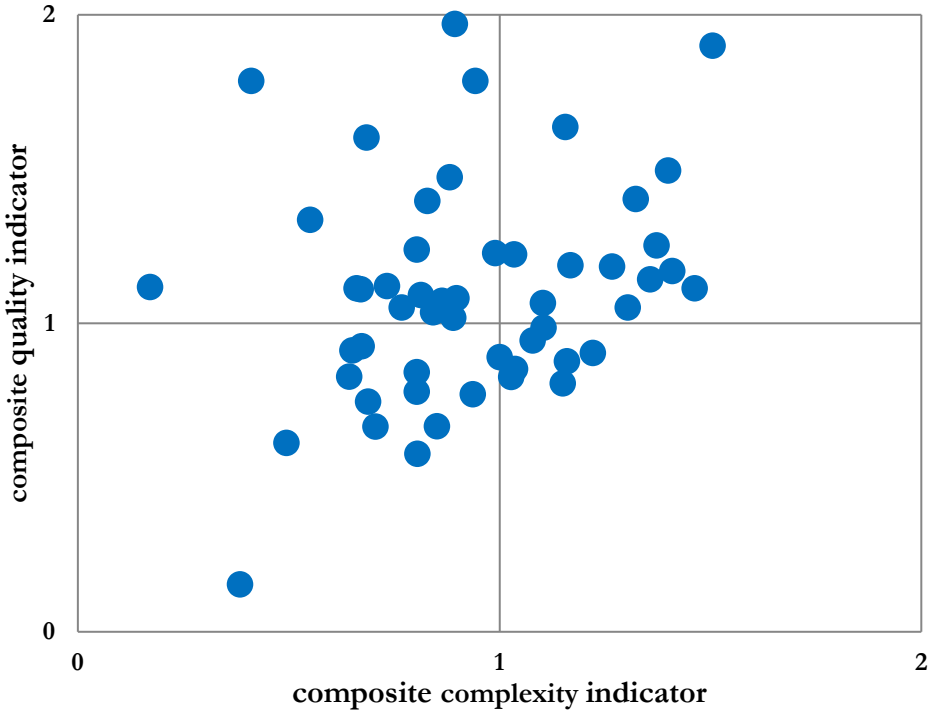
Figure 1.6 shows the positioning of the main reporting entities of the 'banks and Poste' category in the four classes of quality/complexity of active cooperation. Each entity was

compared with the average values for the category. The exercise was performed for 52 entities that sent more than 100 STRs in 2020.

The quality indicators of the reports transmitted by the sample were, on average, in line with the measurements of the previous year, but with less dispersion of the positions with respect to the average values.

Figure 1.6

Scatter graph based on the quality/complexity of the reporting entities in the 'banks and Poste' category that submitted more than 100 reports in 2020 (1)



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

In detail, 18 of the intermediaries scrutinized submitted reports of above-average quality and complexity compared with the benchmark for the group (34.6 per cent of the sample, against 25.0 per cent in 2019). Another 12 operators submitted reports of lower complexity but above-average quality (23.1 per cent. of the sample, against 36.5 per cent in 2019).

The reports of 4 intermediaries were of below-average quality but above-average complexity (7.7 per cent of the sample, against 15.4 per cent in 2019). Another 18 fell in the worst-case group, with reports below average in both quality and complexity (34.6 per cent of the sample, against 23.1 per cent in 2019).

The ever-greater complexity of the data present in suspicious transaction reports and the continual innovation in possible anomalous scenarios spurred the Unit to consider additional profiles of report quality and content adequacy in its evaluations. Specifically, it looked at the diagnostic capacity and diversification of the tools for singling out suspicious contexts in order to detect their different anomalies. The initial results show that STRs not infrequently intercept generic suspicious elements, often indicated by automatically generated

texts, or contexts that have already received attention, rather than the emergence of new possibly anomalous contexts. If this profile is taken into account, the average quality of the reports transmitted by the sample worsens. It is necessary to prompt a refinement of the criteria of selection and assessment of the contexts to be considered suspicious by the reporting entities, so as to enhance the added value of the information contained in STRs.

1.4. Threshold-based communications

Legislative Decree 90/2017 amended Italian AML legislation by introducing the requirement of periodic transmission to the UIF of so-called threshold-based communications containing data and information identified on the basis of objective criteria concerning transactions at high risk of money laundering or terrorist financing.

Such communications enrich the body of information at the Unit's disposal and are used to undertake specific analyses of potentially anomalous financial flows.

The communication requirement, governed by the UIF Measure (only in Italian) of 28 March 2019, applies to banks, Poste Italiane SpA, payment institutions and electronic money institutions (including their EU branches and contact points) and covers all cash transactions of €10,000 or more executed during the calendar month on accounts or by means of occasional operations, via single transactions of at least €1,000. The communications must be transmitted to the UIF monthly through the Infostat-UIF portal by the 15th day of the second month following the reference month.

The UIF's decision to focus on cash reflects the particular risks bound up with the instrument. The ease of use and the untraceability of cash transactions can serve to facilitate money laundering. Italy is among the euro-area countries where cash is most widely used. With the introduction of threshold-based communications, Italy has joined the group of countries that survey cash transactions for the purpose of preventing money laundering.

Quality of threshold-based communications

The Annual Report for 2019 observed that the first months of collection of threshold-based communications had brought to light widespread problems in the ability of the obliged entities to correctly collect data of particular importance for the prevention of money laundering. These problems mainly concerned erroneous communication of virtual cash transactions and failure to communicate cash transactions which showed up, instead, in the suspicious transaction reports transmitted by the same obliged entities.

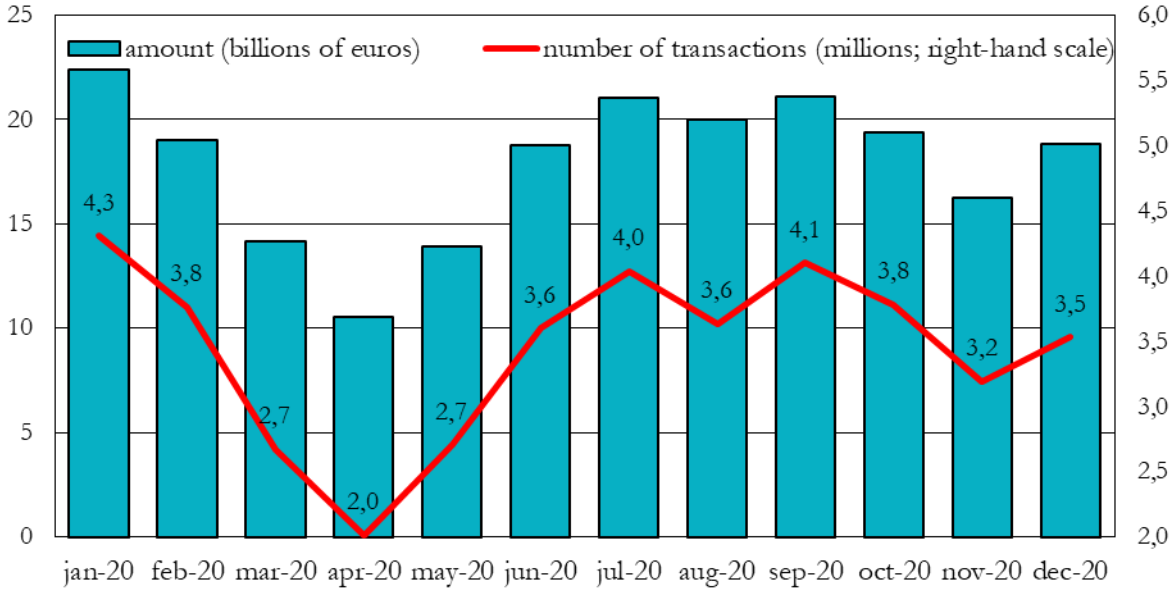
Accordingly, during 2020 the Unit monitored the quality of threshold-based communications, the transmission of which had begun in September 2019. On the one hand, it conducted checks of a general nature to detect cash transactions whose size or structure might suggest the presence of errors; on the other, it checked for inconsistencies with the information from suspicious transaction reports (for example, cash transactions reported as suspicious but not included in the threshold-based communications).The Unit's observations induced the operators involved to take steps to improve the recording of cash transactions and adjust the methods for extracting data from their own databases in order to prepare the reporting flow. In the light of the shortcomings it found, the UIF has developed further controls to conduct during the data-acquisition phase and is introducing checks, including on-site controls, of the measures taken by operators to remedy the shortcomings.

The communications for 2020 showed an average of 3.4 million transactions per month (about 220,200 withdrawals and 3.2 million deposits) for a monthly average amount of €18.0 billion[4] (Figure 1.7).

The flow of threshold-based communications

Figure 1.7

Threshold-based communications



The average transaction amounts remained practically stable over the period at about €5,300 for deposits and €3,600 for withdrawals, while the median amounts were about €3,200 for the former and €2,000 for the latter. The total transaction amount fell sharply in March and April during the lockdown for the COVID-19 pandemic, declining by 40.5 per cent compared with the first two months of the year.

The two-month reduction in transaction amounts was uneven across regions. It was steepest in Valle d'Aosta (55.4 per cent). Trentino-Alto Adige (52.8 per cent), Lombardy (49.9 per cent) and Lazio (42.2 per cent); the contraction was less sharp in Puglia (32.0 per cent), Sardinia (32.6 per cent), Basilicata (34.6 per cent) and Sicily (34.9 per cent).

A second, more moderate decline occurred in November, when new, tighter restrictions were introduced against the spread of COVID-19. Between October and November 2020, the total transaction amount fell by 16.2 per cent; the declines were sharpest in Trentino-Alto Adige (30.9 per cent), Valle D'Aosta (25.2 per cent), Lombardy (23.9 per cent) and Piedmont (19.2 per cent), all of which were classified as 'red' by the first week of November. In December, cash transaction amounts swung back into line with the averages for the year, increasing by 15.8 per cent with respect to November.

Regional distribution

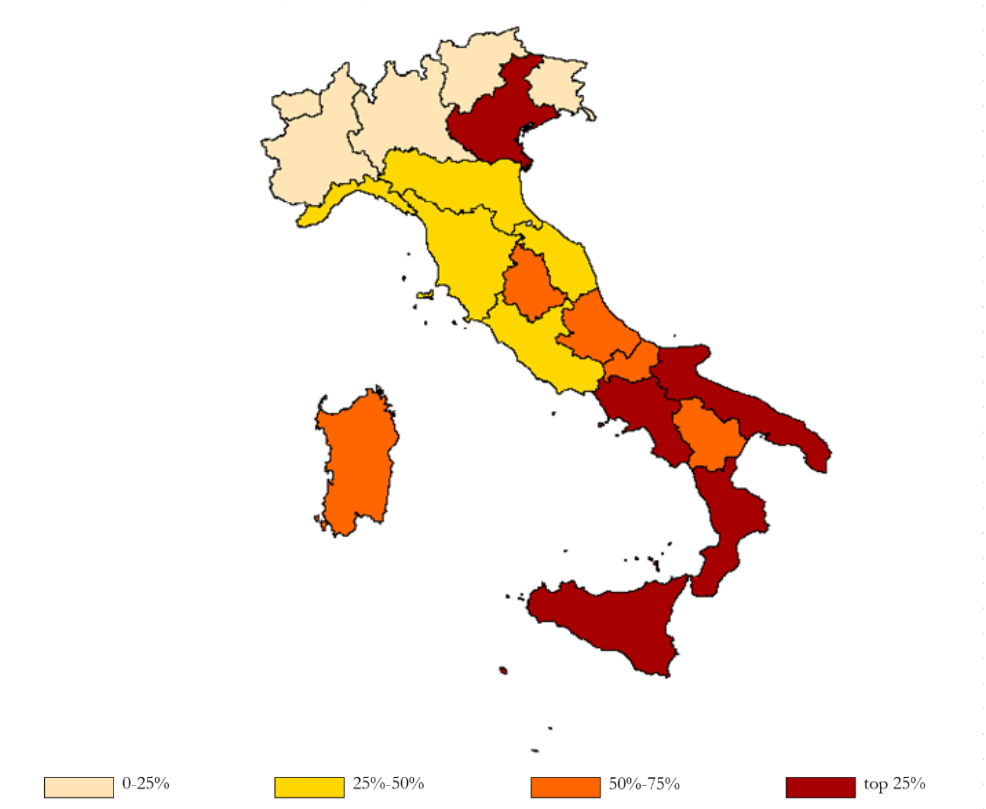
The total transaction value was highest in Lombardy, Veneto, Lazio, Campania and Emilia-Romagna, which together accounted for 56.8 per cent of the national total. However, in relation to nominal GDP for 2019, transaction amounts were highest in Puglia, Veneto, Campania, Calabria and Sicily (Figure 1.8).

[4] The data are subject to rectification by the reporting entities. The numbers given here are based on data updated to 6 April 2021.

Figure 1.8

Threshold-based communications in 2020: amount by region

(as a percentage of nominal GDP in 2019; quartiles)

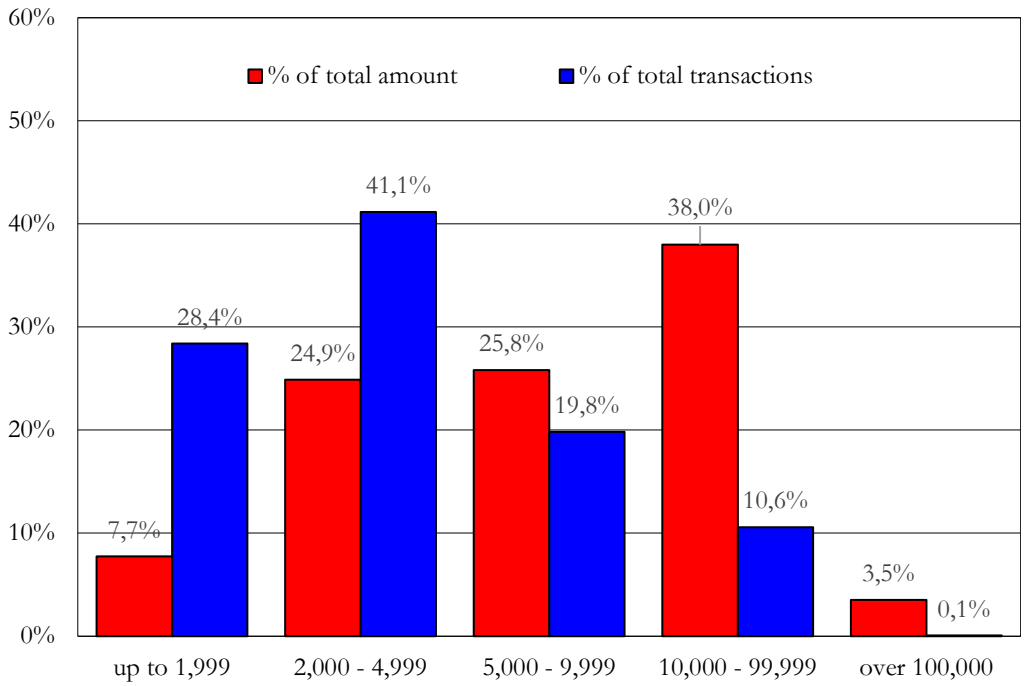


Distribution by amount

The statistics show a concentration of transactions by number in the €2,000-€4,999 range and by amount in the €10,000-€99,999 range (Figure 1.9). Transactions exceeding €100,000 numbered more than 30,600 in the period and amounted to about €7.6 billion.

Figure 1.9

Threshold-based communications: transactions classed by amount
(amounts in euros and percentage shares)



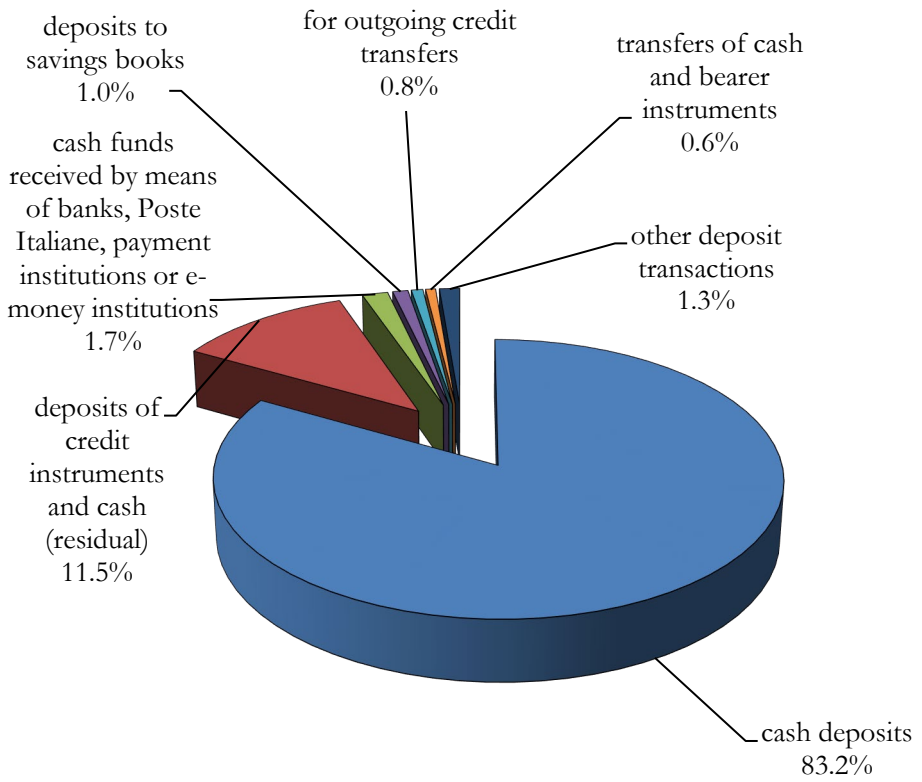
Transaction typologies

Deposits again far outweighed withdrawals, accounting for 93.6 per cent of number and 95.6 per cent of the value of total transactions. The difference in the size of the two flows appears to reflect, on the one hand, the need for households and firms to reduce the cost and risks of holding large sums for making purchases and, on the other, the large size of the deposits made by major retailers, who receive a high volume of small payments in cash. Cash deposits by means of ATMs or night safes, mainly ascribable to large-scale retailers, made up 57.6 per cent of total cash deposit transactions, followed by over-the-counter deposits and deposits of credit instruments and cash (Figure 1.10).

Figure 1.10

Threshold-based communications - deposit amounts (1)

(per cent of total deposits)



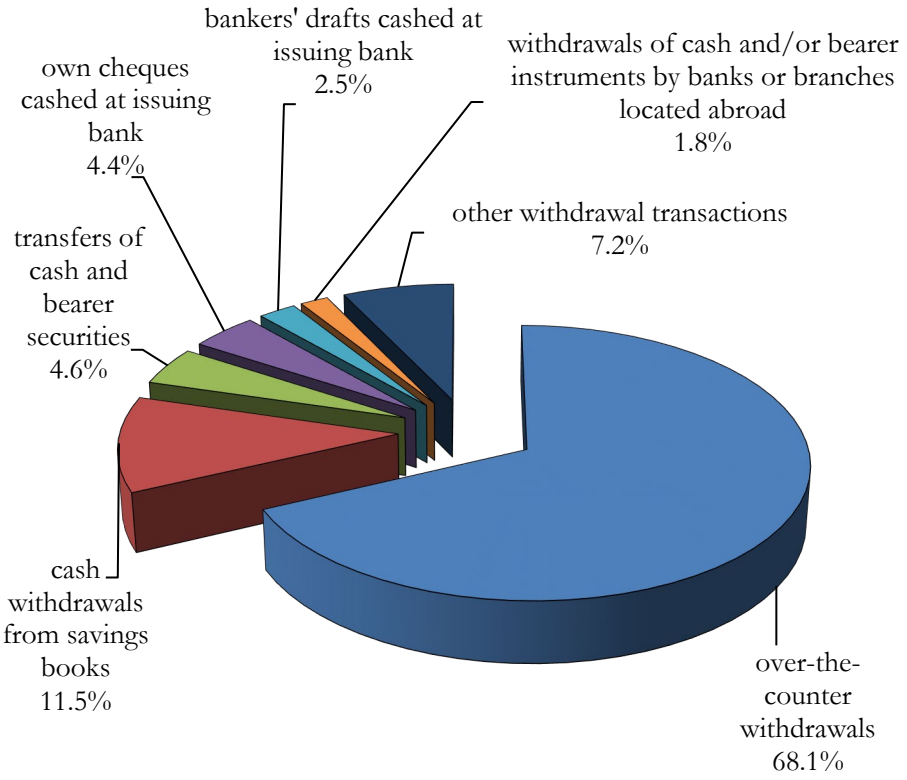
(1) Excluding cash deposits at ATMs or night safes.

For withdrawals, just under 80 per cent of the total amount refers to withdrawals with branch withdrawal forms or on savings passbooks (Figure 1.11).

Figure 1.11

Threshold-based communications: withdrawal amounts

(per cent of total withdrawals)



In 2020, there were 579 entities registered with the threshold-based communication system, of which 157 enjoyed exempt status. Specifically, 112 asked for the requirement to be waived because they do not allow transactions in cash with their customers, while 45 benefitted from the exemption for sectors for which legislation limits the use of cash to amounts below €1,000. Banks and Poste Italiane SpA represent the vast majority of active reporting entities (402 out of 422), accounting for 99.3 per cent of the amounts surveyed in threshold-based communications (Table 1.7). The communications of the first five entities of that category accounted for 58.5 per cent of the total by amount. Payment institutions and electronic money institutions were responsible for less than 1 per cent of the total amount, in part because they are subject to operating restrictions that generally limit the size of their transactions to amounts below the reporting requirement threshold.

Table 1.7

Transactions by category of reporting entity

	Amount		Number of transactions	Average amount
	(millions of euros)	*(% share)*	*(thousands)*	*(euros)*
Total	**215,479**	**100.0**	**41,356**	**5,210**
Banks and Poste Italiane SpA	**213,951**	**99.3**	**41,017**	**5,214**
Top 5 reporting entities	126,038	58.5	23,773	5,402
Other obliged entities	87,913	40.8	17,264	5,195
Payment institutions and contact points of EU payment institutions	**1,244**	**0.6**	**231**	**5,392**
Electronic money institutions and contact points of EU electronic money institutions	**284**	**0.1**	**88**	**3,208**

The utilization of threshold-based communications

Threshold-based communications are essentially different from suspicious transaction reports, in that the related obligation is triggered simply when pre-established thresholds are reached, independently of any assessment of the purposes of the transactions, which instead distinguishes STRs. Consequently, the transmission of a suspicious transaction report does not absolve a reporting entity from sending a threshold-based communication on the selfsame transaction; conversely, the transmission of a threshold-based communication does not require a suspicious transaction report unless there are elements suggesting money laundering or terrorist financing.

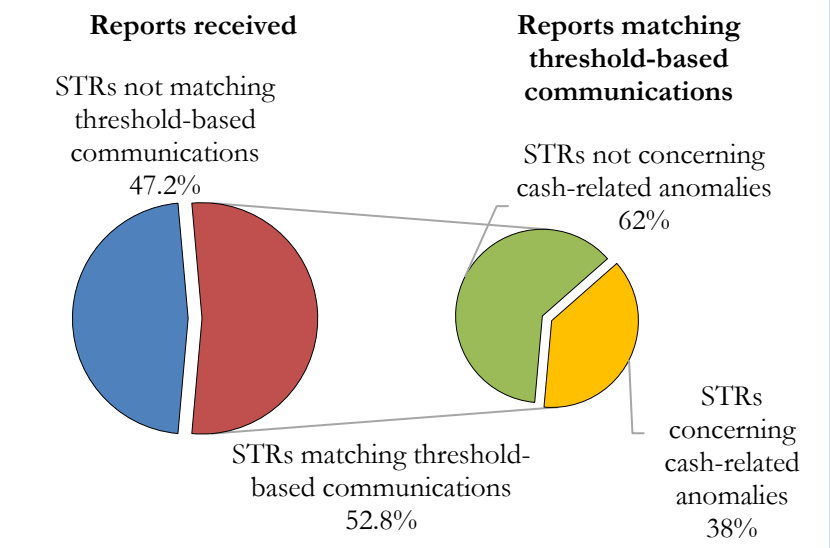
The data collected with the two observations overlap and complement one another significantly, given that they involve the same set of actors, namely persons carrying out suspicious transactions that involve significant amounts of cash and the same accounts, those to and from which these flows of money go. In 2020, 11.5 per cent of the persons and 5.2 per cent of the accounts surveyed in threshold-based transactions also showed up in the suspicious transaction reports received during the year.

In 2020, 52.8 per cent of the suspicious transaction reports received involved persons or accounts also recorded in threshold-based communications. For one out of two STRs, therefore, the Unit's analysts had access to information on the ways the persons flagged in the threshold-based communications used the cash, which enriched the investigative toolkit at their disposal and facilitated identification of the anomalous contexts. Of the latter, 38 per cent were found to have stemmed from mere instances of anomalous utilization of cash, but the remaining 62 per cent raised suspicions of various irregularities, about a third of which relating to tax evasion and judicial proceedings (Figure A).

Figure A

Suspicious transaction reports and threshold-based communications

(per cent)



The distribution by category of reporting entity of the STRs matching threshold-based communication is uneven. In 2020, more than 56 per cent of the STRs transmitted by banks, Poste Italiane S.p.A., payment institutions and electronic money institutions had links with persons or accounts cited in threshold-based communications. At any rate, the incidence was also high (above 29 per cent) for reporting entities not obligated to transmit threshold-based reports, such as insurance companies, gaming service providers and some categories of professionals.

The information contained in threshold-based reports not only serves directly to enhance suspicious transaction reports but also makes it possible to explore financial flows with statistical tools or analysis of networks and relationships in order to detect potentially anomalous transactions not yet recorded in STRs.

The various investigative strands that the Unit is studying concern the evolution over time of the flows in specific territories, the characteristics of the transactions, the actors involved and the sectors of economic activity in which they operate.

2. OPERATIONAL ANALYSIS

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

The analysis, preceded by automatic enrichment of the data received from the reporting entities, exploits the UIF's dataset and enables the Unit to classify the reports according to the risk and the related phenomenon. The most important contexts are then selected, handled in the most effective way and disseminated for subsequent investigation. The process follows the risk-based approach established by international standards and allows the Unit to adapt its action in light of the threats and vulnerabilities identified in the course of risk assessment exercises and taking account of the results of strategic analysis.

2.1. The data

The UIF analysed and transmitted to investigative authorities 113,643 suspicious transaction reports in 2020, 6.9 per cent more than in 2019 (Table 2.1).

Table 2.1

Reports analysed by the UIF

	2016	2017	2018	2019	2020
Number of reports	103,995	94,018	98,117	106,318	113,643
Percentage change on previous year	*22.9*	*-9.6*	*4.4*	*8.4*	*6.9*

As in the preceding years, the Unit processed and transmitted slightly more reports than those received, despite the persistent increase in the latter.

2.2. The analysis process

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

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

Processing time

The UIF has worked constantly to shorten STR handling time. In 2020, the reduction achieved was greater than in the preceding years, with average processing time falling from 20 to 16 days. The share of reports sent to investigative bodies within 30 days of receipt by the Unit rose from 79.5 to 86.1 per cent. Processing time for reports with higher risk profiles decreased sharply: 63.0 per cent were analysed and transmitted within 7 days of receipt (against 47.8 per cent in 2019) and 93 per cent within 30 days. A factor in this was the decision, in the case of especially complex analyses, to transmit the results and findings progressively, as they were reached, in order to help financial and investigative analysis to proceed in parallel.

The adjustments required by the pandemic

The need to shorten report transmission times was especially acute against the background of the pandemic. Specific adjustments were made to working procedures in order to identify and handle with top priority incoming reports that displayed some relationship with the risk situations created or exacerbated by the series of measures that the authorities took to contain the pandemic and support the economy. In particular, the Unit prepared an internal classification system to select the riskiest contexts; these related chiefly to the supply of masks and PPE in an initial phase and subsequently to guaranteed loans and outright grants (see Section 3.1, 'The impact of the pandemic'). In addition, the Unit undertook systematic cross-checking of the STR databases against information from the pertinent government ministries in order to promptly pick up the names of persons reported in STRs who received guaranteed financing. The absolute priority assigned to the analysis of such reports enabled the Unit to transmit them immediately – on average, within 7 days of receipt – to the Special Foreign Exchange Unit of the Finance Police (NSPV) and the Anti-Mafia Investigation Department (DIA).

Exchange of data with the DNA

Coordination with investigative bodies and with the National Anti-Mafia and Anti-Terrorism Directorate (DNA) benefited from the new procedure for weekly exchanges of name registries and information, pursuant to Article 8 of Legislative Decree 231/2007, with reference to suspicious transaction reports and spontaneous communications received from abroad relating to the COVID-19 pandemic. On the analysis side, the matches found helped in the selection and deeper investigation of the operational contexts involved in reports.

This exchange with the DNA comes on top of the monthly exchange already in place, whose results have been automatically integrated into the STR handling processes since the second half of last year. In addition, in 2021 the UIF and the DNA signed an agreement to shorten the data-exchange interval from monthly to fortnightly, permitting more effective sharing of the results of data exchange not only with the DNA but also with the NSPV and with the DIA, and speedier activation of the competent public prosecutor's offices for the aspects regarding organized crime and terrorism.

Interventions on the RADAR system

More in general, and even apart from the emergency context, the ever-increasing number of STRs, the growing complexity and variety of the body of information accompanying them and the progressive expansion of the typology of reporting entities have prompted a rethinking of working procedures, the related IT infrastructures and the tools available. In this direction, during 2020 the UIF launched a RADAR system development project aimed at identifying technologically innovative solutions that can assist more efficient selection of the contexts deserving further examination by automatically distinguishing between those that are more similar to known operational paradigms and those that instead present novel features, are less intelligible and are marked by higher risk factors (see Section 10.4, 'IT resources').

Tools of graph analysis

In the same vein, the Unit undertook a project to enhance its exploitation of the information at its disposal by creating a graph database. This method of information management will facilitate the application of sophisticated tools of visual analysis, which the Unit already brings to bear, in part, on the payment card, money transfer and virtual asset sectors (see Sections 2.4, 'Methodology', and 10.4, 'IT resources'). At the same time, the project will serve to devise additional innovative solutions that permit advanced data modelling and analysis by means of semantic techniques (knowledge graphs).

Ma3tch

The analysis process benefited in 2020 from improved matching between the RADAR database and the data drawn from the archives of the European FIUs participating in the FIU.NET platform by means of the Ma3tch function. In particular, steps were taken to extend and harmonize the spectrum of data covered by this data exchange designed to bring out cross-country links that are not discernible from the transaction context reported.

2.3. Risk assessment

Appropriate risk assessment of STRs is instrumental both to financial analysis and to the subsequent investigative phases.

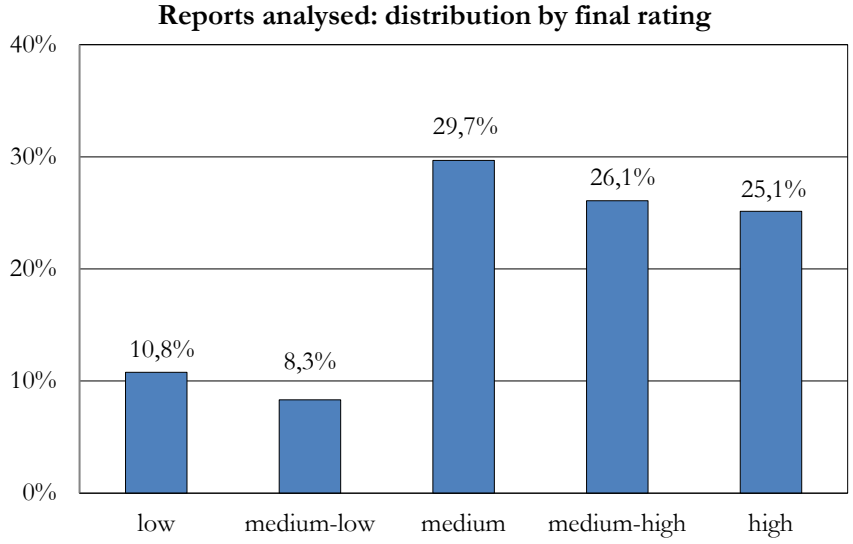
An initial appraisal is made by the reporting entity itself, on the basis of the information in its possession, by assigning a rating on a scale from 1 to 5.

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

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

The distribution of the final ratings of the STRs analysed and processed by the Unit in 2020 shows a slight accentuation of risk compared with the previous year: 51.2 per cent of the reports were considered to be medium-high or high risk, compared with 47.8 per cent in 2019 (Figure 2.1).

Figure 2.1



Against this increase, the share of reports that received a risk rating towards the lower end of the scale declined from 22.3 to 19.1 per cent, while those rated 'medium' remained stable at 29.7 per cent.

Again in 2020, the reclassifications made following analysis mainly involved reports that the RADAR system had initially rated as low or medium-low risk: 44.4 per cent of these STRs received a final rating of medium and 5.7 per cent medium-high or high risk. As in the previous year, there were fewer reclassifications in the opposite direction: of the reports initially rated as medium-high or high risk, 10.7 per cent got a final rating of medium and 4.5 per cent of low risk.

There was significant convergence between the risk assessments of the reporting entities and those of the UIF, albeit less than in the previous year: 40.7 per cent of reports (44 per cent in 2019) received a final rating in line with the reporting entities' assessments (of the latter, 35.6 per cent consisted in those rated as low or medium-low risks and 64.4 per cent in those rated as high or medium-high risks; Table 2.2).

Comparison of STR risk ratings by 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	14.5	3.4	1.2	**19.1**
	Medium	16.5	8.1	5.1	**29.7**
	Medium-high and high	15.4	17.7	18.1	**51.2**
	Total	**46.4**	**29.2**	**24.4**	**100.0**

Determination of the risk level of a report, also through the assignment of a composite rating, is part of a well-established overall methodology that benefits from the feedback from investigative bodies and at the same time orients the developments of the UIF's analyses and the subsequent phases of investigation. If the process underlying these assessments is to preserve its significance over time, it must be revised periodically both in order to take account of the elements present in the new sources of information available to the Unit and prevent the enrichment of the databases from producing a proliferation of the factors affecting the determination of the risk level. The recently launched project activities are therefore also directed at assessment of the tools and related methods so as to identify the adjustments needed to achieve greater selectivity of high-risk situations and maintain the standards of effectiveness (see Section 2.2, 'The analysis process').

2.4. Methodology

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

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

When further scrutiny is needed to reconstruct the financial trail of suspicious funds, the STR is subjected to a second-level analysis, ending with the assignment of a final risk rating and a document accompanying the report to the investigative bodies that details the results of the financial checks.

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

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

The ever-growing number of STRs and the consequent enrichment of the UIF's information assets, owing in part to the progressive expansion of the datasets, make it increasingly necessary for the Unit to acquire, already during first-level analysis, an integrated vision of all the significant information so that it can make an exhaustive assessment of the risk profile and underlying phenomena.

First-level analysis itself often finds links with previous STRs; accordingly, the examination of an STR cannot proceed without careful collection and interpretation of all the potentially significant pieces of information contained in the various reports involved. The links can also be quite numerous, to the point that they render reconstruction complex, prolonging analysis and increasing the risk of overlooking crucial information.

Risk indicators in first-level analysis

Consequently, for some sectors typified by the above-mentioned features (payment cards, money transfers, gaming, virtual currencies), the traditional tools of analysis have been supplemented, on an experimental basis, by a reading-support system that organically aggregates the data that can be gleaned both from the STR being analysed and from the set of connected STRs, and uses a series of indicators to flag the most relevant ones from the standpoint of risk. This enables the analyst to rapidly access the data most useful for getting an adequate overall picture for the first-level assessment of the context.

By means of an ad hoc reporting and weighting system, the indicators highlight the subjective risk factors (e.g. presence of politically exposed persons), investigative risk factors (e.g. involvement of persons under investigation) and financial risk factors (e.g. anomalous activity) as well as specific elements regarding the reach of the network of persons to whom the report under analysis is linked.

Aggregate analysis

In the course of 2020, the Unit also developed 'third-level' analyses designed to capture more effectively the illegal phenomena characteristic of the above-mentioned sectors and to identify, thanks to a broader perspective, the significant contexts to be submitted to further scrutiny – for example, those relating to criminal networks. In this field, the Unit strengthened its exploitation of specific techniques, such as social network analysis, which it had already employed with positive results in examining highly complex financial networks.

Payment cards

One of the most promising fields of application is that of payment cards. The Unit's work has revealed the exceptional fragmentation of the transactions carried out in this sector, in part as a consequence of operational ceilings that foster the splitting of transactions across multiple cards and multiple persons. The reports describing these flows typically show a significant number (hundreds) of persons and accounts, usually with equally numerous links to other STRs.

By way of an example, in 2020, aggregate analysis of 87 reports regarding 1,324 payment cards held by 1,124 different persons turned up a particular operating method employed by criminal associations, mostly formed by Nigerian nationals, to launder, in Africa, substantial illegal proceeds from computer fraud, contraband, and trafficking in weapons, drugs and human beings (see Section 3.5, 'Further case studies').

Money transfer agents

Like the reports regarding payment cards, the STRs transmitted by money transfer agents lend themselves particularly well to network analysis applications, as they ordinarily refer to a large number of low-value transactions which, taken one by one, do not provide significant elements of assessment. The experimental analysis performed by the UIF detected the existence of networks of persons connected to anomalous financial flows. Once completed, the development of this tool will make available to the Unit a network analysis, alongside the well-established aggregate analysis of money transfer agents that it has been conducting for some years, further enhancing its ability to probe contexts tied to exploitation of human beings, fraud and other illegal trafficking and providing useful elements for mapping the underlying criminal organizations.

Gaming and gambling

In the gaming sector as well, traditional analysis has been flanked by a new technique aimed essentially at intercepting significant phenomena that can only be evaluated based on an aggregate view of the contexts. This is the case, for example, of concentrations of anomalous bets placed at a given gaming parlour or at interconnected gaming parlours, which make it possible to detect unknown links or hypothesize instances of the involvement of gaming-parlour managers which traditional analysis would not immediately pick up.

An initial experiment of aggregate analysis of this kind concerned the identification of the most anomalous videolottery parlours based on the records in the UIF's database. To this end, the Unit developed a specific risk indicator allowing it to compile a list of the highest-risk parlours for further scrutiny.

2.5. Suspension orders

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

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.

The Unit carried out 308 evaluations with a view to the issue of suspension orders, against 342 in 2019; the value of the transactions examined amounted to €175.1 million, 25.2 per cent less than in 2019. The Unit undertook 68 of these on its own initiative, up from 55 in 2019 thanks to the procedure for systematic monitoring of high-risk STRs on transactions whose execution is pending.

In all, the Unit found grounds for issuing a suspension order in 37 cases (12.1 per cent of those it assessed, compared with 12.6 per cent in 2019, for a total value of €13 million; Table 2.3). In 11 of these cases, the order stemmed from evaluations undertaken by the Unit on its own initiative, which produced a higher rate of positive outcomes than those undertaken at the prompting of a reporting entity (16.2 against 10.8 per cent).

Table 2.3

Suspensions

	2016	2017	2018	2019	2020
Number of transactions	31	38	47	43	37
Total value of transactions (*millions of euros*)	18.9	66.4	38.8	11.4	13.0

In 2020 the majority of the evaluations again concerned transactions being carried out at insurance companies or, to a lesser extent, at banks (respectively 80 and 15 per cent of the total). Nearly all the transactions examined concerned policy surrenders or payouts at maturity traceable to persons under investigation for corruption or tax evasion or close to organized crime.

Anomalous transactions attributable to contexts linked to the COVID-19 emergency were prominent among the examinations initiated during the year. In this field, the examination concerning a request for bankers' drafts and credit transfers to be debited to a company's bank account for an amount equal to its outstanding balance was concluded with a positive outcome. The request was presented by the company's sole director, already a politically exposed person under investigation for irregularities connected with imports of personal protection equipment. The order suspending all debit transactions on the company's account was followed by a seizure order issued by the competent investigative authority, which described how the request for the debit transactions had the evident purpose of emptying the account, thus constituting attempted self-laundering.

2.6. Information flows of investigative interest

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

Feedback on the investigative interest of the reports it transmits continues to be of fundamental importance for the Unit. Although such information is also affected by factors not directly attributable to the Unit's work, it offers the Unit indications as to the validity of its methods for STR enrichment and for developing the criteria for selecting and assessing future reporting flows.

In relation to the STRs sent to the investigative bodies in the two years 2019-20, as of the beginning of May 2021 the Finance Police had sent the Unit 43,386 positive feedback reports, of which 83.2 per cent concerned STRs classified as high or medium-high risk and only 3.2 per cent referred to STRs rated as low or medium-low risk. During the same period,

the Unit received 5,577 positive feedback reports from the Anti-Mafia Investigation Department, of which 91.7 per cent referred to STRs with a high or medium-high risk rating.

3. RISK AREAS AND TYPOLOGIES

With its operational analysis of suspicious transaction reports, the UIF identifies typologies characterized by recurring elements material to the assessment of the risks of money laundering or terrorist financing. This enables the Unit to classify STRs and to disseminate updated indications to facilitate reporting entities' identification of suspicious transactions.

3.1. The impact of the pandemic

The customary paradigms of risk recognition and classification were conditioned in 2020 by the insurgence of the pandemic, which in a matter of months brought new threats to the fore, while also changing the scale of already known risks. The speed of transmission of the virus, the restrictive measures taken to contain it and the consequent deterioration of the economic situation of households and firms required a complex series of public interventions, initially to procure medical supplies and personal protective equipment (PPE) and then to support the economy.

The need for a speedy response to the deepening health emergency led to an easing of administrative controls that in some cases created manoeuvring room for illicit behaviour in dealings with public counterparties and, indirectly, also between private parties. In the background, the social and economic repercussions of the pandemic magnified the risks of infiltration of businesses by organized crime. This ensemble of factors prompted the Unit to issue two communications to stimulate obliged entities' attentive monitoring of such risks and ensure the active cooperation of all the actors in the AML system (see Section 9.3, 'Secondary legislation'). At the same time, the need for prompt identification of any reports of cases of anomaly relating to COVID-19 required the UIF to make rapid adjustments to its STR handling procedures and fine-tune its synergies with investigative bodies (see Section 2.2, 'The analysis process').

STRs in the context of the pandemic

In 2020, the Unit received 2,277 STRs pertaining to pandemic-related circumstances of risk in respect of transactions amounting to €8.3 billion. Initially, 80 per cent of these transactions mainly concerned sales of medical supplies and PPE, subsequently joined by the incongruous disbursement and use of guaranteed loans or outright grants. Some 64 per cent of these STRs elicited positive feedback from investigative bodies

The remaining 20 per cent of STRs classified as belonging to the COVID-19 risk area concerned cash withdrawals, most of which apparently prompted by fears of a liquidity shortage with the inception of the lockdown and with the general climate of uncertainty in the early months of the pandemic. Their lower degree of risk is borne out by the fact that only 9.2 per cent of them were found to be of investigative interest. Overall, 18.4 per cent of the STRs that the Unit received in 2020 and classified in the COVID-19 risk area resulted in positive matches in the exchange of names with the DNA.

A minority of STRs (281 out of 2,277) but nevertheless an important share in terms of amount (€5.9 billion, or 70.9 per cent of the total) concerned transactions that were

ordered but not executed, mostly relating to attempted fraud in connection with disbursements of public financing. The STRs on transactions that were executed, for smaller average amounts, chiefly involved accounts recording a high use of cash or anomalous funds transfers, hypothetically compatible with the misappropriation of the public funds granted or with invoicing fraud. In total, 25.2 per cent of this subset of STRs involved individuals under investigation; the share rises to 32.3 per cent if STRs on attempted but unexecuted transactions are included.

Practically all of the COVID-19 suspicious transaction reports came from the financial sector: 94.2 per cent counting those sent by banks or Poste Italiane, 96.8 per cent also including those transmitted by electronic money institutions or payment institutions. The STRs sent by professionals were a residual number.

The regions figuring most prominently as places of execution of the suspicious transactions were Lazio (18.7 per cent) and Lombardy (14.4 per cent), followed by Emilia-Romagna (8.8 per cent), Campania (8.5 per cent) and Veneto (7.6 per cent).

In the first five months of 2021, the Unit received 1,796 pandemic-related reports regarding suspicious transactions worth €1.86 billion. Most of the cases examined involved financial incentives and, to a lesser extent, the procurement of medical supplies, while cash withdrawals connected with the health emergency became residual. The level of investigative interest of the COVID-19 STRs also remained high, at 37.5 per cent. The STRs on attempted but unexecuted transactions (14.8 per cent of the total, a significantly smaller share than in 2020) mostly concerned the negative findings of background checks on the persons ordering the transactions. The cases detected among the transactions that were executed were again tied to tax-related aspects, often in connection with monetization operations and the suspected forging of documents. In this subset of STRs as well, individuals involved in penal proceedings show up in just under one fifth of COVID-19 reports.

Examination of the reporting flow brought to light a sequence of cases of anomaly that broadly tracked the evolution of the pandemic.

In the first part of the year, with the outbreak of the pandemic and the adoption of severe restrictions on economic activity and personal mobility, the Unit recorded a reporting flow concerning anomalous recourse to cash on the part of households and firms, apparently motivated, at least for withdrawals, by uncertainty about the duration of the lockdown and the resilience of the banking and financial system, but which in some cases displayed anomalies with respect to the relevant economic context (for example, substantial deposits by business establishments that were closed due to the lockdown).

The onset of the health emergency significantly increased the demand for medical supplies, particularly on the part of general government, whose all but total reliance on fast-track procedures allowed the participation in tenders or the award of contracts to firms that could be traced to individuals with doubtful backgrounds or whose offers later turned out to lack the technical requisites. In some cases, the contracting entities' system of controls intercepted these deficiencies and excluded the firms or voided the contract awards as a measure of self-protection. The related communications of general government underscored serious problems raised by the backgrounds of company representatives with criminal records or significant past violations of tax and social contribution laws. In nearly all the cases, the firms had suddenly repurposed themselves to enter the medical supplies sector and their assets and finances were inadequate to the size of the procurement contract.

In several other cases, including some very significant ones that drew media coverage,

the above-mentioned anomalies were not promptly picked up by the contracting entity: in these situations, the Unit's analysis of the reports immediately brought into focus significant anomalies, later confirmed by investigative developments. Despite the recurrence of these anomalies (insufficient resources to fulfil the contract, activities in heterogeneous sectors having nothing to do with medical supplies), fast-track procedures were used to award high-value contracts to companies that received large advance payments from the contracting entities, sometimes in derogation of the rules that the awardee must provide the required performance guarantee. In some cases, the guarantee, though provided, turned out to be false or to have been issued by a foreign company lacking the necessary authorizations. There was also a case in which the foreign guarantor company was linked to Italian individuals known to be close to organized crime. Given these weaknesses, the companies proved unable to fulfil their contractual obligations on time and with goods satisfying the technical specifications.

In this framework, a factor drawing attention to some of the larger procurement contracts was the presence of ownership and financial links of the awardee companies with politically exposed persons or with individuals who, as consultants or intermediaries, appear to have acted as facilitators of the contract award. Reconstruction of the financial flows underlying such cases often corroborated investigative findings that suggested an ability to influence administrative action in the emergency setting.

The widespread need for PPE, particularly for masks, also had repercussions on the private component of the market, inducing small firms engaged in a great variety of sectors to hurriedly convert to the medical equipment sector in order to try to supply private operators such as pharmacies and businesses seeking equipment for their own personnel. Several reports highlighted the surge in financial dealings on the part of small firms with foreign, mainly Chinese suppliers for the purchase, at least apparent, of masks for resale in the private sector. These reports flagged a variety of suspicious elements, ranging from the size of mark-up upon resale of the items to the possibility of counterfeiting, as suggested by the documentation exhibited to customers. In several cases, the very existence of the procurement is called into question, raising the suspicion of false invoicing or of fraud, especially where the transactions to employ the presumed proceeds of the procurement contract have unusual features.

An example of this involved a foreign company, with bank accounts also in Italy, that used the proceeds of a fraud in the marketing of PPE (failure to deliver the goods), perpetrated at the expense of a company headquartered in the European Union. The analyses, prompted by a spontaneous communication by an EU FIU, ascertained that the proceeds were invested, via a loan to an Italian company linked to an accountant, in notes issued by a special purpose vehicle (SPV) as part of a securitization operation for the purchase of specific impaired claims. In the ensuing months the SPV, after cashing or reassigning the claims it had acquired, repaid the amounts to the company that had purchased the notes, which in turn transferred the entire sum abroad to the accounts of the foreign company that had carried out the fraud.

The spread of the health emergency led, especially in the first half of 2020, to the birth of a multiplicity of associations that offered to collect donations to aid the national health system, particularly in the purchase of medical devices for the expansion of intensive care units. Unfortunately, these associations also fell victim to misappropriation, usually by persons in management positions. This was the case of an individual with power of attorney on the accounts of a non-profit organization set up in March 2020 to deal with the COVID-19 emergency at local level, who diverted part of the amounts donated by individuals to a complicit company through payments on account of invoices issued for non-existent operations.

The analyses found that the sums were transferred to foreign accounts and then withdrawn and/or spent in Italy by means of payment cards issued by the foreign financial intermediary to the manager of the organization.

The second phase: loans and grants

In the second part of the year, with the increasing disbursement of various forms of economic support, the reporting flow polarized around anomalies tied mainly to firms' access to state-guaranteed loans or grants.

The measures to support the economy

Both of the UIF Communications on the potential risks of financial crime connected with the health emergency referred to the financial support measures of the Government to cope with the economic shock caused by the pandemic, considering the risks of undue access to such measures by ineligible persons or even by firms infiltrated by organized crime. There were, in fact, a good many cases in which obliged entities activated the reporting procedure in the face of apparently anomalous behaviour during the various stages of the disbursement of the relief.

During the application phase, a central role is played by self-certification under Presidential Decree 445/2000, whereby the interested parties declare that they satisfy the legally established requirements for eligibility to receive financial support from the state. Aimed at speeding up and simplifying the disbursement procedure (given that the lending institution is not called upon to check the truthfulness of the information furnished by the applicant), self-certification often lent itself to fraudulent conduct by the applicants, such as the alteration and falsification of data and documents, probably knowing that the reduced pervasiveness of controls, deemed appropriate because of the rapid nature of the measures, might allow them to escape the possible penal consequences associated with such conduct, at least in the short run.

In multiple cases, which often did not result in the granting of loans, suspicions arose in connection with the subjective profile of the applicants, who had been found guilty of various types of offence, were under investigation or displayed characteristics that suggested contact with criminal environments. The same goes for the doubtfulness of the information they provided concerning the designated use of the amounts and/or the actual realization of the projects for utilization of such amounts. In many cases of this kind, the loan examination triggered an inquiry into all of the customer's transactions, usually bringing out a more complex set of anomalies than could be picked up by the ordinary detection activity for assessments carried out pursuant to Article 35 of Legislative Decree 231/2007.

With regard to the uses of the funds credited, the obligation for the beneficiary to comply with the mandated use, where envisaged, made the monitoring of positions by obliged entities crucially important, and they detected a good many transaction schemes all characterized by diversion of the funds to a host of purposes other than the revival of business activity.

Split-up cash withdrawals (over the counter or from ATMs) were again among the instruments most frequently employed. However, the preponderant method was to use tracked instruments such as cheques (especially bankers' drafts) and credit transfers, for which, even when the stated reasons for payment are perfectly explanatory and not deceptive, the most disparate destinations are found. To give some examples: non-interest-bearing loans to relatives (including relatives abroad, particularly for foreign nationals), gifts to persons whose connection with the beneficiary of the loan is unknown or unascertainable, extravagant non-essential expenditures (automobiles, luxury goods, etc.), online payments

to gaming and betting companies, and investments in financial assets (including crypto-currencies) and real estate.

Monitoring by the disbursing entities is often hampered by the transfer of sums to the borrowers' accounts with other intermediaries, which in such cases are not always aware that the funds originally derived from a state-guaranteed loan for the COVID-19 emergency. The problem becomes even more acute in the case of intra-group transactions, since the company that received the loan can transfer the funds in whole or in part to one or more group companies for reasons that are apparently consistent with the purposes of such loans or that, in any event, are not deemed anomalous for normal intra-group transactions (e.g. transfers relating to treasury operations).

Even outside the sphere of intra-group relations, the transfer of the entire amount of the financing to a third company immediately after disbursement is a scheme that emerged repeatedly in the course of analysis. This strategy is designed to get around the fact that the ultimate beneficiary of the transfers is ineligible to obtain the loan by using the loan examination conducted on the probably complicit applicant.

In other cases, there was an artificial splitting up of loan applications by apparently different legal entities belonging to the same overt or concealed beneficial owner. Such situations often involve the intervention of individuals apparently extraneous to the ownership or management of the applicant companies, described from time to time as presenters, assistants, advisors, contact persons or the like, who facilitate the establishment of relationships between the companies and the lender or, where the companies already hold accounts with the lender, the preparation of everything necessary for the start of/to start the loan examination procedure. For cases of this kind, the fact that the different loan applications are not manifestly traceable to a single directing hand represents a serious obstacle to determining their overall perimeter.

3.2. Organized crime

Over 18 per cent of the suspicious transaction reports that the Unit received in 2020 pertained to contexts at least potentially traceable to the interests of organized crime. This figure, about twice those recorded in the previous years, reflects the Unit's greater ability to pick up such cases thanks to the systematic exchange of information with the DNA under Article 8 of Legislative Decree 231/2007, which was put on a permanent footing in the third quarter of the year (see Section 2.2, 'The analysis process'). Nearly all of the reports in question were considered significant, and targeted examinations were performed on 11 per cent of them, with an increase of 21 per cent in the number of STRs so treated compared with 2019.

Some 2.6 per cent of the reports classified as at risk of organized crime concerned anomalies discovered in contexts tied to the COVID-19 emergency; the Unit received positive feedback during the year from investigative bodies in 62 per cent of these cases, compared with 18.5 per cent for all the reports so classified.

The distribution of the reports by region, in line with the findings of the previous years, confirms a high degree of correlation with the regional distribution of mafia organizations mapped by the DIA and the DNA: 23.5 per cent concerned Campania, followed by Lazio (14.2 per cent) and Lombardy (13.0 per cent); then came Sicily (10.1 per cent), Puglia (6.7 per cent) and Calabria (6.2 per cent); Emilia-Romagna, Veneto, Piedmont and Tuscany also accounted for not insignificant shares (5.3, 4.5, 3.9 and 3.6 per cent, respectively).

The typology of transactions reported does not differ substantially from the findings of previous years, with a recurrence of tax-related anomalies, often accompanied by transfers with foreign countries. In addition, the operations examined were frequently carried out through cross-transactions between natural or legal persons with no apparent relationship or economic links, in some cases framed ostensibly as corporate and/or real estate transactions. As in the preceding years, the technical forms used do not differ from the patterns characteristic of contexts that are extraneous to organized crime.

In this area of risk as in others, the Unit's special attention to reports relating to the health emergency enabled it to pick up some important signals regarding the strategies of criminal organizations during the course of the pandemic.

On the basis of the evidence now available, in the initial phase of the epidemic, persons presumably connected with organized crime showed an interest in entering the field of the production and/or marketing of medical equipment and PPE. This entry was achieved via the conversion of production from textile goods to masks and other PPE and the assumption by individuals with shady backgrounds of operational roles in the companies, including by means of nominees, in order to control their production or marketing after their corporate purpose had been changed. In this phase, there were significant instances of fraud connected with the sale, sometimes not followed by delivery, of PPE at apparently disproportionate prices with respect to market prices. In some cases, public procurement contracts were found to have been awarded to firms whose corporate officers were tied in various ways to companies for which anti-mafia interdictions had been issued.

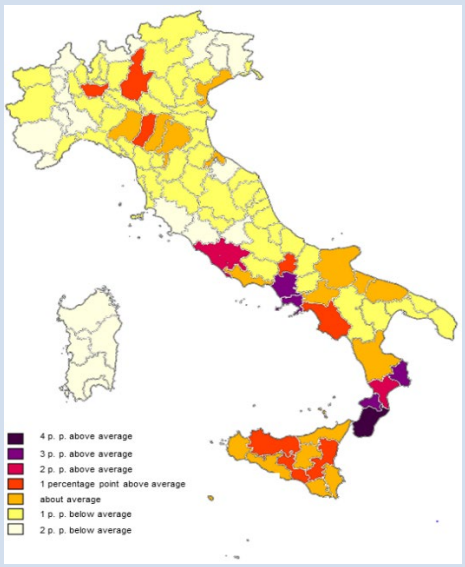
In a second phase, there were increasingly frequent possible cases of outright infiltration of firms and of attempted appropriation of public funds meant to support the economy by means of sham transactions designed to create the credentials for access to the funds. The Unit detected probable cases of centrally orchestrated operations also involving the intervention of advisers and professionals. Emblematic in this sense were some reports regarding the activity of persons, members of criminal groups according to the information available, who by means of false or misleading tax declarations fraudulently obtained VAT refunds that were then transferred abroad; the proceeds of the crimes were subsequently repatriated to Italy either in cash or through the transfer of equity interests in firms whose value did not tally with the amounts shown in the transfer agreements. Additional reports that came in later showed that some of the firms involved in this operating scheme had used the false turnover generated with VAT fraud to artificially create the necessary credentials for eligibility to receive public loans and grants disbursed under the measures to support the economic system following the onset of the COVID-19 emergency.

An experimental mapping of the firms potentially connected to organized crime

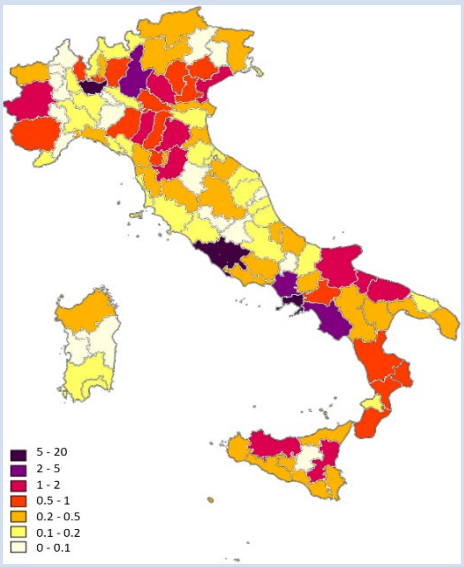
The Unit recently completed a preliminary mapping of the firms in Italy potentially connected to organized crime circles. The identifying particulars of all the firms listed in the Company Register and of their respective corporate officers (some 14 million subjects) were cross-tabulated with RADAR data (suspicious transaction reports, information exchanges with the DNA, requests for information from the judicial authorities), resulting in the identification of more than 150,000 active firms as at November 2020. The firms included in the mapping belong to one (or more) of the following subsets: 1) they were flagged in STRs that appear to relate to organized crime circles and that the Unit received between January 2016

Figure A

a) Local incidence of the firms included in the mapping
(as a percentage of the provincial total)



b) Suspicious transactions of the firms included in the mapping
(as a percentage of the national total)



and September 2020; 2) their directors and other corporate officers include persons mentioned in the STRs referred to in the preceding point); 3) their directors and other corporate officers include persons of interest on the basis of information exchanges with the DNA, persons investigated for mafia crimes who appear in business archives, or persons named in information requests from the judicial authorities regarding organized crime.

The firms included in the mapping exercise cannot be deemed with certainty to be infiltrated or controlled by or linked to organized crime, a circumstance that can only be ascertained at the investigative and judicial level. On the contrary, the mapping surveys (on the basis of the data available to the Unit) a firm's potential 'proximity' to organized criminal circles, which may then be verified in the appropriate forums.

The largest portion of the firms surveyed in the mapping are located in the South and Islands (41.9 per cent), but significant portions also operate in the North (36.2 per cent) and the Centre (21.9 per cent), corroborating the latest analytical and investigative findings. The local incidence of 'mapped' firms with respect to all the firms entered in the pertinent provincial register tends to be higher in the southern provinces, with peaks in Calabria, Campania and Sicily; in the Centre and North, the provinces most involved according to this criterion are Rome, Milan, Brescia and Reggio Emilia (see panel (a) of Figure A).

The largest anomalous financial flows are found not only in the mafia organizations' home regions in the South and Islands, but also in the rich provinces of the North and Centre where economic activity is liveliest, signally Rome, Milan and Naples (see panel (b) of Figure A).

The results of the mapping can assist the analysis of STRs and make possible analysis and research on the phenomenon of potentially infiltrated firms.

3.3. Corruption and misappropriation of public funds

The health emergency underscored the crucial importance of the characteristic risks of the public sector, whose vulnerability to corruption and, more generally, to the exercise of influence on administrative action was significantly aggravated by the dramatic circumstances of the pandemic. Outside the context of the pandemic as well, during the year under review the Unit encountered cases that confirm how the different forms of public subvention are exposed to risks of abuse and fraud.

Improper use of public financing

In particular, the Unit discovered patterns of behaviour that were ascribable to the improper use of funds obtained through public financial subsidies. Joint analysis of multiple reports of suspicious transactions, having in common their use of the same subsidy measure within a limited geographical compass, enabled the Unit to identify networks of physical and legal persons whose activity was presumably directed at securing fraudulent access to financing and then misusing the funds so obtained; persons involved in criminal proceedings in the past or linked to organized crime participated in such networks.

One of the characteristic features of such networks is the central role played by some firms, apparently unconnected to the others, that assist the applicants with advisory services or by providing the capital, sometimes paid in cash, that they require in order to access a subsidy measure. The funds disbursed are withdrawn in cash or transferred to these firms, in breach of what had been declared in the application for financing; in some cases, the funds are monetized by means of a preliminary transfer to prepaid cards held by connected persons and issued by foreign intermediaries.

Investment funds and public entities

There were some cases of anomalous transactions set up by investment funds in which public entities had subscribed an interest and that were intended to bring harm to the funds and unjustified economic advantages to private persons having consulting arrangements with the subscriber entities.

In one case of particular interest, the investment fund purchased goods and equity interests from a foreign company attributable to a consultant of the subscribing public entity, a company that had purchased them a few days earlier at a significantly lower price. Also taking part in the transaction was a firm headed by professionals and linked to the fund by a consulting contract generously remunerated by the company that had sold the assets to the fund.

In addition, the Unit discovered financial flows that directly involved officials of public entities. This was the case of the transfer of funds to the benefit of the president of an entity on the part of a company attributable to an entrepreneur who, via other firms, acted as a consultant for an investment fund subscribed by the same entity. In another case, an official of a public entity sold a property he owned to a newly established firm, which had received the money to purchase the property from consultants of the same entity, and then immediately regained use of it with a lease.

In 2020, the Unit commenced work on a composite indicator to be used in the automatic selection of STRs potentially connected with crimes against the public administration.

The need for a specific tool for identifying contexts characterized by such risks derives from the Unit's experience of analysis, which shows that significant cases are often identified upstream of the examination of STRs which, prima facie, do not appear to be connected with public interests or resources. In addition, illicit ends are pursued with diverse kinds of conduct that do not necessarily involve a financial transaction or procedures traceable by the

roster of reporting entities. The indicator is composed of subjective and objective information, divided by macro areas; its aim is to extend the perimeter of attention beyond transactions immediately attributable to classic patterns, by taking into account manifold elements that may be insignificant taken one by one but become significant for the interception of illegal phenomena when considered together.

3.4. Tax evasion

Assignments of tax credits and assumptions of tax liabilities

Suspicious transaction reports pertaining to possible tax evasion remained broadly unchanged from 2019 as a share of all STRs, standing at around one fifth. The majority of such reports (80.6 per cent) concerned familiar schemes involving transfers of funds between connected natural and legal persons, possible false invoicing, the use of personal accounts for the transit of what appear to have been business transactions, and cash withdrawals from companies' accounts.

During the year, the Unit received several reports concerning assignments of tax credits and assumptions of tax liabilities whose probable purpose was to obtain improper offsets of tax liabilities. The examinations conducted enabled it to identify additional cases regarding, in particular, the origin and manner of formation of the fictitious tax credits covered by the above-mentioned contractual arrangements.

Noteworthy was the case of a large VAT credit accrued following a property purchase by recently established connected companies. The purchase was made via a swap with equity interests in real estate companies in which the purchaser held stakes, their value being determined on the basis of the properties held by the companies. The value of these had suddenly increased following a transfer valuation report drawn up by a probably complicit professional, given that the aforesaid real estate companies had recently bought the properties at much lower prices in a forced sale procedure.

Other cases concerned firms that took over tax liabilities from other parties and offset them with their own research and development tax credits.

Tax credits of this kind are accorded to firms that invest in R&D and are proportionate to the expenses sustained for realizing such investments, provided the expenses qualify for the credit and are documented by appropriate accounting records and an explanatory technical report.

In the cases examined, the companies assuming the liabilities had accrued a significant R&D tax credit in their first year of activity, making large investments immediately after their formation and producing, in their annual financial statements, only a summary description of the work done and the expenses sustained. Furthermore, for the subsequent financial years the same companies neither deposited financial statements nor filed tax returns. The consideration for the assumption of liabilities, equal to 80 per cent of the value of the taxes offset, was, for the most part, transferred abroad to companies attributable to Italian nationals, with the funds subsequently withdrawn in cash.

Other investigations demonstrated how effective monitoring by the banking and financial sector of improper uses of tax credits directly serves to safeguard intermediaries against financial and/or reputational risks.

One case of particular interest concerned a financial intermediary that, as part of a factoring operation, purchased from a private firm claims on general government which were

later repudiated by the debtor, thus exposing itself to losses of several million euros. Subsequently the intermediary also discovered a previous purchase of VAT credits by its customer firm, a transaction that displayed various anomalies which could have been picked up, including by the intermediary, in the course of loan due diligence (for example, transfer of the VAT credits by means of a simulated transfer of company ownership, failure to specify the means used to pay the price, continual changes in shareholders, and anomalous values entered in the financial statements of the transferor of the credits.

The results of analysis of the different cases of fraudulent transfer and other improper uses of fictitious tax credits went into the drafting of an ad hoc 'pattern of anomaly' (only in Italian) which the Unit issued on 10 November 2020. The pattern was issued together with three others also concerning suspicious transactions connected with tax offences (see the box 'New patterns of anomaly concerning transactions connected with tax offences' in Section 9.3). The matter was also dealt with in the UIF's 'Communication' (only in Italian) of 11 February 2021 concerning the risks connected with the possible improper uses of tax credits awarded under the urgent legislation relating to the pandemic. In particular, the Communication underscored the risks associated with the possible fictitious nature of the tax credits granted under such legislation, the purchase of which could serve to reinvest capital of suspicious origin (see the box 'The UIF's initiatives during the COVID-19 emergency' in Section 9.3).

3.5. Further case studies

Online trading and scams

The year saw an increase in reports regarding scams carried out by means of foreign online trading platforms – often involving complex financial products and cryptocurrencies – that offer their services to financially unsophisticated customers, sometimes without the requisite authorizations or clearances. These circumstances were also examined in light of the possible correlations with the restrictive measures taken to contain COVID-19.

In several cases, the reports give information regarding complaints filed by investors and/or inquiries on the part of investigative bodies that are particularly complex owing to the transnational nature of the phenomenon and the rapidity with which new online platforms are created.

Analyses, conducted also in cooperation with investigative bodies and with the involvement of counterpart foreign authorities, brought out contexts in which the victims, often lured with persistent online and telephone contacts from self-styled financial advisers, are induced to make payments in increasing amounts to foreign accounts attributable to the companies that manage the platforms.

The prime beneficiary companies, headquartered in different countries from those of the investors, then transfer the funds on to companies located in third countries, often by means of virtual asset service providers and payment institutions that offer high-tech services, with a view to making the flows more difficult to trace. Upon customers' requests to disinvest, the platform operators often propose that they make additional payments, justified by citing specious reasons (e.g. tax payments), and make themselves impossible to reach. Sometimes the swindled investors, seeking to recover at least part of the funds, are induced to apply to law firms that request additional outlays and turn out to be linked to suspicious platforms, thus falling victim to further frauds.

In connection with its in-depth analyses of unauthorized online trading platforms not blacked out by Consob, the Unit took organizational steps of its own to facilitate information

exchanges with Consob (see Section 7.3, 'Cooperation with supervisory authorities and other institutions').

Sports clubs

During the year the Unit received some reports of suspicious transactions involving sports clubs whose financial position, balance sheet and economic conditions were under stress in connection both with their field of business and with the persistence of the COVID-19 crisis. Analysis of the transactions brought to light phenomena implying corporate and tax crimes, misappropriation and risks of criminal infiltration.

In the situations examined, the Unit found recapitalizations decided in accordance with the dictates of civil law but carried out fictitiously: the funds contributed on the occasion of capital increases were returned shortly afterwards to the members, including through firms attributable to them or through connected third parties, resulting in a recapitalization merely in accounting terms. The equity interests in such companies were often the object of numerous transfers, between recurring actors and at short intervals, at values far from those shown in the companies' financial statements and with anomalous settlement methods (payments predating the date of sale; non-payment of one or more instalments).

The Unit frequently detected the existence of networks composed of actors (sole proprietorships and companies) connected to the beneficial owner of the sports club; these structures, through complex financial schemes apparently connected with commercial sponsorships and/or the payment of invoices, made possible, alternatively: a) a fictitious improvement in the clubs' economic and balance-sheet situation or b) the misappropriation of the funds that the clubs had received from their respective sports federations.

Finally, the analyses brought out how persistent conditions of economic and financial crisis prompted sports clubs and their beneficial owners to avail themselves of financing and sponsorship payments from firms operating in geographically distant areas and counting among their shareholders persons previously cited in penal proceedings for connections with organized crime, some of whom were then appointed to top positions in the sports clubs.

Real estate and private equity funds

In 2020, the Unit identified several cases of embezzlement from Italian or EU investment funds owned primarily by institutional investors such as pension funds, occupational pension schemes and banking foundations.

The embezzlement from real estate funds involved sales of properties at prices well below their market value as reflected in the half-yearly valuations prepared by the funds' independent appraisers. Such transactions were generally followed shortly by another transaction in which the original buyer of the property resold it to a third party at an appreciably higher price. Often, a substantial part of the capital gains realized by the original buyer was 'distributed' to various persons, including the beneficial owners and/or the top officers of the management company, the fund's asset manager or natural and legal persons connected to these individuals.

The Unit also discovered financial anomalies linked to investment funds operating in the renewable energy sector. These funds typically have exclusive ownership of limited companies which in turn own the green energy production facilities. Periodic transfers from the accounts of the limited companies, for amounts that were individually modest but significant in the aggregate, were made as payments for advisory services to companies linked, including via fiduciary mandates, to the owners and/or top officers of the fund management companies or to natural and legal persons connected to them.

Participating financial instruments

The Unit's investigations enabled it to identify some anomalous uses of participating financial instruments and debt instruments whose subscription appeared to serve for the

reinvestment of foreign funds of dubious provenance. In many cases, the instruments were issued and subscribed by firms traceable to the same persons.

In some cases of conspicuous interest, such financial instruments are issued in disproportionate amounts with respect to the issuers' economic configuration, but only a residual part is taken up, often by foreign firms that turn out to be connected to the issuers by means of individual links. Another circumstance warranting attention is that such proceeds are often practically the sole source of inflows to the issuers' bank accounts. In general, the funds raised with such instruments are then put to other uses than those that had been stated, through intra-group transfers that appear to divert them from use in the issuer's sector of operations.

Virtual assets

In the course of 2020, the Unit continued to monitor STRs regarding virtual assets and found confirmation of trends it had identified in the past. A good many reports are motivated more by the perception of the intrinsic riskiness of the instrument than by actual risks of money laundering or terrorist financing connected with transactions.

Several in-depth financial analyses conducted by the Unit, drawing also on international cooperation, shed light on the frequent association of virtual assets with illegal activities, and notably with unauthorized financial activity and scams. In fact, the demand for virtual assets as alternative investment goods, often coming from investors lacking the technical knowledge necessary to master the instrument, is associated in some cases with the unauthorized performance of restricted activities on the part of Italian and foreign persons. An analogous risk is posed by persons who act as collectors in the purchase of virtual assets, interposing themselves with respect to official exchangers or presenting themselves to the market as virtual asset service providers (VASPs) but without having adequate organizational structures to ensure customer protection or compliance with AML rules.

There were significant cases of fraud associated with virtual asset demand and supply: alongside pyramid schemes, the Unit's attention was drawn to a possible fraud perpetrated against Italian savers by means of an initial coin offering (ICO) and a possible fraud in virtual currency mining. Finally, there are numerous cases where the investment in virtual assets is made with the proceeds of criminal activities, such as computer frauds like phishing or ransomware, or where virtual asset flows are found to be directed to dark web sites for the possible purchase of illegal goods and services.

Additional analyses focused on the purchase/sale of cryptocurrencies by means of ATMs installed on the premises of Italian businesses acting on behalf of a foreign VASP. In such cases, the businesses' bank accounts show sizeable deposits of cash that are incompatible with the economic profile of the business (small retail shops), followed by cross-border transfers to the benefit of the VASP.

The emerging picture shows the difficulty of controlling so-called crypto-ATMs, given the potentially far-flung network of participating commercial establishments and the absence of both financial and AML regulations governing the service.

Pyramid scheme in the algorithms of a cryptocurrency

Again, with regard to virtual assets, some reports revealed the existence of a cryptocurrency trading platform that appeared to be running a pyramid scheme by offering financial products to the public with multi-level marketing recruitment.

In detail, the element of anomaly centred on the price of the cryptocurrency traded on the platform: the price was not determined by the normal interplay of demand and supply but was forced upwards through the application of a platform management algorithm, based in turn on supply/demand for big data and on the traffic of data generated and collected,

guaranteeing a profit from the sale. Exchanger and wallet provider services for the cryptocurrency were offered on a website whose products and contents were issued by a foreign company linked to Italian persons. The amounts paid in, mainly by natural persons for purchases of cryptocurrency, were largely used to send credit transfers to foreign natural persons and companies located at the same address, whose role in managing the cryptocurrency was not clear, possibly with a view to embezzling funds from the investors.

Payment cards

In the payment card sector, in 2020 the Unit detected a particular operating procedure, not especially complex but characterized by large amounts, used above all by criminal organizations rooted in Italy for some time and composed mainly of persons of Nigerian origin. Significant amounts of funds were laundered in Africa, the proceeds of crimes that are the hallmark of the Nigerian mafia: computer fraud, smuggling, exploitation of prostitution, and trafficking in weapons, drugs and human beings.

Compared with what it had seen in years past, the Unit found that the holders of the payment cards used are not only Nigerian nationals but fronts – in general, natural persons in situations of individual and/or social vulnerability or fragility – who, for a small fee, take out prepaid cards that are made available to the associates in Africa. From then on, the cards are recharged at bank or merchant ATMs using cash generated by the above-mentioned crimes or by means of other cards reloaded using cash. Alongside these methods of adding credit, in some cases use is made of domestic and cross-border credit transfers, most of them traceable to frauds. In a short span of time, the funds raised are withdrawn in cash and/or used at merchants in neighbouring countries of West Africa, chiefly the countries bordering the Gulf of Guinea – Benin, Togo, Ivory Coast, Ghana, Nigeria – and Burkina Faso. After that, the cards are generally extinguished by declaring they have been stolen or lost.

In 2020, the Unit investigated this phenomenon by means of an aggregate analysis of 87 suspicious transaction reports, supplemented by specific communications transmitted by the reporting entities and referring to 1,324 cards held by 1,124 different persons, for a total transaction volume of about €17 million in the period January 2019 – June 2020. The average amount transacted for each card at Nigerian POS units, those most representative of the perimeter analysed, was about €15,500, while the principal recipients of the funds were concentrated in the region of Lagos. The phenomenon is in continual expansion: the total amount in the first six months of 2020 (about €10 million) far exceeded that for the whole of 2019 (about €7 million).

Gaming and gambling

Among the principal problems to emerge in the gaming sector was the recurrence of intermingling between the persons in charge of operating points and the assets passing through those points. On multiple occasions, the Unit identified gaming accounts held by different persons with family or business ties to the person in charge of the point of sales where the accounts had been opened. The fact that the transactions on the accounts are carried out by means of the same payment instruments (chiefly prepaid cards) suggests that the gaming accounts are actually controlled by the head of the sales point and that the account-holders act as fronts.

The anomalies relating to gaming at video lottery parlours concern the collection of winning tickets for a recurring amount, frequently issued within minutes of one another, or clusters of wins realized on video lottery terminals in the same parlour by a few recurring persons, including foreigners, and with reiterated collection of the winnings in cash. In other cases, the shop manager failed, sometimes repeatedly, to fulfil the obligations of customer due diligence, and at times the signatures on the identification forms did not match the documents used to identify the players. There are many instances of bets for amounts just under

the identification threshold, and nearly all the customers on whom due diligence is performed have been reported multiple times to the UIF, especially by gaming and gambling sector operators.

The Unit also encountered cases, probably traceable to a single nexus of interest, of winning tickets bet within a very short span of time on the same sports events at the same sales point, with the winnings collected in cash. Among the anomalies most commonly found is the repetition of the transaction at multiple betting halls (including in provinces other than those of residence of the gambler) or on multiple websites, repeated opening and closing of accounts by the same persons, the use of debit accounts held by third parties (some of them implicated in investigations on irregular bets).

In online gaming, along with the familiar scheme of topping up gaming accounts using stolen or cloned payment cards and with collusive practices such as chip dumping and best-hand play, the Unit found several cases of betting accounts being used as non-bank deposits (sometimes with the temporary self-exclusion of the holder). In fact, betting accounts are not among the accounts that have to be declared to the Registry of Accounts and may thus be a way to shield funds from tax assessments or seizures. Similarly, there are cases of large amounts of cash being paid into online gaming accounts within a circumscribed period by individuals with positions in companies of the gaming and gambling sector who have already been reported by banks for transactional anomalies on personal accounts and prepaid cards.

In parallel, the STRs convey a picture of a growing use of prepaid cards in cases of suspected unauthorized collection of bets by individuals officially registered as students or unemployed, some of them recipients of the 'minimum income' benefit, or active in the past in the gaming sector or owners of Internet points. These persons operate as collectors, gathering, by means of recharges to prepaid cards, credit transfers and cash deposits, a cumulatively significant sum of individually small amounts that is then employed on online gambling sites. The operations of collectors present evident risks of money laundering in that they determine an interposition that prevents gaming service providers from knowing the beneficial owner of the amounts employed.

4. COMBATING THE FINANCING OF TERRORISM

Analysis of suspicious transaction reports relating to terrorist financing proceeds through the same operational phases as analysis of money laundering reports. However, given that the suspicion concerns organizations or persons that could plan and carry out terrorist attacks, first-level analysis of the reports plays a crucial role and is conducted with the utmost speed so as to share their contents promptly with the investigative bodies.

The examination of terrorist financing STRs, in which the subjective element of the actors involved carries fundamental weight, aims at reconstructing the network of interpersonal and financial links using methods appropriate to the operational peculiarities of the contexts in question: the Unit employs network analysis techniques to identify high-risk individuals and transactions on the basis of the recurrence of operational patterns already associated with the financing of terrorism in previous financial analyses or investigations. It shares the results with the investigative bodies in the customary form of technical analysis.

For some time now, the terrorist threat in European territory has been largely unconnected with the military vicissitudes of the so-called Islamic State in the Mideast, manifesting itself in improvised and unpredictable actions often carried out by 'lone wolves' who act on their own, having espoused the jihadi ideology following self-indoctrination via the Internet. These attacks, limited to the initiative and individual resources of their perpetrators, are characterized by their low technological and organizational level, which makes preventing them materially and financially more difficult.

On the whole, in 2020 the terrorist threat was also weakened by the prolonged period of restrictions connected with the pandemic, which naturally made it harder for potential attackers to move around and reduced the suitable opportunities for attacks. It is no coincidence that the terrorist attacks in Nice and Vienna took place at a time when the restrictions in response to the second wave of COVID-19 had yet to be applied. Both attacks displayed ties with Italy, based on which the UIF immediately undertook a wide-ranging reconnaissance of the information in its possession and activated every form of cooperation with the DNA and the investigative bodies.

4.1. Suspicious transaction reports

The Unit received 513 reports of transactions suspected of terrorist financing in the course of 2020 (0.5 per cent of all the STRs it received during the year), with a reduction of about a third compared with 770 in 2019 and half compared with 1,066 in 2018.

Examining the flow of terrorist financing STRs in the five years 2016-2020, which saw the rise and then the progressive retreat of the Islamic State and the spate of terrorist attacks it inspired, one sees a peak in 2017-18 followed by a decline, which also reflects obliged entities' diminished perception of the threat (Figure 4.1).

The breakdown of terrorist financing STRs by type of reporting entity shows the predominance of banks and financial intermediaries (98.8 per cent), with money transfer agents in the lead (39.4 per cent), followed by banks and Poste Italiane SpA (33.9 per cent) and

electronic money institutions (24.0 per cent). The share attributable to non-financial entities dwindled further to less than 2 per cent.

Figure 4.1

Terrorist financing reports received

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

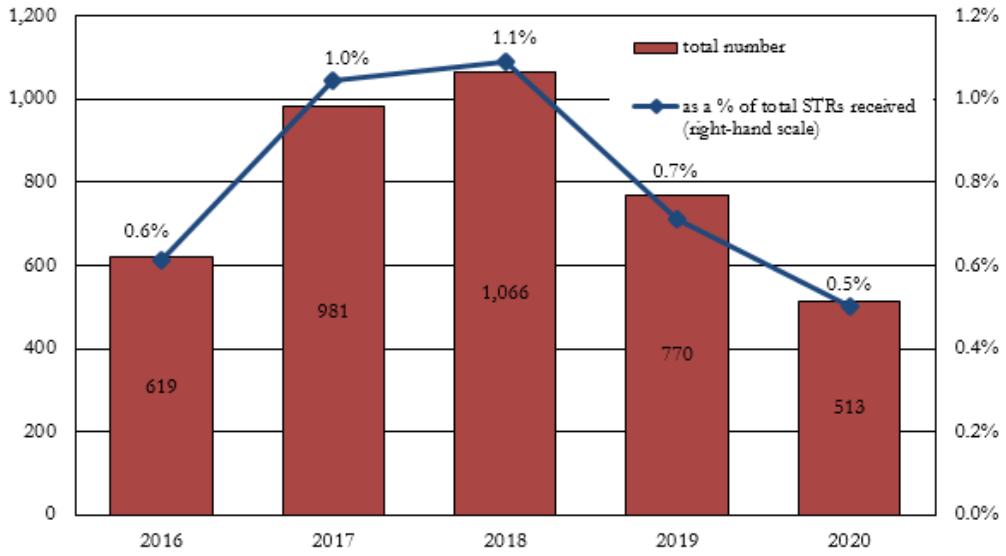


Table 4.1

Terrorist financing reports by type of reporting entity

	2019		2020	
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*
Banking and financial intermediaries	**736**	**95.6**	**507**	**98.8**
Payment institutions and contact points	378	49.1	202	39.4
Banks and Poste Italiane SpA	267	34.7	174	33.9
EMIs and contact points	72	9.3	123	24.0
Other (1)	19	2.5	8	1.6
Non-financial obliged entities	**34**	**4.4**	**6**	**1.2**
Notaries and Nat. Council of Notaries	14	1.8	5	1.0
Other (2)	20	2.6	1	0.2
Total	**770**	**100.0**	**513**	**100.0**

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

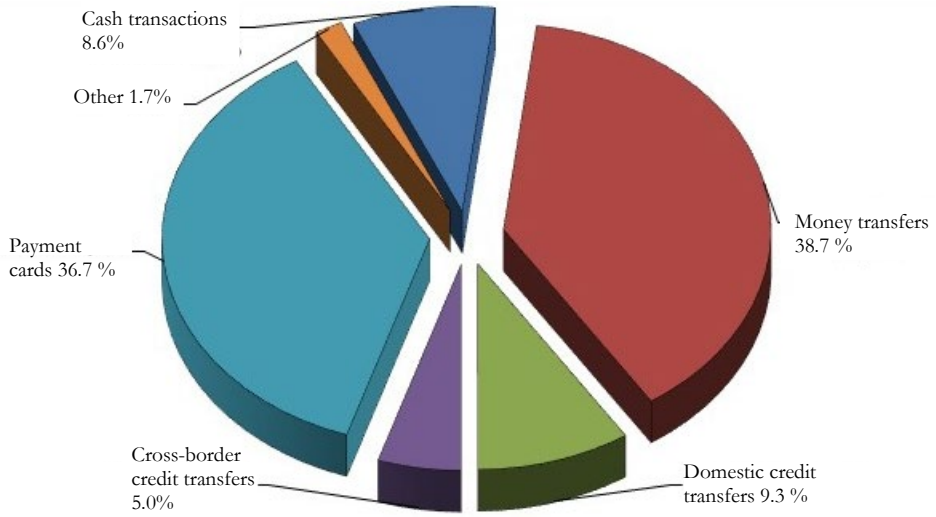
The 513 reports refer to a very large number of transactions (nearly 56,000). This is partly due to the significant number of money transfer and payment card transactions, the latter up sharply from the previous year. The remaining transactions reported consist of domestic credit transfers (9.3 per cent), cross-border credit transfers (5.0 per cent) and movements of cash (8.6 per cent, down from 27.0 per cent in 2019; Figure 4.2).

The attention paid by obliged entities appears to reflect the new landscape that features the ebbing of some phenomena closely linked with the situation in the Middle East; the transactions potentially attributable to the conduct of foreign fighters or returnees (purchases of specific items, expenditures for travel to areas at risk, loans to third parties, asset liquidations) were in fact less frequently the trigger for STRs than in the previous year. On the other hand, there was an increased perception of the risk relating to some anomalous financial networks composed of foreign individuals in the most exposed sectors (money transfer agents and payment cards).

Figure 4.2

Technical forms of terrorist financing transactions reported (1)

(*percentage shares of transactions reported*)



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

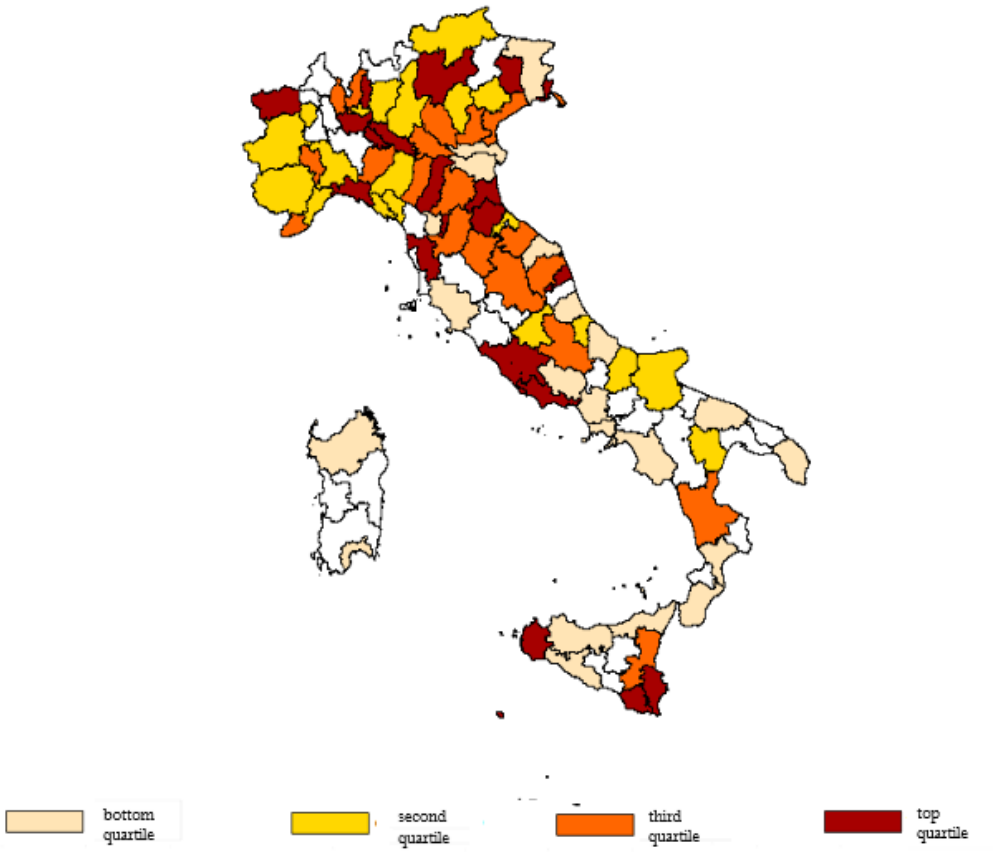
Geographical distribution

The geographical distribution of the reports, though broadly in line with that of 2019, shows a further concentration around four main areas: (a) the regions of northern Italy, in particular the metropolitan city of Milan and the adjacent provinces; (b) central Italy, especially Rome and Latina; c) the coastal provinces of western Sicily (Trapani) and eastern Sicily (Ragusa, Siracusa, Catania); (d) the border zones from east (Trieste, Gorizia) to west (Imperia, Aosta), passing through northern Lombardy (Varese, Como, Lecco; Figure 4.3). This may reflect a different perception of the risk associated with immigration in Italy, particularly in those areas – specified at points (a) and (b) – with the greatest concentration of immigration, partly in response to economic opportunities or as a result of the previous establishment of foreign communities originating from the areas abroad linked to jihadism in various ways. The high percentages recorded in areas (c) and (d), instead, might signal the more acute perception of risk profiles connected with the transit of migratory flows.

Figure 4.3

Terrorist financing reports received by province

(number of reports per 100,000 inhabitants)



4.2. Types of transactions suspected of financing terrorism

In a pattern quite like that of 2019, the STRs on suspected terrorist financing divide into two macro-categories based on the triggering element: in the first category, the suspicion derives purely from the parties' links with religious radicalism; in the second, still numerically marginal, the significant element consists in transaction characteristics which, partly on the basis of the indicators published by the UIF, suggest possible financing of terrorist organizations or activities.

More and more frequently, the transactions reported in all the areas described above take the form of networks for the transfer of money among multiple parties by means of money remittances, card top-ups or bank credit transfers. The reconstruction of these networks, thanks in part to integration with the information already in the Unit's possession, can make a decisive contribution to combating the phenomenon, by discovering links with terrorist organizations or identifying operational schemes already found in financial analyses or in law enforcement investigations that have turned up episodes of functional or instrumental contiguity with the financing of terrorism.

Practically all the reports in which the suspicion involved non-profit entities were submitted by banks. These reports diminished in number by about 30 per cent with respect to

2019, in keeping with the overall trend, and so remained relatively stable at 6-7 per cent as a share of total terrorist financing STRs (Table 4.2). A factor in the decline may have been the diminished perception of a risk of distorted use of funds collected for humanitarian assistance to the populations caught up in the conflict with the so-called Islamic State, as well as the consideration of the limited extent of these associations' involvement in organizing the isolated attacks that are now the main form taken the jihadist threat in Europe.

Table 4.2

Reports on non-profit religious entities (1)

	2016	2017	2018	2019	2020
Number of reports	125	81	71	54	38
As a percentage of the total reports classified as financing of terrorism	16.8	7.3	6.0	6.5	6.9

(1) The number and percentage share include STRs originally filed on grounds of suspicions of money laundering.

4.3. The UIF's analyses

With the types of reports of suspected terrorist financing remaining broadly stable, the UIF decided to exploit the full potential of the techniques already applied to money transfer circuits by extending them to payment cards.

The reason for this extension of scope[5] lies not only in the increased number of terrorist financing reports sent by electronic money institutions, but also in the enhanced content of such reports following the information campaign that the UIF conducted in 2019 on the use of the new reporting procedures, similar to those already employed for money transfer agents. The leading issuers of payment cards responded to the Unit's prompting by broadening the contexts reported and the information associated with them, particularly as regards the financial counterparties and the completeness of the related individual data.

The greater number of individuals named in STRs, together with the wide distribution of payment cards, produced an increase in the matches identified by the name matching algorithm. Overlap between segments of the customer base of electronic money institutions and of money transfer circuits (who rarely have bank accounts) resulted in immediate integration into the analysis of the transactions respectively reported, especially when weblike features on both sides made it possible to link seemingly unconnected contexts through network analysis techniques. Thanks to the greater information potential of payment card transactions, the reduced margins of doubt as to the identification of customers with persons of the same name connected in various ways with terrorism helped in the discovery of network 'critical nodes' and the acquisition of further information from obliged entities, from the databases at the Unit's disposal and from cooperation with foreign FIUs.

[5] Prompted in part by the assignment of the tasks of analysis to the Special Sectors and Anti-Terrorist Financing Division set up at the beginning of 2020 (see Section 10.1, 'Organizational structure').

Analysis of the terrorist financing STRs sent by money transfer agents

In the course of 2020, the Unit carried out a detailed analysis of the reports of transactions suspected of involving the financing of terrorism submitted by money transfer service providers, with a view to identifying recurrent features and interpreting them against the backdrop of the trends recorded for all STRs of this type. The study covered the five years 2016-20 (the period following the onset of terrorist attacks in 2015) and the introduction of the new massive reporting procedure for money transfer service providers, so as to ensure uniformity with reference both to the phenomenon under observation and to the available dataset for each transaction reported. The dataset for the analysis comprised 1,572 STRs referring to 69,324 transactions.

For the STRs sent by money transfer agents, the results were generally in line with the findings for the totality of reporting entities set out in Section 4.1 regarding the relationships between perceived risk and migration/immigration:

- by a wide margin, the prevalent trigger for the reports is personal identity (names of interest for Italian or foreign investigative bodies). In such cases, the reporting entity focuses on reconstructing the network of counterparties, which usually has a complex structure (many-vs.-many: 55 per cent) and less frequently hinges on a single individual (one-vs.-one/many: 45 per cent);
- in keeping with the position of Italy, which is almost exclusively a country from which the financial flows originate, the proportions of the total volumes reported as sent and received are 70 per cent sent and 30 per cent received (compared with 78 and 22 per cent, respectively, for money transfer agents' money laundering STRs) and remain roughly stable over the five years considered;
- the distribution of the total amounts received or sent, considering the countries of provenance and destination of the funds or of origin of the customer and counterparty, shows four prevalent geographical areas: North Africa, the Middle East, Central Africa and the Balkans;
- the analogous distributions by Italian province sending or receiving the funds are essentially concentrated in the parts of Italy identified in Section 4.1.

This analogy confirms how much the activity of the networks financing or supporting terrorism tends to blend in with the trafficking of migrants and consequently, how complicated it is to intercept and extract specific elements of anomaly.

The improvements in analysis were accompanied by a further enhancement of the Unit's cooperation with the DNA and the investigative bodies. In 2020, cross-checks of the personal ID data contained in the terrorism reports with the DNA's databases signalled matches for about 25 per cent of the reports received, contributing significantly to the process of selection and financial investigation, which resulted in feedback showing investigative interest for about 47 per cent of the 561 reports that the Unit transmitted to the investigative bodies during the year.

The quality and promptness of information exchanges with the DNA and the investigative bodies proved fundamental in connection with the attacks carried out in Europe by lone wolves in the course of 2020. On those occasions, on the basis of the financial traces contained in the STRs or brought to light by examination of the funds movements retrievable

from the Registry of Accounts, the Unit was able to expand the network of persons connected to the attackers and identify those whose transactions indicated possible involvement in organizing or financing them.

4.4. International activities

The Unit contributes to the projects underway at international level. In particular, the use of virtual assets to finance terrorism and the possible weaknesses in intercepting the related illegal flows are being studied, as are the interconnections between arms trafficking and the financing of terrorism. The new presidency of the FATF has indicated the fight against the financing of terrorism linked to racial or ethnic discrimination as a priority project.

In the European sphere, action to combat the financing of terrorism proceeded under the Action Plan adopted by the European Commission in 2016. The lines of action laid out include strengthening cooperation among competent authorities (especially the FIUs) and eliminating forms of anonymity in financial transactions.

The Counter-ISIL Finance Group of the Global Coalition against Daesh, in which the UIF participates, continued its work. The Group further updated its information on ISIL's possible sources of finance at global level, which today mainly take the form of abductions, illegal trafficking of antiquities and flows of funds from third countries. In its most recent meetings, the Group underscored that ISIL no longer has a territorial dimension but continues its propaganda campaign to win recruits and still conducts organized operations through its affiliates in Africa and South-East Asia.

As part of the Egmont Group's ISIL Project to study the financial support of foreign fighters, a group of FIUs, including the Unit, continues to conduct multilateral information exchanges on persons and activities potentially of interest, based on a broader set of indicators than outright suspicions.

In 2020, the Unit received 105 requests and spontaneous communications from foreign FIUs regarding terrorist financing; 14 of the communications referred to networks of remittances, especially via the Internet, by possible facilitators of terrorists. In a few cases, the communications received from abroad also regarded persons linked to domestic subversive terrorism. A significant share of the exchanges concerned cross-border reports sent by a European FIU. The Unit's requests concerning terrorist financing were addressed mainly to European FIUs.

5. CONTROLS

5.1. Inspections

The UIF's contribution to preventing and combating money laundering and the financing of terrorism includes on-site inspections of the obliged entities. Inspections check compliance with the reporting and communication requirements and acquire data and information on specific transactions or financial activities that are deemed to be significant in terms of size and risk.

Inspection planning takes account of the degree of exposure to the risks of money laundering and terrorist financing of the different categories of obliged entity and of the control measures taken by the other authorities responsible for checking compliance with the AML/CFT provisions. General inspections assess the efficacy of active cooperation, in part by analysis of the procedures for reporting suspicious transactions; targeted inspections are directed at reconstructing specific financial movements, supplementing the information obtained in the analysis of STRs or from foreign FIUs, or examining matters that have emerged in the framework of cooperation with the judicial authorities, investigative bodies and sectoral supervisory authorities. Through this direct interaction with the obliged entities, moreover, the UIF also seeks to intensify their active cooperation, enhance their ability to identify suspicious transactions and improve the quality of their reporting contribution.

In 2020, the UIF performed general inspections of one Italian bank and two branches of EU intermediaries (a bank and an electronic money institution) and wound up 12 inspections that it had begun in 2019. The number of inspections, down significantly from the previous year, showed the effects of the restrictive measures taken in the first months of the pandemic and of the social distancing rules subsequently imposed by the governmental authorities in order to limit the spread of COVID-19 (Table 5.1). These measures resulted in the interruption of all on-site activity on the part of the supervisory authorities from February onwards.

Table 5.1

Inspections

	2016	2017	2018	2019	2020
Total	**23**	**20**	**20**	**21**	**3**
Banks	8	4	8	15	2
Trust companies	4	4	3	1	-
Payment institutions, EMIs and other financial intermediaries	3	3	2	2	1
Asset management companies and securities investment firms	1	-	4	-	-
Insurance companies	-	6	-	-	-
Other entities (1)	7	3	3	3	-

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

COVID-19 health emergency

In light of the emergency conditions, the Unit completed the inspections already begun by making ample use of remote communication techniques in its dialogue with the entities inspected, reducing the physical presence of inspectors to a minimum. The persistence of

the pandemic has led the Unit to consider alternatives to the traditional inspection procedures, making use of innovative modes of interaction with the entities subject to the requirements of active cooperation. To this end, it is experimenting with new procedures for performing checks, involving a substantial reduction in the duration of inspectors' on-site presence (so-called delocalized inspections) and reliance on off-site controls featuring more intense remote interaction with the obliged entities.

The UIF's inspection teams were supplemented by personnel from other units of the Bank of Italy; likewise, a UIF staff member took part in an anti-money laundering inspection carried out by the Bank's Directorate General for Financial Supervision and Regulation. The UIF and the Directorate General implemented the procedures to facilitate reciprocal transmission of information in support of the AML/CFT controls under way, in order to respond to specific needs for information regarding the entity under inspection.

The inspections carried out at the branches of EU intermediaries confirmed shortcomings in some important respects, specifically: absence of automated profiling of customers during onboarding; deficiencies in monitoring transactions with counterparties located in countries at risk; internal rules not well calibrated to Italian conditions and contradictory as well in some matters; absence of autonomous safeguards for selecting the anomalous transactions to be assessed for the possible transmission of an STR. In addition, adequate consideration was not given to the significant risks of money laundering associated with transactions at ATMs, both in relation to the large total quantity of cash moved, mostly without predetermined limits on withdrawals, and with regard to the types of merchants on whose premises the machines are installed, some of them operating in sectors at risk.

Independent ATMs

The UIF has begun inspections to probe more deeply into the transactions carried out on automated teller machines operated by non-banks, so-called independent or IAD (independent ATM deployer) ATMs.

Machines of this kind are increasingly widespread in Italy. In addition to offering cash withdrawal services by means of cards issued by intermediaries belonging to the major payment circuits, they also allow customers to make cash deposits and to buy or sell virtual currencies for cash.

The absence of limits on the total amounts that can be withdrawn also by means of successive transactions, the placement of the machines on the premises of non-financial operators with high money laundering risk, the possibility of providing deposit and withdrawal services jointly and thus allowing forms of recirculation of cash, heighten the risks of money laundering connected with the activity of independent ATMs.

In addition, there are regulatory uncertainties. The PSD2 Directive on payment services in the internal market appears to permit the disbursement of banknotes to be performed also by entities not subject to supervision, provided they do not jointly perform one of the payment services envisaged by the directive. The presence of unregulated managers can increase the risk of the use of banknotes of illicit origin if there is collusion between the owner of the ATM and criminals. Furthermore, since these managers are not subject to the AML/CFT obligations or to forms of disclosure to the competent authorities, the activity would be carried out without any form of monitoring whatsoever.

Problems also arise when the service is provided by foreign intermediaries operating in Italy without a branch, under the freedom to provide services. Reconstructing the financial flows handled by such intermediaries, even though they are subject to home country AML/CFT regulations, may be difficult when the information exchanges with the competent national authorities are not straightforward.

This situation has induced the UIF to advocate a flexible interpretation of the current provisions of Legislative Decree 231/2007 according to which operating in another EU country with an extensive network of ATMs should be considered a form of 'establishment without a branch', with Italian requirements consequently applicable to EU intermediaries that carry on such activity under the freedom to provide services; this would be consistent with what the EBA has already foreseen in cases of high AML/CFT risk.[6]

Naturally, the requirements would have to be calibrated in relation to the limited data available on users. Since the cash withdrawals are occasional, the managers only have some data referring to the transaction itself, but they cannot trace the identity of the user, nor do they have access to the debit item written to the underlying bank account or payment card.

Additional risk profiles are discerned in the operations of ATMs enabled to convert virtual currencies into cash. In purchases of cryptocurrency, the transactions could be used systematically to introduce cash of illicit origin into the financial circuit; and in sales of cryptocurrencies, the stock of banknotes to be withdrawn from the ATMs could derive from criminal activity. The two kinds of transaction can be combined if the ATMs' technical specifications permit the recirculation of cash.

These risks are attenuated insofar as the ATMs belong to virtual asset service providers, since they are subject to the anti-money laundering rules.[7] Where the conversion of virtual currencies into cash is done directly by foreign VASPs that engage in business in Italy remotely, the control and enforcement problems are the same as in the case of independent ATMs executing transactions in legal tender that are managed directly by EU intermediaries under the freedom to provide services.

The inspections at entities providing virtual asset exchange services and the banks where they have accounts were completed in the course of 2020.

The inspections confirmed the risks of the anomalous use of virtual assets for money laundering or terrorist financing, given the scope for carrying out basically anonymous and hard-to-trace transactions, which are de facto impediments to reconstructing the transfer of funds.

[6] See the *Report* of 29 October 2019 on potential impediments to the cross-border provision of banking and payment services. Referring to the minimum harmonization approach that characterizes the Fourth AML Directive, the EBA specified that the Member States may take additional steps to mitigate money laundering risk and, among other measures, also extend host country requirements to intermediaries making use of the free provision of services.

[7] See Legislative Decree 231/2007, Article 3(5)(i).

Inspections of virtual asset service providers

The virtual asset sector in Italy is highly concentrated: the first four virtual asset service providers (VASPs) cover about three quarters of the market. Each of these four companies (three foreign and one Italian) operates a centralized platform on which their customers' numerous orders to buy or sell virtual assets are matched.[8] Besides managing the platform, they offer an array of additional services, including virtual asset exchange, transfer, deposit and withdrawal and wallet provider services.

Other VASPs operating on the market provide a limited range of services. These legal persons, often established as limited liability companies with minimal capital, avail themselves of the platforms mentioned above in order to obtain the virtual assets that they require for their activity.

In 2020, the Unit concluded inspections of two VASPs.[9] Included within the perimeter of the inspections were three supervised intermediaries with which the VASPs held their accounts for the management of legal tender currency. In addition, during the targeted checks performed at two significant banks, special attention was paid to transactions in virtual assets.

The inspections of the VASPs found small-scale organizational structures with minimum capital endowment; the principal services they offer include conversion of legal tender into virtual currencies (and vice versa), transfer or exchange of digital assets and their conservation in digital wallets. Warranting particular attention for AML/CFT purposes is the service of buying and selling virtual assets for cash by means of ATMs.

From the operating standpoint, what has emerged is the growing interconnection between services offered by VASPs and those provided by supervised intermediaries, based on commercial agreements that make the use of virtual assets available to the customers of the latter.

The inspections carried out by the Unit brought to light some weaknesses in the safeguards adopted both by the VASPs and by the supervised intermediaries in order to mitigate the risks of money laundering or terrorist financing in relation to transactions in virtual assets. The critical observations refer to: i) scant attention in customer profiling and shortcomings in the automatic transaction monitoring systems with regard to transactions carried out with virtual assets; ii) failure to perform checks on third parties to which AML compliance may have been outsourced; iii) the inefficacy of the organizational safeguards in place for the service of virtual asset purchases with payment cards; iv) the problems of the supervised intermediaries in monitoring the transactions of their own customers (including VASPs) in virtual assets.

Moreover, the inspections by the UIF also turned up the presence of numerous natural persons, so-called collectors, who use accounts with the VASPs for conversions of virtual assets on behalf of third parties where they promote virtual asset trading. In the most significant cases, the transaction volumes mediated by the collectors are such as to suggest that

[8] By contrast, on decentralized, peer-to-peer platforms, which are numerically less important, the transactions are set up without the intervention of a party that collects the customers' orders.

[9] In 2019, the UIF performed an inspection at the branch of an EU electronic money institution whose main customer was an Italian company that manages an important virtual asset exchange platform (see UIF, *Annual Report for 2019*, p. 63).

they operate in a professional capacity, most likely without an adequate organizational structure and without respecting the AML rules.

In the context described above, inspection activity suffers from the persistent weaknesses of the regulatory framework, which have been brought to the attention of the Ministry of Economy and Finance and of the Bank of Italy's Directorate General for Financial Supervision and Regulation (see the box 'Regulatory initiatives on virtual assets', in Chapter 9).

Following the inspections conducted during the year, including those at the VASPs, the Unit communicated the results to the supervisory and control authorities for the matters within their respective competence, including the Bank of Italy, the Special Foreign Exchange Unit of the Finance Police, the Customs and Monopolies Agency and the Ministry of Economy and Finance.

The entities inspected were informed of the shortcomings found and were urged to take the necessary corrective measures. In addition, steps were taken for sanctions, including jointly with the Bank of Italy's Directorate General for Financial Supervision and Regulation, with regard to the administrative violations ascertained in the matters of competence.

With reference to some inspections concluded in 2020, the Unit also exchanged information with the judiciary regarding possible criminal offences and, in one case, with the FIUs of the countries involved in the analysis of the suspicious financial flows.

5.2. Sanction procedures

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

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

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

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

Information exchanges and coordination with the authorities

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

To this end, exchanges have intensified for the joint examination of possible violations of AML legislation and for reciprocal communication of the steps taken. There are now well-

established practices between the UIF and the Bank of Italy's Directorate General for Financial Supervision and Regulation for systematic reciprocal participation in their respective collegial bodies responsible for assessing irregularities.

On the basis of the inspection reports that the Unit transmitted in 2020, the Directorate General determined in two cases that there had been violations of the provisions of Legislative Decree 231/2007 and instituted the sanction procedure within its competence.

Cooperation with CONSOB proceeded, with the customary information exchanges on possible failures to report suspicious transactions found during inspections and possible cases of market abuse. The communications transmitted by the UIF also regarded possible cases of unauthorized banking and financial activity, including transnational activity, and online trading scams to the detriment of private investors, in some cases in virtual assets. In addition, CONSOB was informed of possible irregularities in the management of a pension institution's investments on the part of an asset management company; the same operations were also the subject of a communication to the competent judicial authority.

In 2020, the inspection of an audit firm undertaken by the UIF at the behest of and in close coordination with CONSOB was concluded; information was exchanged on the problems found during the inspection, which were also the subject of a joint action letter sent to the inspected firm.

Given the increase in information exchanges, the Unit, in order to enhance the efficacy of the system of sanctions, undertook some initiatives in concert with the other authorities empowered to ascertain irregularities with regard to active cooperation. In particular, in the early months of 2021 a virtual seminar was organized with the participation of representatives of the Bank of Italy's Directorate General for Financial Supervision and Regulation, the Finance Police, the Ministry of Economy and Finance, and a magistrate of the Court of Cassation. The seminar engendered a shared perception of the need to strengthen coordination among the authorities involved.

During the year, the UIF initiated 12 administrative sanction proceedings for failure to report suspicious transactions, as ascertained in inspections (Table 5.2); in one case, there were violations of the obligation to transmit SARA aggregate data. A proceeding was initiated against a virtual asset service provider for violation of Article 49(1) of Legislative Degree 231/2007, with reference to cash deposits, each of an amount above the legal threshold, made by customers at ATMs managed by the inspected party for exchanges between legal tender currency and virtual assets. The violations notified to the persons concerned were transmitted to the MEF for the possible imposition of sanctions.

Table 5.2

Administrative irregularities

	2016	2017	2018	2019	2020
Failure to report a suspicious transaction	17	17	8	18	12
Failure to transmit aggregate data	1	-	1	1	1
Violations of Art. 49 (1) of Legislative Decree 231/2007	-	-	-	-	1
Failure to declare a gold transaction	5	5	26	28	12
Failure to freeze funds and economic resources	8	5	-	-	-

Sanction proceedings on gold transfers

In 2020, the Unit sent the MEF documentation bearing on the investigation conducted as part of 12 sanction proceedings regarding gold transfers. In six cases, the charge of violation was notified in relation to cross-border transactions, some of them under the voluntary disclosure procedure. The MEF agreed with the Unit's reading and imposed the consequent pecuniary administrative sanctions, also in a case of late filing of a gold declaration.

COVID-19: suspension of time limits

The suspension of time limits enacted during the COVID-19 emergency[10] applied both to the administrative proceedings initiated by the UIF following its ascertainment of violations of regulatory requirements and to proceedings in which the Unit has investigative powers. The Unit took organizational measures to safeguard the principles of efficiency, effectiveness and reasonable duration of administrative proceedings, also with reference to the petitions filed by the interested parties.

[10] The suspension period, from 23 February to 15 April 2020, was introduced by Decree Law 18/2020 and then extended to May 15 by Decree Law 23/2020.

6. STRATEGIC ANALYSIS

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

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

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

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

6.1. Aggregated data

SARA reports are submitted monthly by financial intermediaries and derive from the aggregation of data on their transactions in accordance with criteria laid down by a UIF Measure. The data received through December 2020 cover all transactions carried out by customers for amounts (in a lump sum or split up) of €15,000 or more.

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

In August 2020, the UIF issued a new 'Measure' (only in Italian) governing the production and transmission of SARA reports.

The Measure, which applies starting with the reports for January 2021, takes account of the main changes introduced by primary and secondary legislation, including: the extension of the anti-laundering reporting obligations to SICAFs, points of contact of EU payment service providers and electronic money institutions; the lowering of the transaction reporting threshold from €15,000 to €5,000; and the elimination of the requirement to report split

transactions and certain specific types of information. The Measure also made new provisions to increase the information content of the data transmitted to the UIF (see Section 9.3, 'Secondary legislation').[11]

Within the SARA database, cash transactions provide some of the most significant information for the prevention of 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 transaction (such as securities trading and issues of certificates of deposit).

SARA data

The total value of financial transactions reported to the UIF via SARA aggregate data exceeded €80 trillion in 2020 (Table 6.1), an increase of 29.6 per cent compared with 2019. The increase was largely attributable to reports of transactions between intermediaries that began to be filed starting in the second half of 2019. The new SARA Measure clarified that these transactions should not be reported. The number of records sent dipped to 105.9 million, while the number of underlying transactions rose to 369.3 million.

Table 6.1

Aggregate anti-money laundering reports (SARA reports)

TYPE OF INTERMEDIARY	**Number of reporting entities in the year**	**Number of records** (1)	**Total amount** (*billions of euros*)	**Number of underlying transactions**
Banks, Poste Italiane and CDP	496	100,553,667	79,736	340,377,481
Trust companies under Law 1966/1939	199	42,793	22	149,876
Asset management companies	221	1,378,292	210	6,255,769
Financial intermediaries under Article 106 of the TUB	210	1,438,173	326	5,100,246
Investment firms	132	201,219	104	4,796,836
Insurance companies	72	1,355,278	134	2,569,280
Payment institutions	64	693,741	32	7,905,615
Electronic money institutions	13	170,387	47	1,641,754
Trust companies under Article 106 of the TUB	35	115,361	85	517,926
Total	**1,442**	**105,948,911**	**80,696**	**369,314,783**

(1) SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 12 March 2021.

[11] For instance, the Measure introduces new, aggregate payment details for money remittances and new, composite sectors for the classification of customers; at the same time, it excludes from aggregation, under certain circumstances, transactions with customers constituted by banks or other financial intermediaries.

The slight decline in the number of reporting entities, from 1,453 to 1,442, reflected decreases in the number of banks, trust companies and insurance companies (down by 24, 9, and 2 respectively) and limited increases in those of asset management companies, investment firms, payment institutions, and electronic money institutions. Banks continued to account for the preponderant share of the data sent (94.9 per cent measured by the number of records and 98.8 per cent by amount).

After banks, whose SARA reports increased over the previous year by more than 30 per cent in terms of value, the largest increase in the amounts reported was registered by EMIs (from €18 billion to €47 billion). This rise was due chiefly to one EMI's purchase of the merchant acquiring unit of a bank.

In 2020, the total value of cash transactions reported came to €158 billion, representing a decrease of 20.8 per cent from the €200 billion reported in 2019. This sharp drop, due largely to the contraction in economic activity in connection with the COVID-19 epidemic, involved both cash deposits and withdrawals, which fell by 20.5 and 24.7 per cent, respectively to €149 billion and €9 billion.[12]

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

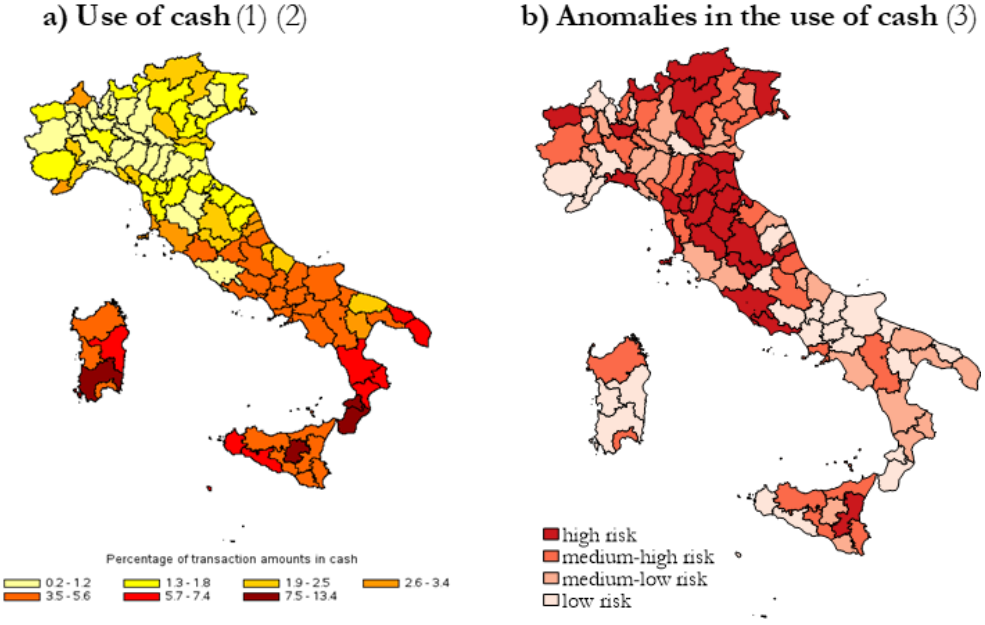
Anomalies in the use of cash

The overall intensity of the utilization of cash as reported to the Unit is highly polarized geographically (Figure 6.1a): generally low in the provinces of the Centre and North, higher in those of the South and Islands.

[12] The total for the aggregate reports is less than that derived from threshold-based communications (€215.5 billion – see Section 1.4, 'Threshold-based communications') because of the difference in the reporting threshold (€15,000 for the former, €10,000 for the latter).

Figure 6.1

Use of cash and anomalies, by province
2020



(1) Share of cash transactions in total transactions. – (2) For uniformity with the preceding years, the SARA data used do not include the transactions of general government or of financial and banking intermediaries resident in Italy, in the European Union or in countries considered equivalent by the MEF Ministerial Decree of 10 April 2015. The SARA data are subject to rectification by the reporting agents; the data used in this chapter are updated to 12 March 2021. – (3) Preliminary results. The target variable (use of cash) is updated to 2020, some explanatory variables only to 2019 or 2018 (the last years available as of March 2020. The shadow economy, at municipal level, is measured as a share of the under-declaration of value added estimated by Istat.

This difference can be ascribed to socio-economic and financial factors, such as preferences for given payment instruments, disparate spending habits and unevenness in the local availability of financial services. By means of an econometric analysis developed at the Unit, the portion of possibly anomalous cash transactions - hence symptomatic of illegal conduct - is identified in cases of systematic inconsistency with the local financial and socio-economic fundamentals.[13] The geographical distribution of the incidence of such anomalies portrays the risk associated with the use of cash (Figure 6.1b). Again in 2020, the risk of money laundering in connection with the use of cash was greater, on average, in the central and northern provinces. In these districts, where the use of cash is nevertheless less intensive than in the rest of Italy, the opportunities for investment are greater, in illicit as in lawful economic activities.

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

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

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

Cross-border credit transfers

The total value of credit transfers to and from foreign countries also declined in 2020, falling by 8.2 per cent from €2,823 billion to €2,591 billion. The reduction involved both inward transfers, which diminished by 8.6 per cent from €1,469 billion to €1,343 billion, and outward transfers, which decreased by 7.8 per cent, from €1,354 billion to €1,248 billion (Table 6.2).

Table 6.2

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

Outgoing	Amount (*billions of euros*)	Incoming	Amount (*billions of euros*)
Total	**1,248**	**Total**	**1,343**
To EU countries	**1,021**	**From EU countries**	**1,081**
United Kingdom	250	United Kingdom	263
France	222	France	233
Germany	205	Germany	215
Belgium	87	Belgium	90
To non-EU countries	**227**	**From non-EU countries**	**261**
United States	86	United States	95
China	18	Russia	13
Serbia	12	Serbia	13
Turkey	7	China	9
***of which*: tax havens**	**60**	***of which*: tax havens**	**71**
Switzerland	36	Switzerland	44
Hong Kong	10	Hong Kong	6
Singapore	3	Principality of Monaco	4
Taiwan	2	Abu Dhabi	4

(1) See Figure 6.1, note 2.

The distribution of credit transfers by counterparty country reflects that of Italy's foreign trade, with an attendant concentration of flows to and from Italy's main trading partners, especially the other members of the European Union. In 2020, the flows to these countries contracted by 6.2 per cent and incoming transfers from them by 7.5 per cent. The contraction of total flows with non-EU countries was even sharper: 13.6 per cent. As for the main non-EU countries, the volume of credit transfers to and from the United States shrank by €13 billion, while outgoing transfers to Turkey diminished by €14 billion. Not following the trend were Russia (with a slight increase in credit transfers to Italy) and China (with substantially stable flows).

Flows with tax havens

Inflows and outflows in respect of tax havens and non-cooperative jurisdictions displayed a marked decrease of 26.8 per cent, more pronounced for outgoing than incoming transfers (which dropped by 29.4 and 24.5 per cent respectively).[14] Compared with 2019,

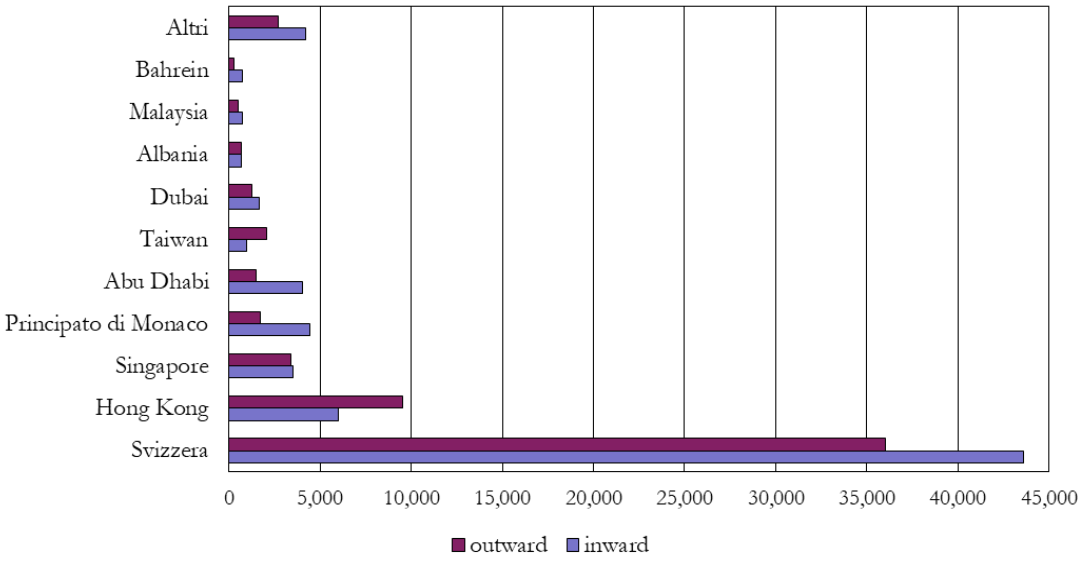
[14] The list of non-cooperative countries and/or tax havens is taken from the ministerial decrees implementing the Consolidated Law on Income Tax (TUIR), the list of high-risk jurisdictions and jurisdictions under

Bahrein and Albania replaced Tunisia and Serbia among the top ten counterparty countries (Figure 6.2).

Figure 6.2

Credit transfers with tax havens or non-cooperative jurisdictions

(millions of euros)



Anomalies in financial flows

The provincial distribution within Italy of the outgoing financial flows to non-cooperative jurisdictions or tax havens was particularly uneven in 2020, as in 2019, while inward transfers from these countries showed greater concentration of provinces with medium-high flows in the central and northern regions and in Sardinia (Figure 6.3a)

For credit transfers too, by exploiting the econometric model it was possible to estimate the component of the flows with these jurisdictions that is explained by the economic and financial fundamentals of the Italian provinces and foreign countries involved. The difference between the credit transfers observed and the value explained by structural factors is used to construct an anomaly index. [15]

increased monitoring published by the FATF in February 2020, the EU list of tax havens (update of 27 February 2020), and the list of countries identified by the European Commission in Delegated Regulation (EU)/2016/1675 as amended, in accordance with the publication of the statistics for 2020 in the UIF's *Quaderni dell'Antiriciclaggio, Dati statistici*. Compared with 2019, Afghanistan, Iraq, Iceland, Nicaragua, Zimbabwe, Jamaica, Myanmar, Albania, Mongolia, Uganda and Palau were added to the list, while Ethiopia, Tunisia, Sri Lanka and Serbia were removed.

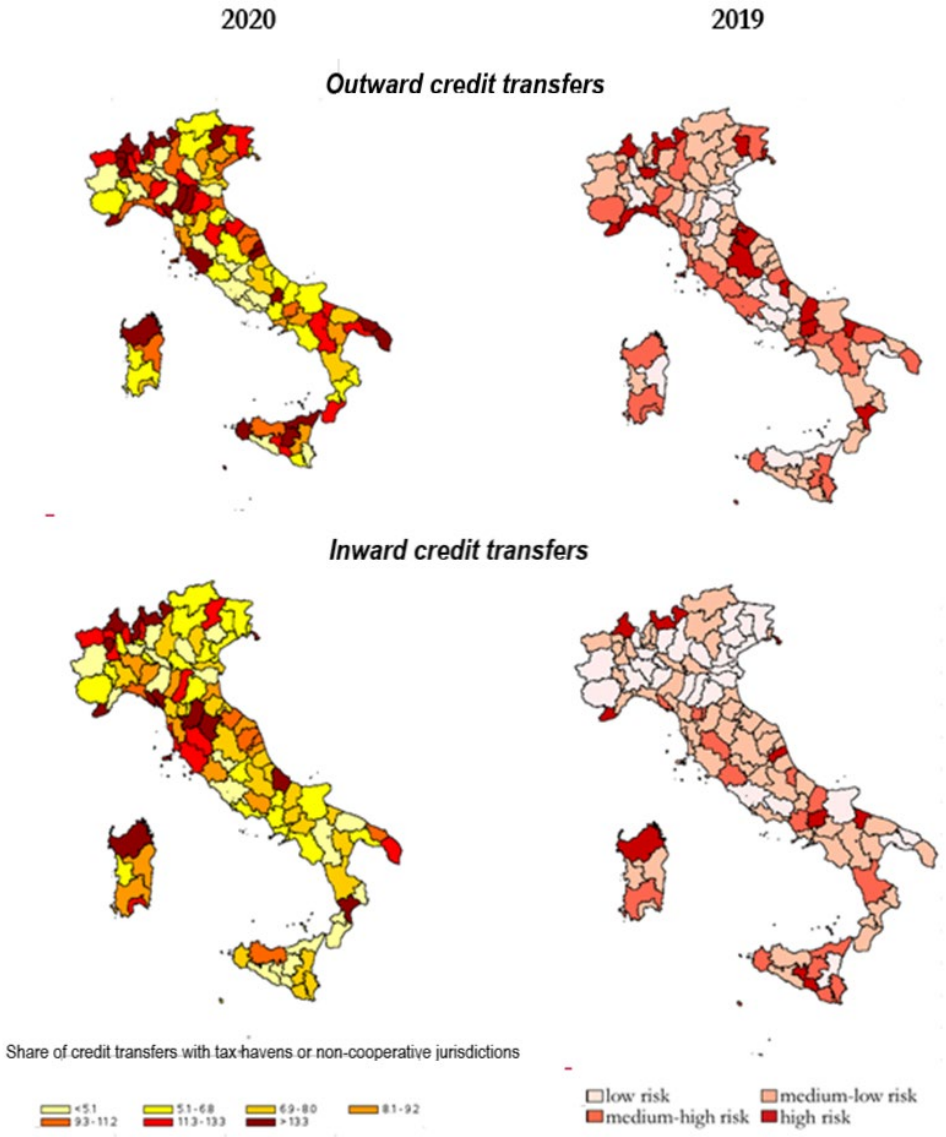
[15] See UIF *Annual Report for 2017*, pp. 85-86.

Figure 6.3

Credit transfers 'at risk'

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

b) Anomalies in cross-border credit transfers (2)



(1) See Figure 6.1, note 2. – (2) The maps refer to 2019, the latest year for which all the data needed to estimate the model are available.

The money laundering risk exposure at province level obtained via this statistical methodology (Figure 6.3b) differs from the distribution of the flows observed. Anomalies in outward credit transfers are found above all in the provinces of the North-West, a few parts of the Centre and some areas in the South, independently of the portion of transfers involving non-cooperative jurisdictions and tax havens. As for inflows, high risk is most common in the Centre, the South and the Islands (except for Basilicata, every region in these parts of

Italy has at least one province with medium-high or high laundering risk); alongside these are a few border provinces in the North of Italy.

6.2. Analysis of aggregated data and research activity

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

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

The UIF is continuing to develop econometrics-based inquiry into the phenomena and financial conduct of interest, with the twofold aim of increasing knowledge of specific phenomena and providing operational guidelines to prevent and combat money laundering. The results of these studies are used internally to identify sectors and geographical areas at risk and situations deserving closer scrutiny. The findings are also shared with other AML authorities according to their respective functions. The methodology and the general findings are published in the 'Analisi e studi' series of Quaderni dell'antiriciclaggio (only in Italian).

Monitoring data quality

Maintaining the high quality of the SARA data is an essential prerequisite for effective strategic analysis on the part of the Unit. In 2020, the automatic statistical checks flagged some 24,500 potentially anomalous data aggregates. As a result, 777 reporting entities (including 459 banks) were asked to check the data they had sent. In 4.7 per cent of the cases questioned, the reporting entities found errors in the data transmitted. In 1.3 per cent (318 cases), the data checked were found to be related to STRs already sent to the UIF. In another 160 cases the reporting entities re-examined the underlying transactions with a view to possibly submitting a suspicious transaction report.

In 2020, the number of requests from reporting entities for the UIF's assistance in preparing SARA reports and gold declarations increased considerably, to about 2,500. The Unit is now implementing a system of controls on SARA reporting entities (see Section 10.4, 'IT resources'), which will allow continuous monitoring of their compliance to detect any behaviour that deviates from the regulatory provisions and intervention to ensure data integrity.

Monitoring of cross-border financial flows to detect abnormal peaks …

The Unit has begun work on a new statistical model using the SARA data at the most detailed level available to identify specific anomalies, such as isolated peaks, in the financial flows with the foreign jurisdictions of interest. The procedure flanks the econometric models already being used to detect anomalies and will permit systematic monitoring of flows with selected counterparty countries based on a rigorous statistical methodology. The most significant of the anomalies detected can then be examined, exploiting the other databases at the Unit's disposal as well, to determine the underlying causes.

… or anomalous trends

Meanwhile, since early 2020, the Unit has conducted a half-yearly monitoring of foreign credit transfers to pick up any discontinuities in inward and outward financial

flows. This system can identify two particular types of phenomena: marked and protracted accelerations (or decelerations); and sudden increases (or decreases) in volume.

With reference to the health emergency, the Unit performed several targeted analyses to identify cases in connection with the heightened risk of infiltration of the economy by organized crime.

Analysis of criminal infiltration of the economy in connection with the pandemic

The SARA data for March and April 2020 indicated that during the first two months of the health emergency, total transactions averaged 1.8 per cent less than in the same period of 2019, with a drastic drop in the use of cash (down 42.2 per cent), a significant decline in domestic credit transfers (down 13.9 per cent) and broad stability in cross-border ones (up 2.0 per cent). In addition, some anomalous cash transactions in a specific local area were noted, and subsequent inquiry brought out evidence that was passed on to the competent investigative bodies for follow-up.

On an experimental basis, the Unit also applied an indicator of risk of infiltration of firms by organized crime in an analysis of the government funding measures in support of economic activity. Using a sample of firms subjected to judicial seizure in proceedings against mafia-style criminal organizations – made available by the Special Operations Task Force (ROS) of the Carabinieri in the framework of an ad hoc collaboration – the Unit identified several recurrent features of the economic and financial structure of the infiltrated firms. On the basis of the variables thus identified, an indicator of 'statistical similarity' was constructed, serving to gauge the extent to which the financial statements of any given firm resemble those of a mafia-infiltrated firm operating in the same province and economic sector. The indicator was calculated using the financial statements for 2018[16] of some 90,000 private limited companies in the provinces and economic sectors where infiltration by organized crime is typically most common.

The capacity to identify firms with a high risk of infiltration was verified both by means of 'in-sample' statistical validation procedures and by reference to the information supplied by STRs. A second type of validation, more strictly operational in nature, is still being conducted together with the Special Foreign Exchange Unit of the Finance Police. While further inquiry and verification are still required, both exercises furnished promising indications as to the capacity of this approach to identify firms potentially controlled by organized crime.

The experimental application of the indicator with specific reference to the health emergency served a two-fold purpose: to supplement the tools already used at the UIF to contribute to the identification, within STRs, of criminal contexts of possible interest, for subsequent operational analysis; and to report, also for the purpose of on-site or off-site controls, anomalous concentrations at a given intermediary of publicly guaranteed financing for firms at risk of infiltration.

Effect of cash on the shadow

One of the research projects initiated in 2020, and now nearing completion, is a study together with the Economics, Statistics and Research Directorate General of the Bank of Italy to estimate the effects of the use of cash on the size of the shadow economy in Italy. Although the literature has documented the relationship between the use of cash and the scale of irregular economic activity, the empirical evidence of this causal link is only limited. A provincial breakdown was made possible by the SARA data on the use of cash, together

[16] The last year available at the time of the analysis.

with the data on under-invoicing made available by Istat. The preliminary evidence gathered so far shows a statistically significant correlation between the use of cash and the amount of shadow economic activity.

The political cycle of opaque payments

In addition, in cooperation with academic partners the Unit undertook an econometric study of the 'political cycle' of opaque payments. This research project is intended to determine whether municipal election periods in recent years have corresponded to significant local variations in the use of cash or in the volume of credit transfers to tax havens. This analysis utilizes monthly extracts of SARA data at municipal level.

The model estimated for this study also takes account of certain contextual factors, such as local socio-economic characteristics, the size of the municipality, and other features of electoral competition. The results to date – here too, preliminary – suggest some elements of interest, chiefly involving the use of cash in smaller municipalities.

Risk indicators for non-bank intermediaries

For years now, the Bank of Italy's supervisory directorates have employed, in their assessments of money laundering risk at banks, an analytical model whose quantitative component comprises a set of indicators developed with the contribution of the UIF. In 2020, the first stage in the development of composite money laundering risk indicators for non-bank financial intermediaries[17] was completed. As the data on these intermediaries are generally more limited and less accurate than those on banks, a special methodology had to be applied. The approach adopted, which relies principally on SARA data and on banks' automated prudential returns, consists in 'fuzzy logic', a technique taken from artificial intelligence.

While this method is more complex than that utilized for banks, it has a series of advantages that make it well-suited to this particular context: *i)* more reliable results where the data are inaccurate and/or incomplete; *ii)* the possibility of incorporating a priori knowledge and qualitative information into the process of defining the indicators; and *iii)* better comprehensibility for end users of the rules for calculating the indicators, thus facilitating their involvement in the construction and maintenance of the applications.

On the basis of a set of indicators representative of the intermediaries' business operations and the application of 'fuzzy logic', the methodology makes it possible to define specific anomaly 'scores' and, as a function of these, to rank money laundering risk according to homogeneous classes of intermediary.

Working group on the payment system

The UIF has formed a working group together with the Bank of Italy to study the use of payment system data for cyclical analysis and forecasting of the main macroeconomic variables, including a territorial breakdown. The group has concluded its work, drafted a series of research contributions and published a report setting out the main results.[18] At the same time, a cooperative project under way between the Bank of Italy, the UIF and Istat is directed to the utilization of transaction data collected from the payment system to produce official estimates of GDP and other national accounts aggregates. An exploratory analysis is being conducted into the statistical correlations between the time series of Istat's data on the shadow economy

[17] Investment firms, asset management companies, electronic money institutions, payment institutions and entities entered in the single register of financial intermediaries under Article 106 of the Consolidated Law on Banking.

[18] Aprigliano V., Ardizzi G., Cassetta A., Cavallero A., Emiliozzi S., Gambini A., Renzi N. and Zizza R. (2021), 'Exploiting payments to track Italian economic activity: the experience at Banca d'Italia', Questioni di Economia e Finanza, No. 609.

and the SARA data on the use of cash. The results could offer useful indications for improving the official estimates of unreported economic activity and at the same time bring out potential anomalies in the use of cash.

Other activities

The health emergency did not prevent the UIF from continuing to be an active participant in the national and international scholarly debate on topics concerning the economy, legality and law enforcement.

In April 2020, two UIF staff members attended a meeting organized by the International Monetary Fund, presenting the methodology developed by the UIF to define the indicator of risk of mafia infiltration of Italian firms. The Unit's strategic analytical activity was presented as part of a programme of technical assistance to the AML authorities and the private sector of Kosovo, organized by the UN Development Programme. Finally, the report 'SupTech applications for anti-money laundering' – a review of advanced data collection and data analytics tools, the product of collaboration between the BIS Financial Stability Institute and the UIF[19] – was presented at a summit organized in November 2020 by the Philippine FIU (the Anti-Money Laundering Council).

Publications

Last year, a scholarly journal published the revised and updated version of a study, which first appeared in the 'Analisi e studi' series of Quaderni dell'antiriciclaggio, on the adequacy, in quantitative terms, of the province-by-province flow of Italian banks' suspicious transaction reports. [20]

6.3. Gold declarations

The law governing the gold market in Italy provides that transactions involving investment gold or gold material for mainly industrial uses (other than jewellery) must be declared to the UIF. This requirement applies to gold sales and to physical transfers of gold out of or into Italy for amounts of €12,500 or more.[21]

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

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

The value reported in gold transaction declarations increased substantially in 2020 to almost €25 billion, with a rise of 31.2 per cent (Figure 6.4). At the same time, the number of declarations declined by 2.0 per cent and the number of underlying transactions by 12.3 per cent. These developments are largely explained by the price of gold, which, despite a decline starting in August, rose by 26 per cent on average for the year.[22]

[19] See UIF, *Annual Report for 2019*, pp. 76-77.

[20] Gara M., Pauselli C. (2020), 'Looking at 'Crying Wolf' from a Different Perspective: An Attempt at Detecting Banks Under- and Over-Reporting of Suspicious Transactions', Italian Economic Journal, 6, pp. 299-324.

[21] Law 7/2000 and subsequent amendments.

[22] The average price was €50.00 per gramme in 2020 compared with €39.70 in 2019.

Table 6.3

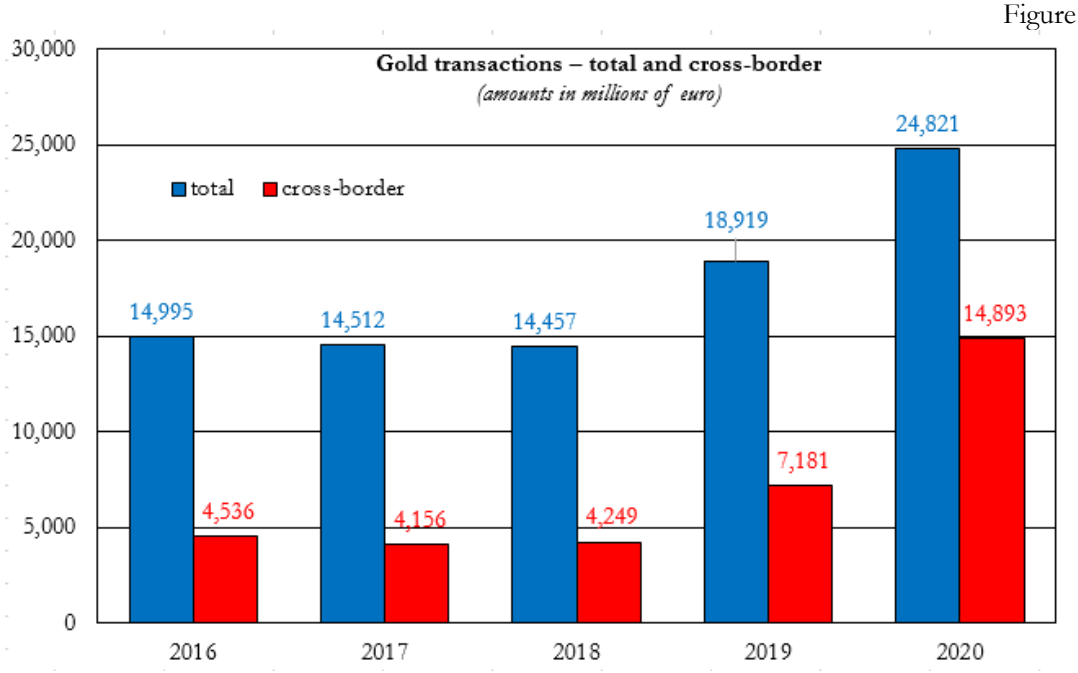
***Ex-post* monthly declarations on gold transactions**

TYPE OF TRANSACTION	**Number of declarations**	**Number of transactions**	**Declared value** *(millions of euros)*
Sales	38,337	90,045	23,894
Gold loan for use (concession)	822	1,492	511
Gold loan for use (restitution)	389	472	81
Other non-financial transactions	91	91	79
Personal imports of gold	107	126	151
Investment gold delivery services	277	280	105
Total	**40,023**	**92,506**	**24,821**

Gold sales' share in the total value declared rose from 93.6 to 96.3 per cent, with a significant contribution from cross-border transactions.

Transactions consisting in 'restitutions in respect of loans for use' and 'other non-financial transactions' – in any case residual – increased respectively by €25 million and €35 million (or by 45 and 80 per cent). The other types of transaction diminished both in number and in amount.

Figure 6.4



Categories of declarants

The growing interest in this sector was confirmed last year by the continuing increase in the number of entities registered with the system; furthermore, unlike previous years, 2020 also saw an increase in the number of entities that were active (Table 6.4). The rise in the number of registrants was due to the entry of 19 new professional gold dealers, 63 other natural persons and 20 other legal persons. The number of registrants who effectively submitted gold declarations rose by 61 (or by 14.7 per cent). The preponderance of professional

dealers was further strengthened, as their share of total gold declarations rose from 82.6 to 85.4 per cent, offsetting the decline in the banks' share from 16.3 to 13.5 per cent.

Table 6.4

Reporting entities engaged in gold transactions

CATEGORY OF REPORTING ENTITY	**Number of reporting entities registered**	**Number of reporting entities active in the year**	**Number of declarations**
Banks	71	26	5,564
Professional gold dealers	461	364	35,287
Other, natural persons	188	57	151
Other, legal persons	107	30	341
Total	**827**	**477**	**41,343**

The share of investment gold transactions increased in 2020, from 46.0 to 49.4 per cent, and the share of gold for industrial uses continued to rise, from 44.3 to 45.9 per cent. The incidence of cases in which the purpose of the transaction was not specified fell significantly, from 9.7 to 4.7 per cent.

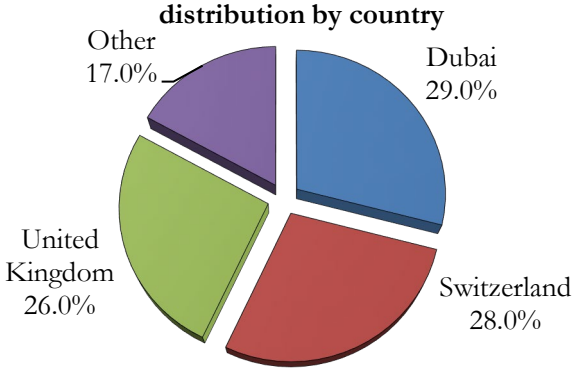
Geographically, the Italian counterparties were again concentrated in the traditional goldsmithing districts of Arezzo (market share of 45.3 per cent) and Vicenza (9.1 per cent). The share of counterparties located in the province of Turin rose to 5.6 per cent, surpassing Alessandria (4.6 per cent).

Transactions with foreign counterparties

Gold transactions with foreign countries more than doubled in value, from €7.2 billion to nearly €14.9 billion (Figure 6.4). Sales increased more sharply than purchases (up by 122.7 against 88.3 per cent). Most of the growth was accounted for by two countries: transactions with Dubai increased more than six-fold, owing to the extraordinary growth in purchases; while those with the United Kingdom more than tripled (growth of 249 per cent) owing to sales (Figure 6.5).

Figure 6.5

Gold transactions with foreign counterparties - distribution by country



In both cases the increase was accounted for by a small group of leading Italian gold operators. On the other hand, the share of Switzerland, which was Italy's leading counterparty country until 2019, slipped from 36.8 to 28.0 per cent, even though transactions rose by 50 per cent in absolute value. In short, there was a radical alteration in the make-up of

foreign counterparties; those in the three countries mentioned accounted for 83 per cent of the total, the rest being distributed among a few others (including the United States, Colombia and Spain).

In keeping with the expansion described above, the value declared in advance gold declarations more than tripled between 2019 and 2020, owing mainly to the increase in sales and mere transfers.[23] The increase in personal transfers of gold abroad by travellers continues to be under the examination of the competent authorities.

Statistics on advance gold declarations

It is worth noting that the ratio of the value of advance to *ex-post* declarations for sales (for which advance declarations are compulsory) rose from under 60 per cent in 2019 to over 80 per cent in 2020; Italian gold market participants are evidently paying greater attention to fulfilling their obligations in this regard.

Table 6.5

Advance declarations (transfers of gold abroad) (1)

TYPE OF TRANSACTION	**Number of declarations/ transactions**	**Declared value** *(millions of euros)*
Sales	1,164	6,325
No transaction (mere transfer)	137	560
Other non-financial transactions	15	52
Gold loan for use (restitution)	3	6
Investment gold delivery services (2)	1	0,0
Total	**1,320**	**6,943**

(1) Advance declarations are incorporated in *ex-post* declarations where the transfer underlies a commercial or financial transaction - (2) The amount declared in the sole transaction of this type was €10,000.

Analyses of the ORO databank

In managing the system for collecting gold declarations, in view of the high risk of criminal infiltration in this sector, the UIF also pursues the objective of detecting anomalous operating practices and devising anomaly indicators. Last year the data collected were again subjected to analysis. In some cases, anomalies emerged via checks on the names of the persons subject to the declaration requirement. Special attention was paid to cross-border gold transactions, which in 2019 had displayed very significant variations, most notably as regards a few countries.[24] Further inquiries in this regard were carried out by the Unit, and the results transmitted to investigative bodies. Following the commencement of investigations into administrative and tax irregularities, the investigative bodies asked for additional details on the anomalous transactions observed by the UIF in previous inquiries.

[23] Other non-financial transactions in gold, in connection with goldsmithing, increased in value from €400,000 to €52 million.

[24] See UIF, *Annual Report for 2019*, p. 80.

7. COOPERATION WITH OTHER AUTHORITIES

7.1. Cooperation with the judicial authorities

International and European principles and rules prescribe the broadest possible cooperation between FIUs and the other authorities responsible for preventing and combating money laundering and the financing of terrorism, having regard to their respective institutional powers and the principle of reciprocity in information exchange. Under Italian legislation the system hinges on the principle of coordination between prevention and enforcement, with various forms of cooperation and information exchange between the UIF, the investigative bodies and the judiciary, in compliance with the limits and the separation of roles provided for by law. Within this framework, the UIF has adopted increasingly effective and advanced forms of interaction and channels of information exchange.

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

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

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

Information exchanges with the judicial authorities and investigative bodies increased sharply in 2020. The UIF received 558 requests from the judiciary (an increase of 41.3 per cent) and sent back 1,188 responses (up 52.5 per cent), including follow-up transmissions of further information regarding the same persons of interest to the investigating authority (Table 7.1).

Table 7.1

Cooperation with the judicial authorities

	2016	2017	2018	2019	2020
Information requests from the judicial authorities	241	226	265	395	**558**
Responses	473	429	488	779	**1,188**

The pandemic was a factor in intensifying the UIF's cooperation with the investigative bodies, the DNA and the judiciary.

In addition to asking the UIF for STRs and the related technical analyses, any available information from foreign FIUs, and threshold-based communications, the judicial authorities have displayed increasing interest in more sophisticated forms of cooperation with the Unit. They have asked the UIF to assist in their investigations with analyses of the financial flows traceable to persons of interest both in Italy and abroad.

With regard to these requests, the Unit performed specific, in-depth financial analyses to describe complex criminal organizations operating internationally and to map flows in connection with serious crimes, in particular crimes against general government and against property. In a significant number of cases, finally, the cooperation involved investigations of crimes in connection with the epidemic emergency.

Under Article 12(3) of Legislative Decree 231/2007, the judicial authorities, as they deem necessary to a criminal proceeding, may request the UIF to furnish any and all pertinent information. In the framework of its cooperation with the judiciary, in 2020 the Unit received 20 new requests which, like the 20 received previously and still being processed, involved reconstructing the origins and destinations of the fund movements ordered at intermediaries by the persons under investigation; these requests led to specific, in-depth inquiries into those persons' corporate holdings, their beneficial ownership of accounts, and their cross-border transactions.

The Unit activated international cooperation with counterpart FIUs abroad to acquire information relevant to the investigations under way. There were 575 such cases in 2020, an increase of 31.3 per cent over the previous year. The information so obtained was shared for intelligence purposes with the judicial authorities, with the prior consent of the relevant counterpart FIUs.

The requests for foreign information on behalf of the judicial authorities were directly principally to the FIUs of the United Kingdom, Germany, Spain, Switzerland, Malta and Bulgaria. There were also significant exchanges of information with the FIUs of the Netherlands, Lithuania, Romania, Croatia, the Czech Republic, Hungary, the United States, the United Arab Emirates, Hong Kong and China.

International cooperation produced major results also on the front of illegal activities in connection with the pandemic.

As noted in an FATF *Report* released on 16 December 2020 on the most common instances of COVID-related illegal activity, in one case the UIF, with the invaluable cooperation of the relevant foreign FIU, succeeded in promptly blocking the transfer of funds abroad by an Italian company that had been induced, via a business e-mail compromise scam, to order a substantial transfer for the purchase of medical products. In another case, thanks to international information exchange, the Unit looked into anomalous transactions in connection with the supply of healthcare equipment and devices by legal persons linked to politically exposed persons.

The Unit's analytical contributions also concerned possible cases of usury, unauthorized exercise of banking and financial activity, and tax and bankruptcy offences. There were also

an especially large number of requests for information involving financial cyber-fraud, such as 'man-in-the-middle' attacks,[25] 'smishing,'[26] 'vishing,'[27] and 'sim swaps'.[28]

These judicial requests for cooperation escalated in 2020 (there were 80, compared with 20 in 2019). The total amount reported as proceeds of IT frauds in Italy with the funds diverted abroad was put at over €15 million. The most common technique was the 'man-in-the-middle' scam.

The countries to which the proceeds of IT fraud were most commonly sent are European (first of all the United Kingdom, followed by Spain, Germany, the Netherlands and Sweden). However, the cases of fund hijacking to non-European countries (especially Asian countries) involved a larger total amount.

The number of reports pursuant to Article 331 of the Code of Criminal Procedure also rose significantly in 2020. The increase in reports to the judiciary mainly involved crimes in connection with anomalies discovered in the course of customer due diligence (the submission of counterfeit documents or communication of false data), or in connection with IT fraud (Table 7.2).

Table 7.2

Reports to the judicial authorities

	2016	2017	2018	2019	2020
Reports per Article 331 of the Code of Criminal Procedure	157	115	87	106	257
of which: submitted to judicial authorities	2	3	-	2	1
made in connection with technical reports sent to inv. bodies	155	112	87	104	256
Informative reports for investigative purposes	16	26	16	11	11

Cooperation with the DNA

The Unit's cooperation with the DNA, under the memorandums of understanding signed in 2017 and 2018,[29] was fruitfully reinforced in 2020.

As regards STRs and informative reports from abroad in connection with the COVID-19 pandemic, in the framework of cooperation with the DNA a special panel of technical experts was instituted by the National Anti-Mafia Prosecutor's Office, comprising the UIF, the Finance Police and the Customs and Monopolies Agency, for the purpose of sharing

[25] For a definition, see UIF *Annual Report for 2019,* p. 84.

[26] 'Smishing' (abbreviation of 'SMS phishing') consists in text messages to users' telephones, usually asking them to contact a certain telephone number or consult a website to effect a specified activity (e.g. open an email attachment or click on a link). Via these contacts the users are asked to supply personal information such as passwords or credit card data.

[27] 'Vishing' ('voice phishing') is the fraudulent practice of creating a system of automated phone calls or voice messages asking for personal information. With respect to other, similar techniques, the voice call creates a sense of urgency that can more easily induce individuals to supply the data requested.

[28] 'Sim swap' is a computer fraud resulting in acquisition of the victim's home banking data and credentials through techniques of hacking or social engineering (deceptive action to collect information on the victim and induce mobile phone service providers to issue a new sim card). Then, using false documents, the fraudster replaces the victim's sim card and, via the same telephone number, acquires from the bank the credentials needed to operate on the on-line account.

[29] See UIF *Annual Report for 2018*, p. 83.

their respective actions to prevent and combat criminal activity. The Unit's informative reports helped in the prompt detection of the presence of persons known for their potential links with organized crime; through further inquiry into situations brought to light by crossing the respective databases, they triggered additional requests from the judiciary for the Unit's cooperation.

To enhance the efficacy of the anti-crime action of the UIF and the DNA,[30] on 12 March 2021 the protocol signed in May 2018 was updated. The new MoU will speed up information exchanges, halving the time allowed for communications between the National Prosecutor's Office and the UIF; and it will increase the quantity of data to be exchanged for name matching, which now extends also to certain types of communications from foreign FIUs to the UIF. The objective is more immediate utilization by the investigative magistrates of the information contained in STRs and foreign FIUs' communications and more thorough financial analysis by the Unit. The other forms of cooperation with the DNA – regarding analysis and examination of individual anomalies, economic sectors held to be at risk, types of payment instrument and local economies – were also confirmed.

SAFE

The SAFE portal is more and more commonly used for the transmission to the UIF of requests for cooperation from the General Command of the Finance Police, within the framework of investigations on behalf of the judicial authorities, in particular for more in-depth international investigation. Prosecutor's offices, however, continue to send most of their requests for cooperation via conventional channels.

7.2. Cooperation with the MEF and the FSC

The UIF cooperates with the Ministry of Economy and Finance (MEF), contributing to the design of prevention policies, helping to draft regulations, participating in international organizations, and taking part in sanction procedures. The Unit participates in the work of the Ministry's Financial Security Committee (FSC), with tasks of analysis and coordination to prevent the exploitation of the financial and economic system for purposes of money laundering and the financing of terrorism. All the authorities involved in prevention and enforcement are represented on the Committee, which serves as a focal point for strategy development and is responsible for applying international sanctions.

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

In addition, the UIF monitors the application of freezes of funds and assets under financial sanctions adopted by Italy or the European Union to combat the financing of terrorism and the activities of countries that constitute a threat to world peace and security.

The Unit also gathers financial information on the frozen funds and assets and facilitates the dissemination of the lists of designated persons. In this role the Unit assists the FSC in resolving operational and interpretative problems concerning the application of international financial sanctions.

[30] Pursuant to Legislative Decree 231/2007, Article 8.

In the course of 2020, the UIF provided support to the FSC in considering and either granting or denying requests for authorization to transfer funds or provide financial assistance to persons subjected to sanctions or to export specific types of goods to countries subject to restrictions (mainly dual-use products and those that can be used for purposes of repression).

Within the framework of the international sanctions adopted by the European Union, the UIF's inquiries pursuant to Article 10 of Legislative Decree 109/2007 found no accounts or assets in Italy susceptible to freeze measures beyond those already discovered in years past. The communications received from the obliged entities (nine in number in 2020, all from banks) therefore consist only in updates on accounts already frozen and for which the UIF checked compliance with the conditions laid down for the utilization of the funds (unfreezing) or the crediting of liquidity, the latter too to be frozen.

The amounts of funds and assets frozen remained broadly at the same level as in 2019 (Table 7.3). The main changes involved the delisting of three persons on the consolidated UN list relating to ISIS and Al-Qaeda,[31] and the crediting of funds (these too frozen) to an account held by an Italian entity attributable to a person on the list, necessary for the payment of charges and the management of assets, authorized by the Financial Security Committee.

Table 7.3

Measures to freeze funds at 31/12/2019

COUNTRY OR ORGANIZATION	**Accounts and transactions frozen**	**Persons subject to freezing**	**Amounts frozen**		
			EUR	**USD**	**CHF**
ISIS / Al-Qaeda	26	22	17,819	114	
Iran	17	4	1,086,120	158,453	37,593
Libya	4	3	2,140,204	132,357	-
Syria	28	5	17,969,016	240,825	149,872
Ukraine/Russia	2	1	434,908	-	-
DPR of Korea	3	4	8,000	-	-
Total	**80**	**39**	**21,656,067**	**531,749**	**187,465**

As regards the financing of the proliferation of weapons of mass destruction, the overall framework of the sanctions adopted by the European Union against North Korea, also pursuant to UN Security Council resolutions, remained broadly unchanged.

The European Union adopted two amendments to the regulation on North Korea (Regulation (EU)/2017/1509), specifying details concerning persons already designated in order to make it easier for Member States to identify assets attributable to these persons. The requirement to send reports to the FIUs in the case of suspected financing of proliferation was maintained, as was the specific authorization requirement for transfers of funds above certain threshold amounts.[32] As part of its work within the FSC, the UIF carried out the assessments within its competence regarding compliance with the relevant legislation, specifically upon

[31] Adopted in the European Union with Regulation (EU)/2002/881.

[32] Provided for, respectively, by Article 23 (1.e) and Article 21 of Regulation (EU)/2017/1509.

request of the UN panels of experts tasked with verifying compliance with the requirements of the Security Council resolutions relating to the various sanctions in force.

7.3. Cooperation with supervisory authorities and other institutions

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

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

Exchanges with the Bank of Italy's supervisory directorates

The exchange of information between the UIF and the Bank of Italy's financial supervisory directorates continued to be intense. The supervisory directorates submitted informative reports to the Unit, mostly in connection with inspections, concerning possible shortcomings in active cooperation on the part of obliged entities. The UIF conducted further inquiries, which in some cases led to the institution of sanction proceedings for failure to make suspicious transaction reports (see Section 5.2, 'Sanction procedures').

... with Consob

Collaboration continued with Consob, with the usual exchanges of information on possible failures to submit STRs uncovered in the course of supervisory inspections and analyses of market abuse. The two organizations also continued coordinated inspections at auditing firms, to check for compliance with the AML obligations and heighten the sector's awareness of anti-money laundering issues (see Section 5.1, 'Inspections').

... with IVASS

Again in 2020, continuing information exchanges with the insurance supervisor IVASS mainly concerned applications to acquire significant stakes in insurance companies, for the purpose of ruling out grounds for suspicion of links with money laundering or terrorist financing.

In many instances, the requests of IVASS stemmed from the information needs of foreign insurance supervisors. In these cases, given the special secrecy rules governing the data exchanges, the Unit transmitted to the FIUs of the countries involved the information from its own files for possible AML analysis, together with its consent to informing the local insurance supervisory authority, in compliance with national and international regulations. IVASS has been informed of this procedure for cooperation with the foreign authorities.

... with MISE and the Customs and Monopolies Agency

The findings of the Unit's analyses of trust companies and gaming operators were transmitted, for their respective areas of competence, to the Ministry for Economic Development (MISE) and the Customs and Monopolies Agency. The Agency in turn transmitted various informative notes to the Unit, enabling the UIF to conduct further inquiry into anomalous financial flows, including cross-border flows, some of which proved to be connected with 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 in Italy for significant amounts.[33]

The Committee received 17 applications between 4 February 2020 and the start of 2021. They concerned investments in firms and innovative start-ups formed and operating in Italy, as well as Italian government securities. The investors came from Syria, Russia, the United States, Canada, Colombia, Azerbaijan, Libya and Israel.

Ministry of Justice

Again last year, the UIF examined the codes of conduct drawn up by representative associations pursuant to Legislative Decree 231/2001 for the prevention of the crimes of receiving, laundering or utilizing money, assets or goods of illegal provenance, and of self-laundering. The Unit then delivered to the Ministry of Justice its opinion on each code, with specific observations and requests for amendment.

Specifically, in 2020 the UIF transmitted to the Ministry of Justice five opinions pursuant to Article 25-*octies*(3) of the Legislative Decree. The Unit also continued to participate in the inter-institutional technical group to draft guidelines to provide the representative associations with the necessary procedural and substantive indications for easier and faster drafting of codes that fulfill the legal requirements.

Anti-corruption Coordinating Committee

The UIF's representatives participate in the inter-institutional Anti-corruption Coordinating Committee established by the Ministry of Foreign Affairs, which brings together the main Italian authorities engaged in combating corruption. This forum enables the participating institutions to share their experiences in preventing and combating corruption and to strengthen the principles of transparency and integrity at national level. The interdisciplinary expertise developed within the Committee is essential to the G20's Anti-Corruption Working Group, of which Italy was co-chair in 2020 (together with Saudi Arabia) before taking over the chair in 2021. The UIF is a member of the Ministry's task force to support Italy's activity within the Working Group and contributes to the actions that the Italian chair considers priorities.

Specifically, this involves the development of detailed, objective indices to measure corruption and the drafting of 'high level principles' on the relations between corruption and organized crime, corruption in sports, and combating corruption in the context of the economic crisis induced by the pandemic. The G20's anti-corruption work will aim to identify national best practices and to establish and translate into 'high level principles' a model of prevention and suppression based on a system of institutional relations, coordination between specialized authorities, exchange of experiences, and a shared culture of legality and integrity.

---

[33] See UIF *Annual Report for 2017,* p. 23. The rules on this matter were modified by Decree Law 76/2020, converted into Law 120/2020 (the 'Simplification Decree') and Decree Law 34/2020, converted with amendments into Law 77/2020 (the 'Relaunch Decree'). The latter, in Article 38(10), halved the minimum investment thresholds for visa eligibility; for equity investments in limited companies operating in Italy and held for at least two years, from €1 million to €500,000; for investments in innovative start-ups entered in the special section of the company register referred to in Decree Law 179/2012, Article 25(8), from €500,000 to €250,000. Law 120/2020, Article 40-*quarter*, provides that the investor visa can be granted to foreign citizens who intend to make investments or donations in their own name or on behalf of a legal person of which they are the legal representative. Further, the person holding the residence permit for investors, for an overall period of five years' duration from the original issue of the visa, is exempt from the requirement to sign the supplementary agreement referred to in Article 4-*bis* of the Consolidated Law on Immigration and also from the requirement of continuous residence in Italy laid down in the Consolidated Law's implementing regulation (Presidential Decree 394/1999).

OECD evaluation of international bribery

In December 2020, the UIF attended the International Anti-Corruption Day, which – in concomitance with the start of the Italian Presidency of the G20 – sought to encourage dialogue among the main national institutions involved in anti-corruption action. The UIF is engaged in the fourth phase of the evaluation of Italy in implementation of the OECD Anti-Bribery Convention. The monitoring exercise, coordinated by the Ministry of Justice, was postponed by a year owing to the pandemic. It will involve dialogue with the evaluation team, an on-site visit to Italy by the team, and a final report that may include recommendations (new and/or updated versions of those formulated in preceding phases) and judgments on the Italian system and the level of enforcement by the competent institutions.

Again in 2020, the UIF worked together with ANAC, under the renewed memorandum of understanding signed in September 2019,[34] sharing operational practices and general information that serves for the prevention and suppression of corruption.

Istat

The collaboration between UIF and the Italian Statistical Institute (Istat) on setting up an AML-CFT system within the Institute proceeded last year.

Istat is one of the first major Italian entities to have named a 'suspicious transaction report manager,' to be registered with the Infostat-UIF portal for the transmission of the reports, to have mapped and analysed AML-CFT risks in connection with certain 'sensitive' activities (in particular, the payment of grants and subsidies to entities, scientific associations, and public or private committees and bodies; procurement contracts for goods or services or execution of work; conventions for statistical analyses with public and/or private persons; disbursement or utilization of financing in the framework of international cooperation and research projects). Istat developed its internal procedures for evaluating and communicating data and information on suspicious transactions to the UIF, while guaranteeing confidentiality.

In December 2020 the Unit took part in a seminar for Istat staff with a presentation on the prevention of money laundering in general government and its interrelations with the anti-corruption system.

Cooperation with Istat also concerns the possible production, on an experimental basis, of statistical data that could be helpful to the Unit in performing its function of strategic analysis, and in developing anomaly indicators that assist obliged entities in detecting and reporting suspicious transactions for further analysis by the UIF.

General government entities

The UIF's contacts with the National Administration School, initiated in 2020, led to development and scheduling of an AML training course for general government entities in 2021. The course, held in May under the scientific responsibility of the Unit and the School, constituted a major occasion for sensitizing general government bodies and further disseminating an AML culture in the public sector.

The UIF is engaged in dialogue with individual general government bodies, conducting seminars and training sessions to heighten their awareness of their AML obligations. Useful occasions for dialogue and collaboration were created with the municipalities of Milan, Rome, Florence and Ragusa, and with the Regional Environmental Protection Agency of Lombardy.

The UIF takes part in a project, sponsored by the Lombardy branch of the national association of municipalities and the Lombardy Region, entitled 'municipalities' network – competences for legality.' The project, funded in part by the European Union, is intended to

[34] See *UIF Annual Report for 2019,* p. 90.

strengthen the competences of local administrations in combating money laundering and corruption by means of general training and targeted workshops for managers, functionaries and administrators of the Region and a number of city governments. The Unit was asked to contribute to both types of training course. With its effective workshop format, the initiative gave rise to productive meetings with a good number of local administrators focusing on concrete problems.

The Rome city government has begun cooperation with the UIF to supply information on the ownership of commercial undertakings and changes over time. The early indications to emerge from crossing these data with those on reporting flows already analysed by the Unit show a good many links and potentially fruitful developments for combating an increment in money laundering induced by the persistence of the pandemic.

8. INTERNATIONAL COOPERATION

8.1. Exchange of information with foreign FIUs

The international anti-money-laundering rules task FIUs with the centralized reception and analysis of suspicious transaction reports and the related exchange of information with their counterparts abroad. These functions are essential to the analysis of financial flows, which increasingly cross national borders and so are 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 on their own initiative or upon request, and in a timely, constructive and effective manner, the utmost international cooperation on money laundering, associated predicate offences and the financing of terrorism.

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

In accordance with the principle of multidisciplinarity, for purposes of domestic analysis and for reciprocal exchange, FIUs must have financial, investigative and administrative information available to them. FIUs must also provide the information requested, exercising the same powers of which they avail themselves for domestic analysis. Information exchanges between FIUs take place via rapid and secure electronic communication systems. At international level, the Egmont Group manages and updates its encrypted platform, the Egmont Secure Web. At EU level, a decentralized communications infrastructure called FIU.NET is used for structured bilateral or multilateral information exchange, guaranteeing standardized, immediate and secure data exchange.

In the course of 2020, the UIF exchanged information with the FIUs of all the EU Member States and with a total of 111 counterparts worldwide.

As support for its analysis of STRs, the UIF requests information from foreign FIUs where there are objective or subjective links to other countries.

Requests sent to foreign FIUs

Requests are generally aimed at reconstructing the origin or use of funds transferred from or to other jurisdictions, identifying economic resources abroad, verifying the formal ownership and the beneficial owners of companies and entities, and ascertaining whether there are inquiries or investigations under way. The exchanges involve all the criminal activities brought to the attention of the UIF. In addition to suspicious transactions involving bribery, tax violations and organized crime, cyber fraud is increasingly common, in some instances in connection with the COVID-19 epidemic. In many cases, the UIF requested cooperation in order to reconstruct suspicious transfers of virtual assets carried out through foreign intermediaries. Moreover, the exchange of information with foreign counterparts enables the UIF to provide Italian investigative bodies and judicial authorities with additional information in support of criminal investigations and proceedings (see Section 7.1, 'Cooperation with the judicial authorities').

In 2020, the UIF sent 1,050 requests for information to foreign FIUs, up from 963 in 2019. There was a very sharp increase of 31.3 per cent in information requests reflecting the

needs of the judiciary or law enforcement bodies in support of ongoing investigations (Table 8.1).

Table 8.1

Requests sent to FIUs in other countries

	2016	2017	2018	2019	2020
Information required by the judicial authority	204	172	367	438	**575**
Information required for internal analysis	340	591	715	525	**475**
Total	**544**	**763**	**1,082**	**963**	**1,050**

The UIF received 1,546 information requests and spontaneous communications from foreign FIUs last year, an increase of 14.5 per cent (Table 8.2). Exchanges with foreign FIUs have increased steadily since 2017, both via Egmont Secure Web and via FIU.NET.

Table 8.2

Requests/spontaneous communications received and responses provided

	2016	2017	2018	2019	2020
Egmont network	1,259	668	594	621	695
Requests/spontaneous communications	*723*	*504*	*577*	*594*	*694*
Exchanges on ISIL	*536*	*164*	*17*	*27*	*1*
FIU.NET					
Requests/spontaneous communications	*580*	*524*	*602*	*729*	*851*
Total	**1,839**	**1,192**	**1,196**	**1,350**	**1,546**
Responses provided (1)	**1,568**	**1,232**	**1,681**	**1,862**	**2,246**
Communications to investigative bodies	**1,430**	**2,031**	**3,070**	**2,533**	**3,296**

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

Requests from foreign FIUs

The UIF provided 2,246 responses to the information requests and communications received from foreign FIUs, 20.6 per cent more than in 2019. The figure comprises both responses to requests for cooperation and feedback on the use of the information acquired via spontaneous communications. In a good number of cases, the feedback refers also to the quality and usefulness of the assistance received.

There was stepped-up utilization of the Ma3tch function provided by FIU.NET for the anonymous matching of entire databases. Mat3ch makes it possible to identify recurring names in the archives of participating FIUs, and hence links with other countries that would otherwise go undetected (see Section 8.2, 'Cooperation between FIUs'). The UIF's dataset for this matching was expanded and is updated constantly. The findings are integrated into the Unit's internal analysis procedures. The successful, systematic exploitation of Ma3tch is the result of a common commitment of FIUs at European level. Many of the requests received from European counterparts refer specifically to cases identified thanks to this system of massive matching.

In keeping with the evolution of the terrorist threat worldwide and the declining operational capability of ISIL, there was a decrease in instances of multilateral cooperation directed to the identification of financial support networks for that organization. Bilateral exchanges relating to transactions and networks of possible terrorist facilitators, in some cases not of religious origin, continued nevertheless to be numerous.

In addition to the ordinary exchanges summarized in Table 8.2, there was a significant intensification of the transmission of cross-border STRs under Article 53(1) of the Fourth AML Directive, which mandates that European FIUs transmit STRs with significant links to other member countries to the relevant counterparts. This is an important source of information, allowing targeted further inquiry into cases of illegal activity carried out in Italy by means of foreign operators not subject to the Italian reporting requirement (see the box 'Developments regarding cross-border STRs' below).

Significant phenomena

The most important criminal phenomena investigated by means of cross-border cooperation involved the use of foreign accounts to transfer funds not declared to the tax authorities, the withdrawal and transfer of cash, and the layering of funds transfers to or from various countries. The use of trusts and trust companies to which to ascribe accounts or assets for purposes of interposition or dissimulation is common. A significant number of communications regarded complex fraud schemes or corrupt practices resulting in the transfer of the proceeds abroad; often the persons involved are under investigation in Italy.

There was a considerable increase, due in part to the pandemic's impact on use of the Internet, in various kinds of cyber fraud (love and romance scams, phone scams, CEO and business email compromise frauds, ransomware) and in the theft of funds via hacking into IT systems. In these cases, cooperative investigation seeks to trace the fraudulent transfers and promptly freeze the assets found in order to permit their recovery.

Close attention continues to be paid to trade-based money laundering, which involves sophisticated import-export schemes of over- or under-invoiced goods. In the most significant cases, complex trading in goods and funds transfers through multiple countries were the work of criminal organizations re-investing large volumes of illicit proceeds (see Section 8.3, 'The EU FIUs Platform'). Other important subjects of foreign communications were fiscal matters (invoicing fraud, intra-EU VAT fraud, tax evasion) and misappropriation of funds. The transactions frequently relate to complex operations detected and reported also domestically by obliged Italian parties.

The information exchanges with counterparts abroad included a number of requests and communications concerning suspicious transactions carried out in order to profit from the health emergency and the related economic relief measures. Between April 2020 and March 2021, the UIF received 66 STRs from foreign FIUs regarding this type of crime. Some of the cases brought up by foreign FIUs, while not relating specifically to the COVID-19

epidemic, nevertheless displayed significant linkage with the emergency, as revealed by further investigation on the part of the UIF.

Cross-border cooperation has not uncovered significant peculiarities in the financial schemes associated with pandemic-related crimes. Both in the commission of the predicate offence and in the subsequent money-laundering phase, one finds recourse to established, versatile instruments, sometimes exploiting new technology. For example, there may be receipt of payments in electronic form or on foreign online platforms for speculation or fraud in sales of personal protective equipment or medical supplies; the ascription of illegal sales of medical products to producer or exporter companies established in other countries (in some cases, officially engaged in sectors other than healthcare) but traceable to Italian interests; the management on foreign accounts of funds deriving from offences in connection with the health emergency or otherwise traceable to persons involved in investigations of such offences.

A fair number of foreign reports concerned possible online computer fraud, drug trafficking, trafficking in human beings, counterfeiting, money changing from or into virtual currencies, funds transfers and transactions on the dark web. In some cases, these operations were traced to suspected terrorist financing.

The UIF continues to receive from foreign counterparts a good number of requests and reports concerning online payments in connection with child pornography and the sexual exploitation of minors. In 2020, the Unit received 64 communications on cases of child pornography with links to Italy.

These payments are frequently settled through foreign intermediaries that operate online under the freedom to provide services. The transactions are carried out by Italian nationals in Italy or in other countries, or else by foreigners who log onto the Internet in Italy using devices located through the IP address. The transactions reported, mostly for small amounts, are especially useful in locating persons and tracing the cross-border criminal networks that such individuals typically form for trafficking in child pornographic material.

Cooperation for the suspension of transactions

Again in 2020, there were numerous instances of cross-border cooperation regarding the suspension of transactions or the freezing of funds in Italy or abroad (84 cases, compared with 50 in 2019 and 66 in 2018). In 29 cases, foreign FIUs contacted the UIF to request the application of measures to freeze accounts or other assets, traceable mostly to fraud, often computer fraud, or identity theft, with the transfer of the proceeds to Italy only to be quickly withdrawn in cash or transferred onward. In these cases, the Unit acted promptly with the cooperation of the Italian intermediaries involved to keep the funds from vanishing, thus enabling the foreign authorities to judge the situation and initiate the procedure for requesting seizure.

International cooperation in the suspension of transactions and freezing of funds

Article 6(4.c) of Legislative Decree 231/2007, as amended by Legislative Decree 90/2017, provides expressly that the UIF can order the suspension of suspicious transactions at the request of foreign FIUs, where certain preconditions are met. This provision transposes into Italian law Article 32(7) of the Fourth AML Directive, Directive (EU)/2015/849.

The number of suspension requests from foreign FIUs has increased steadily. They are directed to blocking transactions or freezing funds at Italian intermediaries, often in the framework of asset seizures in connection with investigations of fraud resulting in the misappropriation of money on accounts abroad with immediate transfer to accounts in Italy.

In the context of cross-border cooperation, the UIF's suspension procedure reflects the urgency of the intervention requested. The Unit immediately contacts the relevant Italian intermediaries to verify the transactions reported by the requesting FIU and the presence of the funds. Depending on the circumstances, the Unit asks the intermediaries to take appropriate precautions in their dealings with the customer involved (e.g. reinforced monitoring, account freezing). At the same time, the competent Italian investigative authorities are contacted, to verify the existence of investigations under way and obtain feedback on elements of possible investigative interest.

Only rarely, in the case of requests for intervention from foreign FIUs for purposes of analysis or investigations in their respective countries, is investigative activity under way in Italy as well. This fact, together with the short-lived efficacy of a suspension ordered by the UIF (five days), makes it hard in this brief interval to consolidate the freeze by means of restrictive measures, which must inevitably come after the completion of international investigative or judicial assistance procedures activated by the competent authorities of the requesting FIU's country.

Nevertheless, the Unit's intervention often proves effective, as it may lead the intermediaries themselves (which often file STRs of their own) to freeze the illicit funds and the accounts identified. Interbank instruments for reversal and recovery can be activated, which are effective when the illicit transfer was made at nearly the same time as the request for intervention. The investigative bodies in the country of the requesting FIU, at the latter's invitation, ask for urgent action by their Italian counterparts, invited in their turn by the UIF.

In one recent case, investigators identified credit transfers for very large amounts that a foreign firm had been induced to transfer to Italian accounts in execution of fraudulent orders sent in such a way as to appear to come from the competent corporate officers ('CEO fraud'). The UIF immediately issued a suspension order, preventing the transfer or withdrawal of the funds, which the perpetrators of the fraud had insistently requested. The foreign court, informed of these developments by its local FIU, issued seizure orders, which the Italian judicial authorities executed immediately.

On 55 occasions, foreign FIUs notified the UIF of the freezing, in their respective countries, of accounts or other assets traceable to persons with links to Italy, most of them under investigation. In these cases, the UIF promptly informed the Italian investigative bodies and, in the case of foreign assets, contacted the counterpart FIU to prevent the assets from being released. In this way, it was possible to identify, freeze and seize assets of persons under investigation that had not come to light in the domestic inquiries.

As in years past, the UIF passed on to the competent investigative bodies the information from foreign sources, after procuring the necessary consent from the foreign FIU (3,296 communications, compared with 2,533 in 2019, an increase of 30.1 per cent).

The investigative data necessary for the UIF to perform its duties of international mutual cooperation are transmitted with considerable delay and are significantly limited in content, owing in part to systematic requests for judicial authorization even in cases where investigative secrecy does not apply.[35] The information received continues to be scanty and for

[35] Article 12(4) of Legislative Decree 231/2007, as amended by Legislative Decree 125/2019, not only subjects the UIF's access to investigative information to the authorization of the responsible judicial authority as regards information covered by investigative secrecy but also provides that the Unit cannot be informed of the cases where a police investigation is under way and a communication has already been transmitted to the judicial authority but the latter has not yet decided whether to initiate a penal action. On this issue see UIF, *Annual Report for 2019,* p. 95.

the most part concerns events that are not recent, of little use for the foreign FIUs submitting the requests.

In May 2021, the UIF signed a memorandum of understanding with the South African FIU, the Financial Intelligence Centre, for cooperation in preventing and combating money laundering and the financing of terrorism.

The agreement, in keeping with international principles, provides that on a reciprocal basis each authority shall communicate, on request or on its own initiative, the information acquired in the performance of its duties, ensuring its confidentiality and its exclusive use for the purposes specified in the memorandum. The memorandum takes account of some constraints laid down in South African law and allows the extension of bilateral cooperation to a broader range of information, facilitating deeper financial inquiry in cases of suspected money laundering or terrorist financing.

8.2. Cooperation between FIUs

In the course of 2020, inter-FIU cooperation was further stepped up and extended to new forms. Despite persistent difficulties in utilizing FIU.NET due to infrastructural obsolescence, the FIUs of the European Union have demonstrated an increased capacity to share information on cases of common interest, frequently availing themselves of a broader range of national databases.

Exchanges have been sustained also by greater exploitation of the network's functions. There was increased use of the matching system, which serves to identify cases with otherwise unobservable linkages with other countries, in particular exploiting the common criteria identified by the FIUs Platform and the greater breadth of the data shared. Joint analyses, while still a relative rarity, are now an established instrument. The flow of cross-border reports makes a wealth of information available.

However, significant differences persist in methods of analysis, in the single FIUs' powers and in the information available to them. Although the Fifth AML Directive provides for a higher degree of harmonization, the effectiveness of the exchanges still suffers from limitations on the FIUs' access to significant types of information. In many countries there is no central register of data on bank accounts (mandatory in EU countries) or on the beneficial ownership of entities and companies (required also by FATF standards). There are also significant limits on access to tax and customs data, as on the possibility of acquiring data from obliged parties in all the circumstances necessary.

Exchanges of cross-border STRs among European FIUs still follow unsatisfactory procedures, in spite of the appreciable improvements in the quality of cases and a substantial increase in volume. In 2020, the Platform assigned high priority to the continuing work on refining the criteria for selecting, in appropriate number, the cases with significant cross-border links. A new project in which the UIF takes part has drafted guidelines for more fluid and uniform exchanges.

Among the automatic exchanges there are, first of all, reports filed by entities operating under the freedom to provide services. Then there are cross-border reports, selected according to subjective or objective criteria, aimed at focusing exchanges on cases of effective practical interest to the receiving FIU. Here, subjective criteria may refer to the person's place of residence or to investigations under way in other countries. Objective criteria may relate to the origin or destination of the financial flows or to the presence of accounts or assets held

abroad. Reference is also made to links with illicit activity carried out in another jurisdiction and to the importance of the case for other countries, as gauged by information in special archives or discretionary judgment. Given the wide range of reports that may qualify under these criteria, further screening is envisaged with matching via FIU.NET to extract significant matches of cross-border connections.

Developments concerning cross-border STRs

The UIF received 23,089 cross-border reports in 2020, mostly from the FIUs of the Netherlands, Luxembourg and Austria, which all have a good number of intermediaries that do business with non-resident customers or engage in activities abroad. Especially helpful are reports on transactions carried out in Italy by Italian or foreign persons using payment services provided by intermediaries established abroad and not subject to information or reporting obligations to the UIF.

The most significant cases involve credits or transfers of the proceeds of trade fraud or extortion, frequently committed in Italy by means of sophisticated falsification of identity, data theft, and simulated sales. A number of reports cited drug trafficking by Italian persons via e-commerce sites or social networks; possible cases of financial support to terrorist cells; trade in hazardous materials or in connection with child pornography, through instant messaging applications and online payments; transfers of virtual assets to and from IP addresses correlated with the dark web; financial transactions or payments by persons under investigation in Italy; or the use of pre-paid cards to conceal funds.

In 2020, the Unit also received multiple cross-border reports concerning the proceeds of illegal activity in connection with the COVID-19 health emergency. The activity reported involved trade in medical products and personal protective equipment on the part of Italian citizens or residents, speculating on the intense demand or engaging in outright fraud (for instance, 'non-delivery' scams).

Many European FIUs have not yet instituted systems for selecting potential cross-border STRs and transmitting them to the relevant foreign counterparts, often owing to difficulties in developing standardized procedures and the differences in format, content and language between the suspicious transaction reports of different FIUs.

There continue to be problems with the cross-border STRs received, due above all to the generic criteria adopted and widespread failure to apply them. In particular, the STRs suffer from insufficient specification of the grounds for suspicion, insufficient identity data, frequent lack of permission to forward the information to the competent investigative bodies, and transmission of the content in the original language and format. Another problem is the considerable heterogeneity in the use of computer records, making it difficult to institute procedures for automated data processing (which is essential, given the volume of data).

Legislative Decree 125/2019, transposing the European rules into Italian law, provides that the UIF transmit to other European FIUs information on STRs regarding the Member States concerned. In 2020, the Unit completed the work needed to implement this new national rule and began transmitting cross-border STRs to the relevant FIUs. In the course of the year, 2,015 of such reports were sent.

An initial trial phase applied systems of automatic selection and extraction of structured data from the STRs, with the capability to identify significant cross-border connections, significant types of transactions, descriptions able to characterize cases for the benefit of the receiving FIU. The IT support procedures and instruments were improved, and the system went operational. The extraction and reporting of suspicious cross-border transactions was

performed via screening for selected types of suspicious transaction that also featured medium-high risk and amounts above a preset threshold. Special descriptions of the cases in English provide the receiving FIUs with a synopsis permitting reconstruction of the transactions reported and the criteria for linkage, with a view to analysis and the development of more closely targeted forms of cooperation. In this context, the Unit added two new classification codes to the domain 'report category,' which must be used by Italian financial intermediaries for reporting transactions carried out exclusively abroad under the freedom to provide services.

8.3. The EU FIUs Platform

The activity of the FIUs Platform[36] last year centred on matters relating to implementation of the new European rules, which introduce new forms of cooperation, and on the development of proposals for the ongoing revision of European AML arrangements.

Contacts with the European authorities were intensified during the year, and coordination was tightened with the Italian customs agency for implementation of Regulation (EU)/2018/1672. By the end of June 2021, the FIUs must obtain access to multiple types of information on physical cross-border movement of cash: declarations for amounts above €10,000, suspicious cases detected in the course of controls, failure to make the required declaration.

The Platform examined the contents and formats of the data to which FIUs will have access and began discussion on the future mode of connection between FIUs and the European Customs Information System, which will bring together the data acquired from national customs agencies.

The Platform also organized an initial survey on forms of cooperation between FIUs and the national and European prudential and AML supervisors, introduced by the CRD-V Directive and the EBA Regulation. The FIUs met with the EBA, which is empowered to adopt guidelines on this matter, to discuss the characteristics and scope of future cooperation such as to facilitate performance of their respective tasks of analysis and supervision (see Section 9.1.1, 'European regulatory developments').

In the framework of the EU Commission's 'Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing' (see Section 9.1.1, 'European regulatory developments'), the European FIUs have developed analyses and proposals for the design of a new European AML system, with special regard to harmonizing the rules on suspicious transaction reporting and cooperation. The focus will be on the characteristics and tasks of the 'European Support and Cooperation Mechanism' for FIUs, with specific, detailed proposals.

An ad hoc technical working group was instituted to develop ideas based on operational experience and serving the practical needs for greater efficiency in analysis and cooperation, in particular given the highly diversified overall situation and the necessity to cope with significant risks entailing a cross-border dimension.

[36] The Platform, which has been active since 2006 and was formally recognized by Article 51 of the Fourth Directive, is the forum in which EU FIUs and the Commission discuss application of European rules, development of instruments of analysis and cooperation, and the conduct of joint operations.

The working group, with the UIF's active participation, has identified the areas of activity where the application of the Mechanism will be most useful, indicating in particular joint analysis of cross-border cases, the specification of the sources of information that FIUs should be able to access, and the management and development of FIU.NET and of other IT tools to support cooperation among FIUs.

Through the Advisory Group, the body that the Platform uses to follow the management of FIU.NET, the FIUs have dealt with the complicated questions involved in the migration of the system from Europol to the European Commission.

The Platform has also furthered the identification of supranational risks, based on the sharing of updated typologies emerging from analyses and of vulnerabilities relating above all to the development of new, technology-intensive and highly innovative forms of economic activity. The ideas developed are not only channeled into individual, national risk assessments but also contribute to the updating of the Commission's Supranational Risk Assessment.

Operationally, the Platform continued to foster and support joint analyses of cases of cross-border relevance. The results constitute a substantial contribution of methods and experiences for work towards the design and launch of the activities in this field that will be assigned to the European Mechanism.

Joint analyses

At the Platform meeting of 1 December 2020 the UIF presented the conclusions of the joint analysis exercise, conducted together with the FIUs of France, Germany, Spain and Hungary, on financial flows from Italy and other European countries stemming from tax and customs violations in commercial transactions with China. The analysis is based on a series of investigations done by the UIF with the cooperation of the Customs and Monopolies Agency, which in turn was in contact with its counterparts abroad. Using the secure channels of cross-border information exchange, the team of analysts designated by the FIUs shared the information in their databases and the data acquired from outside sources and obliged entities; the team performed joint analysis of this information, working out the complex operational scheme with the various countries. The work was done in virtual mode, with regular contacts.

The very substantial remittance outflows of years past have now been replaced by transfers, either credit transfers or physical transport of cash, associated with large-scale commercial operations in connection with imports of goods from China, settled for under-invoiced amounts. The overall operating scheme, which embraces real – not fictitious – international shipment of goods, was reconstructed by comparing financial, corporate and customs data. Companies that import goods from China are common throughout the countries of the Union, and concentrations of them were found in particular in Italy, France, Germany, Spain, Greece, Portugal, Slovakia and Slovenia. These firms make credit transfers to 'central treasurers' located mostly in Hungary. A portion of the transfers is made in cash, shipped and deposited in Hungary without the requisite declarations. The funds are then collected and rerouted from Hungary to China. Both the importing firms and those acting as treasurers are ultimately controlled by Chinese individuals and organizations. The customs agency checks (at European and global level, like the FIUs' analyses) indicated that the goods imported generally take routes different from those of the financial flows, which highlights the need

for more thorough study of customs inspection activity and of the application of the 'customs transit' procedure[37] in some European countries.

The findings of the joint analysis are set out in a detailed operational report, transmitted by the UIF to the Special Foreign Exchange Unit of the Finance Police, the DIA and the DNA.[38]

8.4. Developments in the FIU.NET

FIU.NET is the European Union IT infrastructure for cooperation and information exchange among FIUs for AML financial analysis.[39]

On 1 January 2016, Europol became the service provider for FIU.NET. The FIUs take part in the system's governance through the Platform and a special Advisory Group. On 19 December 2019, following an inquiry, the European Data Protection Supervisor delivered an opinion prohibiting Europol from continuing to manage the network and ordered its cessation, in that it violated the data protection rules. The EDPS argued that the suspicious transactions subject to information exchange via FIU.NET are administrative in nature, as support to the FIUs' duties of financial analysis, and do not relate to crimes or criminal investigations, to which Europol's tasks are restricted. The EDPS suspended the application of the order until 19 December 2020, allowing time for the transfer of the infrastructure to another organization without interrupting operations.

The FIUs Platform initiated work on an alternative to Europol for the management of FIU.NET. It accepted the Commission's offer to host the network on a temporary basis, with a view to eventually assigning this task to the nascent European Support and Cooperation Mechanism for FIUs (as indicated in the Commission's Action Plan of 7 May 2020).

The Commission's plan for FIU.NET would mean substantial change to the configuration of the system. The network would become physically centralized, with the transfer to the Commission itself of the local servers currently located at the individual FIUs, where the data on cross-border exchanges are entered and conserved. The transfer of FIU.NET to the Commission is to be accompanied by adequate governance arrangements giving the FIUs direct, independent influence on the system's management.

The EDPS, in its Opinion of 23 July 2020, welcomed the initiative of the Commission to boost the development of FIU.NET and to find a suitable solution for its management that is in line with the personal data protection framework. The EDPS further noted that Article 51 of the AML Directive offers the legal grounds for the Commission's temporary management of the network.[40] Given the technical complexity of the migration process, the

---

[37] The procedure allows importers to perform customs clearance formalities in a European country of their choice, not necessarily at the 'physical' point of entry into the Union.

[38] Article 13-bis(4) of Legislative Decree 231/2007, as amended by Legislative Decree 125/2019, specifies in regard to joint analyses that the UIF 'shall transmit the data and results of said analyses to the National Anti-Mafia Directorate, the Special Foreign Exchange Unit of the Finance Police, and the Anti-Mafia Investigation Department for the exercise of their respective powers, by the procedures and terms established by the memorandums of understanding referred to in Article 13(2).'

[39] Instituted in 2002, over the years the network has grown significantly in the volume of data exchanged and in the functions furnished for cooperation. It has been expressly recognized in European legislation (Directive (EU)/2018/843 – the Fifth AML Directive – and Directive (EU)/2019/1153).

[40] In this framework, data treatment is deemed to be necessary to the performance of a task in the public interest

EDPS later approved the request from Europol and the Commission to extend the suspension to 30 September 2021. On the basis of monthly progress reports, the EDPS retains the right to revoke the extension, failing sufficient progress.

The extension of Europol's transitional management of the system entails postponement of what has become an urgent need for modernization and development of the network infrastructure, now obsolescent and inadequate to the volume of data exchanged, above all in cross-border STRs. The FIUs Platform and the Advisory Group are engaged in complicated talks with the Commission to settle legal and technical issues in order to complete the transfer before the deadline of September 2021.

With a view to the eventual placement of FIU.NET at the Support and Cooperation Mechanism, it is essential to devise an arrangement that can make the most of the infrastructure for information exchange among FIUs, by means of a thorough overhaul and modernization within a governance configuration based on the full involvement of the FIUs themselves in management and decision-making.

8.5. Relations with foreign counterparts and technical assistance

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

The UIF maintained its commitment to international technical assistance in its areas of competence through bilateral and multilateral initiatives. Activities in 2020 included participation in supplying technical assistance to the AML authority and the private sector in Kosovo under the aegis of the UN Development Programme.

In this project, the Unit's experts described specific features of the AML apparatus, with special attention to due diligence as applied to PEPs, rules on transparency of beneficial ownership, risk assessment, and strategic analysis. Significant elements for support to the Kosovar counterpart were drawn from the Unit's practice and experience.

The UIF took part in a remote seminar organized by ECOFEL (the Egmont Group's training and assistance centre) in partnership with the FATF regional body for the Middle East and North Africa, attended by financial analysts and investigators from countries of the region. The panel, composed of experts chosen from among the regional representatives of the Americas, the Middle East and Europe, provided a diversified overview of experiences of cooperation between FIUs and investigative authorities.

The UIF also participates in technical assistance and support activities within the Egmont Group, and in particular the Training and Technical Assistance Working Group and the Membership, Support and Compliance Working Group. This involves assistance to FIUs in the formation or consolidation stages and the development and implementation of training and specialization programmes to enhance institutional activities. Assistance plans are also directed to overcoming problems of compliance with international standards or shortcomings in the efficacy of checking procedures.

---

or relating to the exercise of the public powers attributed to the Commission pursuant to Article 6 of Regulation (EU)/2016/679 and Article 5 of Regulation (EU)/2018/1725.

8.6. Participation in the FATF

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

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

In 2020, the Unit again participated in the work of the FATF as part of the Italian delegation coordinated by the Ministry of Economy and Finance.

The exceptional circumstances of the health emergency affected the work of the FATF, which became more flexible, owing to restrictions on movement and physical meetings. There was no significant slowdown in the activity of the working groups, and work on the various fronts proceeded largely as scheduled. There was a stronger impact on the mutual evaluation procedures, as the postponement of the necessary onsite visits significantly altered the timeframe and calendar for these interventions, with repercussions on the Plenary Meeting agenda and follow-up programmes.

The UIF's 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 follow-up checks. The UIF also cooperates directly, its experts participating in evaluations of the AML systems of individual countries to foster proper implementation of the standards and the effectiveness of the measures.

This contribution covers all the various stages of the evaluation procedure: recognition of the risks posed by each country and the quality of collaboration with the local authorities, analysis in drawing up the reports and participation in the discussion on their approval. UIF experts took part in the Mutual Evaluations of Belgium, Canada, Austria and Switzerland, the follow-up on Spain headed by the FATF, and the Mutual Evaluation of Malta carried out by Moneyval; one expert is involved in the evaluation of France. The UIF's reviewers intervened in the checks on China and on the Czech Republic (the latter as part of Moneyval).

The working groups continue to focus on in-depth analysis of the risks and opportunities connected with technological innovation and the implications for compliance and supervision (RegTech/SupTech).

Specifically, the Unit is part of the project to study the technical opportunities offered by data pooling among financial institutions for more effective monitoring of risks and suspects and the limits to data protection and secrecy, especially as regards suspicious transaction reports. The Unit is also engaged in assessing the effect of the digital transformation of AML/CFT on operational agencies.

The UIF contributes to the analysis of risks and safeguards on virtual assets. There is constant monitoring of implementation of the new, dedicated standards; study has been completed on stablecoins, transferable instruments based on blockchain technology characterized by the stability of their value, which is pegged to an underlying asset, such as legal tender currencies or guaranteed securities (see the box 'Initiatives on virtual assets' in Chapter 9). The Unit collaborated on the FATF report '*Trade-Based Money Laundering – Trends and*

Developments' by supplying case studies and sharing quantitative methods for gauging the consistency between financial flows and trade flows.

The UIF also participates in the project for reconnaissance of typologies of 'Money Laundering through Environmental Crimes,' contributing cases from its own experience traceable to trafficking and illegal disposal of waste.

8.7. Participation in other international organizations

The Egmont Group

The Egmont Group, the worldwide organization of FIUs, increased its membership to 166 in 2020. The UIF is an active participant, in particular contributing to the development of policy and guidelines for cooperation, reconnaissance on risks and typologies of money laundering and terrorist financing, and checks on FIUs' compliance with international standards. The UIF took part in the procedures to verify FIUs' compliance with organizational standards and cooperation obligations. The purpose is to encourage alignment with the common rules and limit, as far as possible, shortcomings in analyses and exchanges deriving from insufficient capability of the FIUs to access and share information. Special attention also goes to compliance with the requirements of independence and confidentiality, which are essential if the intelligence units are to operate effectively, without undue outside interference.

Examination of the regulatory framework governing the action of the Swiss FIU proceeded. In response to the observations of the Egmont Group, Switzerland made legislative changes that should guarantee adequate capacity of the intelligence unit to obtain financial information and exchange it with FIUs abroad. Checks were also begun on FIUs that displayed weaknesses in the protection of data confidentiality and in safeguards against political influence, which took the form of unjustified dismissal of units' top management by the government.

Preliminary studies were begun for an overhaul of the Group's IT infrastructure to renovate the global network of information exchange among FIUs with the introduction of new functions (similar to those provided by FIU.NET in Europe). At the same time, new models for management of the Egmont Secure Web are being considered, embodying higher standards of security and requirements of 'neutrality' for the system manager.

The UIF was involved in the projects for reconnaissance of the international set of providers of virtual asset services (designed to promote knowledge of the entities operating in this sector, typically on a cross-border basis) and on the laundering of the proceeds of corruption and the related action to recover the assets. The latter project, of which the Unit is coordinator, relates closely to the priorities of the G20, under Italian presidency in 2021. The Unit also conducted further inquiry into the possible methods and instruments for analysis of transactions in virtual assets, directed to discussion of the innovative approaches developed by various FIUs to deal with totally unprecedented phenomena.

Special policy relevance attaches to the Group's continuing work to update methods and requisites for checks on compliance and on the effectiveness of individual FIUs. The Group's broad membership makes this task at once essential and burdensome. Sanctions are always preceded and accompanied by support and technical assistance, developed in part through special global programmes.

A UIF staff member has been named Egmont regional representative for the FIUs of the European Union. This regional group contributes to the organization's overall action and

at the same time sponsors studies directed to input and proposals for the development of the European AML system.

Moneyval

As a member of the Italian delegation, the UIF is an assiduous participant in the activities of Moneyval, which is the Council of Europe's anti-money-laundering organization and part of the FATF's global network.

One of the UIF's experts provides support for the activities of the Conference of the Parties under the Council of Europe's 2005 Warsaw Convention on Money Laundering and Financing of Terrorism. The tasks of the Conference include monitoring the transposition and implementation of the Convention by the signatory nations. It avails itself of the analyses of the FATF and Moneyval in their respective activities of mutual evaluation of the member countries and carries out targeted checks of its own on national AML systems, resulting in evaluation reports. In 2020, the Conference examined the transposition of the Convention's provisions for investigative powers to monitor bank accounts and for the reversal of the burden of proof concerning the provenance of assets subject to seizure.

The Report on Italy cites the power of investigative bodies to acquire bank records in order to monitor the use of specified accounts and, where necessary, execute timely seizures. It specifically cites the role of the UIF in cooperation on financial investigations. The evaluation report describes Italy's compliance as satisfactory but not full, given the lack of clear regulations and practical examples.

The FinCEN Files case - developments and impact

On 20 September 2020, confidential information was published concerning more than 2,100 Suspicious Activity Reports filed with FinCEN by banks between 2000 and 2017. The data, procured illegally from the archives of the U.S. Financial Intelligence Unit, were leaked to the American journalistic site 'BuzzFeed.' The latter then shared them with the International Consortium of Investigative Journalists (ICIJ), which brings together reporters in a hundred countries. The reports obtained by the ICIJ bear on transactions worth a total of more than $2 trillion, carried out (and reported to FinCEN) mostly by financial institutions of global dimensions.

This case constitutes a breach – unprecedented both in the mode of dissemination, with integral data, and in the extent of the information published – of an FIU's secrecy protections for suspicious transaction reports and its IT security. In many instances, the data bear on international activity, not limited to the United States. The global banks involved, in fact, report to FinCEN transactions on markets throughout the world, often complex and for very substantial sums, by organizations or entities with enormous amounts of liquidity.

At the conclusion of further study lasting 16 months, the ICIJ released excerpts of the data acquired. They are organized in a database of the transactions and banks involved, accompanied by search tools. In addition, a good number of SARs in original format and content were published. The ICIJ also published several further articles on cases and developments of particular interest.

The leaking of confidential information held by FinCEN does not appear to have involved data from any other FIUs, exchanged as part of international cooperation. The US intelligence unit offered reassurance in this regard, specifying also that the affair cannot be ascribed to shortcomings in its IT security. The Egmont Group has begun a check to reconstruct exactly what happened.

9. THE LEGISLATIVE FRAMEWORK

The UIF follows the development of EU anti-money-laundering policies and rules. It contributes, with its own proposals and research, developed also in coordination with the other European FIUs, to the evolution of the European AML/CFT rules.

The Unit also follows and cooperates in the development of Italian primary and secondary legislation by other authorities in the matters affecting it. In this context the Unit carries out studies of issues relevant to the effectiveness of the AML prevention system, drafts legislative and regulatory proposals and takes part in inter-institutional technical talks and parliamentary hearings.

The Unit drafts and issues Instructions concerning the identification and reporting of suspicious transactions by the obliged entities, the dispatch of threshold-based communications, the transmission of communications from general government bodies and the transmission of aggregated data.

With a view to fostering active cooperation on the part of the obliged entities, the UIF issues and regularly updates anomaly indicators for the identification of suspicious transactions after presenting them to the Financial Security Committee; it develops and disseminates representative models and patterns of anomalous economic and financial behaviour that relate to possible money laundering or terrorist financing. The Unit also issues system-wide communications calling the attention of the obliged entities to certain risk factors and elements symptomatic of possibly illicit operations.

9.1. The global and European context

9.1.1. European regulatory developments

The Commission's Action Plan

On 7 May 2020, the European Commission published its *Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing*. The Plan is the outgrowth of prolonged studies which, for the part concerning FIUs, were initiated by the FIUs Platform with its Mapping Exercise on the characteristics and powers of European FIUs and cooperation among them; the Plan also reflects analyses of the main weaknesses of the EU AML apparatus indicated in the four reports published on 24 July 2019 together with the Communication to the Council and the Parliament 'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework.'[41]

The Action Plan does not make definitive choices but sets out policy options and lines of action, discussed in a public consultation that was concluded on 26 August 2020. One important definitive choice was made, however: the transfer of management of FIU.NET from Europol to the Commission pending its successive passage to the nascent 'European Support and Cooperation Mechanism' for FIUs (see Section 8.3, 'The EU FIUs Platform'). The new rules, scheduled for adoption in 2023, will be laid down in a series of legislative proposals by the Commission, subject to the customary negotiations with the Council and the Parliament.

[41] See UIF *Annual Report for 2019,* pp. 106-109.

The Action Plan: The main elements

The Action Plan builds on six pillars: more effective implementation of European rules at national level; greater harmonization of the rules, among other things by means of a regulation, which is directly applicable; European supervision arrangements, with the institution of a supranational body; closer cooperation among FIUs, thanks to the European Support and Cooperation Mechanism; more incisive criminal law enforcement; and a stronger role of the European Union in international AML policies and in interaction with third countries.

Transposition of the Fourth and Fifth Directives. The Plan recalls the initiatives to encourage proper transposition of the new European rules into national law. These initiatives consist in infraction procedures against a good number of Member States, in ad hoc assessments of the adequacy and effectiveness of the individual national systems, and in assignment to the EBA of the tasks of verifying adequate exercise of AML supervision by the national authorities and of discovering violations of the European requirements.

S**ingle EU AML rulebook**. Under the present system of minimum harmonization, harmful discrepancies persist in such areas as the range of obliged entities, customer due diligence, and the powers of the FIUs. The Plan calls for transposing substantial parts of the Directive into a Regulation, which will envisage more detailed provisions. The new provisions, supplemented by technical standards for application, will result in a detailed AML rulebook.

European AML supervision. The supranational system of AML supervision should bring the various national systems together to overcome the problems caused by fragmentation. In this context, the national authorities would remain responsible for supervision in ordinary cases, while the new European authority would take over tasks of direct AML/CFT supervision vis-à-vis the highest-risk obliged entities. On this point, the Plan retains an open approach, presenting several possible ways of dividing spheres of competence between national and European level. Also left open is the question of the scope of action of the European supervisor, i.e. whether it should be limited to the financial sector alone or extended also to part or all of the non-financial sector, it being understood that the latter too must be subject to some form of supranational supervision.

European FIU Mechanism. On the possible configuration of the new mechanism, see the box below, 'The European Support and Coordination Mechanism for FIUs: From the Action Plan to the Common Position'.

The EU Council Conclusions of 5 November 2020 welcomed the reform of the European AML system as outlined in the Action Plan. These Conclusions followed an analogous position taken by the Council in December 2019.[42] They touch on three of the Plan's six pillars for reform: the harmonization of AML rules, the institution of a European AML supervisory system, and the European Mechanism of Support and Coordination for FIUs.

[42] See UIF, *Annual Report for 2019*, p. 109.

The Council underscores the need for proposals for the new regulatory framework and the new European authorities to be drafted, presented and discussed together, for a comprehensive and organic assessment. It confirms the need to institute a supranational level of AML supervision and to comply with certain conditions in this process of centralization: graduality in defining the scope of supranational intervention, with priority to the regulated financial sectors that are most exposed to risks; the central role of the national authorities, in keeping with the subsidiarity of the European supervisor; the coordinating role of the latter, with the right of arrogation and also powers of direct intervention; and capacity for cooperation with other European and national authorities (among them the FIUs and their Mechanism).

The FIUs Platform has formed a working group, including the UIF, to draw up concrete proposals for the Commission concerning the duties, characteristics and organization of the future European Support and Cooperation Mechanism for FIUs.

The Ministry of Economy and Finance and the UIF have proposed a Common Position among Member States on the tasks and characteristics of the nascent Mechanism. A joint position paper subscribed by eight countries was delivered to the Commission in December 2020. It argues that the Mechanism needs to be assigned major tasks of support for the work of the FIUs, while keeping the core functions of the FIUs – reception, analysis and dissemination of STRs – solidly anchored at national level.

This Italian initiative flanks an earlier one promoted by the Dutch government on the characteristics of European AML supervision and, as a complement, fills a political vacuum concerning the development of the European framework to reinforce FIUs. The new initiative puts Italy in a leadership position on an issue that is fundamental to the effectiveness of the entire apparatus for preventing money laundering, capitalizing on the role of financial analysis and inter-FIU cooperation.

The European Support and Coordination Mechanism for FIUs: from the Action Plan to the Common Position

The Commission's Action Plan reaffirms the need for a supranational Mechanism for support and coordination of FIUs within the Union.[43] The Mechanism should be given the tasks of setting the criteria for identifying cross-border suspicious transactions, promoting joint analyses, detecting trends and factors of risk of money laundering and terrorist financing at both national and supranational level, and strengthening cooperation between authorities nationally and internationally as well as with third-country FIUs. The Plan also notes the possibility of the Mechanism's adopting or proposing implementing provisions to facilitate the creation of a single rulebook.

The Conclusions set out by the Council of the European Union on 5 November 2020 furnish the Commission with guidelines on the organization and its tasks. The Council specifies that the new European authority must have solid guarantees of independence like those enjoyed by the national FIUs. Further, while the FIUs' core functions shall remain solidly anchored at the national level, consideration is given to assigning the Mechanism tasks relating to the definition of methods and instruments in support of the FIUs' operations and empowering it to adopt guidelines and binding technical formats.

The Common Position called for by the Ministry of Economy and Finance and the

[43] See UIF *Annual Report for 2019*, pp. 109-110.

UIF fits into the framework of the Council's Conclusions, developing its references to the Mechanism's role in various spheres and remaining fully consistent with the studies and technical proposals of the European FIUs as part of the ongoing reflection within the Platform. The Position specifies that the tasks of the new European body must not include the core functions of the FIUs: that is, reception of STRs, analysis and dissemination must remain at national level.

Under the principle of subsidiarity, the Mechanism should concentrate on working methods and practices, on types of analysis that cannot be performed effectively at the national level alone and on international cooperation. It must furnish real support to the single FIUs and avoid duplication of activity.

The Common Position argues that the Mechanism should foster convergence in the content of STRs by issuing technical standards; specify common criteria or best practices as regards the 'financial,' 'administrative,' and 'investigative' information that the FIUs must have available for effective analysis; foster the alignment of analytical tools and methods, which is essential also for joint analyses; and develop a common concept of cross-border STR, accompanied by consistent procedures and standards for automated data exchange.

The emerging consensus on the need to make the most of the functional synergies between FIUs and AML supervisors, to contain costs and to guarantee the necessary independence of the FIUs suggests the institution of a new EU AML Agency to comprise, on an equal footing and with symmetrical organizational architecture, the European AML supervisor and the Mechanism.

The institution, organization and functions of the new Agency will be set out in a regulation, following the same approach used for other European agencies (the ESAs, Europol, etc.). Its governance and organization must be consistent with the provisions generally established for these European bodies while also guaranteeing independent action, confidentiality and security in the treatment of information. In this framework, the Mechanism will have its own staff and budget, and the single FIUs will play a direct role, through designated experts, in its operations (above all joint analyses).

Cooperation between FIUs and supervisory authorities

Close relations and flexible channels for dialogue between FIUs and AML supervisory bodies must be maintained on both the national and the European plane. Serious shortcomings in this coordinating machinery, especially in countries where the FIU is patterned on the 'law enforcement' model, have been among the causes of the recent episodes of money laundering and poor governance that overwhelmed various European banks, resulting in instability. The close relation between the FIU and the supervisory entity has been a hallmark of the Italian system.

The new European rules instituting forms of cooperation and information exchange between FIUs and prudential and AML supervisors, both national and European, required studies to determine appropriate procedures for uniform implementation. The European FIUs took part in discussions with the EBA with a view to preparing special guidelines.[44] The principles underlying the UIF's contribution bear first of all on confidentiality safeguards and the limits to the use of information on STRs and the related analyses, the linkage between

[44] Guidelines issued by the EBA pursuant to Article 117(6) of CRD-V, specifying the procedures and the information to be exchanged between prudential supervisory authorities, AML supervisors, and FIUs.

the new forms of cooperation with supranational bodies and diagonal information exchanges, which even in the absence of harmonized European rules need to develop without overlapping or interference.

Brexit and AML defences

In an ever more closely integrated European AML/CFT framework, the final entry into force of British exit from the EU necessitates action to guarantee the continued presence, vis-à-vis operators in the UK, of adequate defences against money laundering and terrorist financing.

Brexit and defences against money laundering

On 31 December 2020, with the end of the transitional period under the Withdrawal Agreement that took effect in February 2020, the United Kingdom became to all intents and purposes a third country with respect to the European Union, exiting from the scope of European rules. The relations between EU and UK following Brexit are governed, in addition to the Withdrawal Agreement, also by a Trade and Cooperation Agreement signed on 24 December 2020.

As regards financial services, Britain's departure from the Union and the single market means that intermediaries established in the UK lose their 'passporting rights' and consequently, if they are to continue to do business in the EU, must apply to the competent national authorities for authorization like intermediaries constituted in third countries. The December agreement does not recognize any form of regulatory 'equivalence', which in the post-Brexit regime is the prerequisite for admitting these financial institutions to the single market. Limited provisions for recognition are envisaged to allow for business continuity on the part of undertakings that provide the services of clearing and settlement of financial assets. The definition of the conditions and procedures required for this type of recognition is left to a separate Memorandum of Understanding.

The Trade and Cooperation Agreement makes no express reference to defences against money laundering and terrorist financing that should be maintained or introduced following the UK's withdrawal from the Union. It does indicate the necessity that the parties exchange relevant information, where appropriate, in compliance with their respective legal systems. It also recalls the United Kingdom's duty to guarantee the transparency of beneficial ownership of entities and companies, with generic reference to the FATF standards and the corresponding EU provisions.

The agreement does not address the issue of cooperation between the British FIU and those of the European Union. The end of the transitional period terminates the reciprocal obligation to transmit STRs on transactions with cross-border features. It also eliminates Britain's obligation to transpose Directive (EU)/2019/1153 on domestic and international cooperation between FIUs and investigative bodies. Further, the British FIU will no longer have access to FIU.NET; operational cooperation will rely on the Egmont network, under the same rules as those applicable to all extra-European FIUs.

The soundness of the United Kingdom's AML defences will be assessed with a view to recognition of some form of equivalence. Although it remains broadly compatible with the European rules for the time being, in the future the British anti-money-laundering system could gradually diverge. It is important to make sure that Brexit does not result in a new kind of race to the bottom and regulatory arbitrage, in the context of continuing close economic integration. In this regard, it will be necessary also to avoid uncertainties and discontinuity in operations and inter-FIU cooperation. Accordingly, the UIF contin-

ues to pay close attention and to be receptive to bilateral relations with its British counterpart.

9.1.2. Further European and international initiatives

Transposition of the AML directives

In the course of 2020 the Commission continued to monitor correct transposition into national law of the fourth and fifth AML directives – the time limits for doing so having expired[45] – taking account of the measures notified by the Member States. Special attention was paid to the institution of national central registers of the beneficial owners of companies and trusts, which must be interlinked among Member States, and of databases or equivalent information systems for the identification of bank accounts.[46]

The Commission initiated several infraction procedures for failure to notify the transposition measures or for incorrect or incomplete transposition. Specifically, for some Member States the Commission found problems in the transposition of certain provisions of the fourth directive, relating in particular to the powers of the FIU, international cooperation, due diligence requirements and transparency of beneficial ownership information. In addition, it found instances of tardiness in communicating the transposition measures of the fifth AML directive.

The monitoring also extended to the practical application of money laundering provisions. Where they are deemed inadequate, the Council can make specific recommendations to the country involved. In support of national efforts and in order to facilitate uniform AML defences, the Commission undertakes technical assistance in the framework of ad hoc programmes.

High-risk third countries

On 7 May 2020, the Commission issued a new delegated regulation[47] identifying third countries at high risk of money laundering or terrorist financing by reason of strategic deficiencies in their AML systems.[48]

At the same time, the Commission issued a Methodology for the comprehensive and uniform assessment of third countries' degree of risk.[49] Given the necessity of compatibility with the equivalent assessment programmes of the FATF, the methodology reaffirms that the latter's 'blacklist' is the starting point for the European list of high-risk countries, which will be supplemented, however, by an independent risk assessment from the specifically European perspective, taking account of additional factors.

Within the planned European AML system, the new supranational bodies can participate directly in risk assessment of third countries. The AML Supervisor and the FIUs Mechanism, each from its own standpoint, will help to detect third-country practices presenting possible threats and to identify vulnerabilities, in necessary liaison with the competent national authorities and drawing on their experience (for example, as regards cooperation with the relevant third-country authorities). The new bodies, given the powers assigned to them, can also take appropriate measures for risk mitigation.

---

[45] On 27 June 2017 for the fourth and 10 January 2020 for the fifth directive.

[46] The Commission must present to the European Parliament and the Council a detailed report on implementation of the Directive by 11 January 2022, and must report every three years from then on, as per Article 65(1).

[47] Regulation (EU)/2020/855 amending Regulation (EU)/2016/1675.

[48] In compliance with Article 9 of the fourth directive, as amended by the fifth directive, which assigns the Commission the task of compiling a list of third countries at high risk for the Union.

[49] See UIF *Annual Report for 2019*, p. 111.

9.2. The Italian legislative framework

Throughout 2020, the Unit followed the development of emergency legislation in connection with the COVID-19 epidemic, suggesting adjustments and regulatory changes to improve and supplement the measures adopted, so as to combine liquidity support and bureaucratic simplification with the defence of legality. Limited changes were made to the AML rules as regards customer due diligence and identification, for more streamlined and secure compliance procedures in the case of remote operations.

In the sphere of secondary legislation, the UIF issued its new Instructions for Aggregate AML Reports and disseminated typical patterns of anomalous behaviour regarding transactions in connection with tax violations.

9.2.1. Legislative measures

The 'Cure Italy' decree[50] suspended the time limit for administrative proceedings for non-compliance with legal obligations (Article 103) and enacted provisions to facilitate notification by mail (Article 108).[51]

The time limit was suspended from 23 February to 15 April 2020; subsequently, Article 37 of Decree Law 23/2020 further suspended it to 15 May.

Liquidity Decree

The 'Liquidity' Decree,[52] which introduced urgent measures of support to enterprises, laid down that in the concession of guaranteed financing in connection with the COVID-19 emergency, the AML reporting requirements remained in effect (Article 1-bis(5)). In order to facilitate tracing of financial flows stemming from the access to credit, the decree also required the exclusive use of dedicated bank accounts[53] for loans guaranteed by SACE SpA.[54]

Applications for financing must include specification by the firm's owner or legal representative of the dedicated bank account to credit. Operations on that account require the indication, in the payment details, of the formula: 'Support pursuant to Decree Law 23/2020.'

In addition, credit access for SMEs was facilitated by easier activation of the Guarantee Fund, with increased recourse to self-certification. The declarations attached to applications for loans guaranteed by the Central SME Guarantee Fund also enjoy simplified forms for the lender, but the AML reporting requirements remain in place.

The decree does not explicitly mention the requirements of customer due diligence and record-keeping. The Bank of Italy, in its 'Recommendation' of 10 April 2020 (only in Italian), nevertheless specified that all the anti-money-laundering obligations had to remain in place, adjusting the intensity of controls as a function of risk.

---

[50] Decree Law 18/2020 converted with amendments into Law 27/2020.

[51] See UIF *Annual Report for 2019*, p. 119. On the impact of these measures on the UIF's own activity, see the 'Communication of 27 March 2020' (only in Italian), containing temporary measures and notices to mitigate the impact on entities obliged to transmit data and information to the UIF.

[52] Decree Law 23/2020 converted with amendments into Law 40/2020.

[53] Article 1-bis(3) of Decree Law 23/2020, converted with amendments into Law 40/2020.

[54] Member of the Cassa Depositi e Prestiti group; CDP SpA in turn is controlled by the Ministry of Economy and Finance and partly owned by bank foundations.

Relaunch Decree

The 'Relaunch Decree'[55] enacted additional urgent measures on health and support for employment and the economy, as well as social policy measures in connection with the COVID-19 emergency.

The measures include: i) creation of the 'SME Capital Fund' for subscription of newly issued bonds or debt securities (Article 26); ii) the 'Relaunch Fund', a dedicated fund that Cassa Depositi e Prestiti SpA is authorized to constitute for interventions and operations to support and relaunch the Italian economy and productive system (Article 27); iii) guarantee provided by SACE for trade credit insurance (Article 35); and iv) various forms of assistance, including direct subsidies, reimbursable advances and tax breaks (Article 54) plus guarantees on loans to firms (Article 55).

CDP must use the Relaunch Fund, worth over €40 billion, to finance firms via equity or debt instruments and the like. In order to ensure rapid and effective intervention while also reinforcing legal safeguards, the law provides that CDP may sign cooperation agreements with public institutions and administrations, including supervisory entities. Pursuant to this, CDP and UIF signed a memorandum of understanding to facilitate fulfilment of the suspicious transaction reporting requirements in managing the Fund, also in cases of rejection of an application or revocation of financing.

To prevent criminal infiltration, a memorandum of understanding governing anti-mafia controls was agreed to by the Ministry of the Interior, the Ministry of Economy and Finance, and the Revenue Agency. It was also specified that in cases of undue receipt of funds, Article 316-ter of the Penal Code shall apply (undue receipt of disbursements at the expense of the state).

Simplification Decree

The 'Simplification' Decree[56] modifies the AML rules to facilitate the acquisition of new customers at a distance. The check on the customer's identity document can be dispensed with; identity is verified on the basis of documents, data and information obtained from a reliable independent source.[57] However, where the customer is physically present, the i.d. document still has to be presented. In order to facilitate operations despite the measures for social distancing, the forms of digital identity for remote identification are extended.

The obligation of remote identification is fulfilled if the customer possesses a digital identity with a level of security that is 'at least significant', in lieu of the previous requirement of maximum security. The law introduces a specific method for remote identification, namely the customer's execution of a credit transfer or direct debit to or from a payment account in the name of the person to be identified, on condition that the credit transfer or debit is ordered following credential-based electronic identification.[58] In addition, the truthfulness of the identification data set out in the documents and information acquired upon identification must be verified only in case of doubts, uncertainties or inconsistencies.

---

[55] Decree Law 34/2020 converted with amendments into Law 77/2020.

[56] Decree Law 76/2020 converted with amendments into Law 120/2020.

[57] Legislative Decree 231/2007, Article 1(2.n) and Article 18(1.a).

[58] Legislative Decree 231/2007, Article 19 (1.a.4-bis). The procedure is envisaged only for the institution of a continuous relationship with reference to payment cards and the like, as well as payment instruments based on telecommunication, digital or IT devices, except for cases in which said cards, devices or instruments can be used to generate the information necessary for directly executing a credit transfer or direct debit to or from a payment account.

Another piece of new legislation during the year was Legislative Decree 100/2020[59] transposing Directive (EU)/2018/822, the Directive on Administrative Cooperation (DAC 6) for mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements.[60]

Legislative Decree 100/2020

The new rules require communication to the Revenue Agency of cross-border arrangements designed to evade automatic information exchange on financial accounts or to prevent identification of beneficial owners by means of opaque structures. Intermediaries and taxpayers are required to notify the Revenue Agency of relevant cross-border arrangements, i.e. those with at least one of the hallmarks of risk of tax evasion and avoidance listed in Annex 1 to the decree.[61] The obligation applies to intermediaries and professionals that, as regards the arrangement, have acted as promoter (responsible for planning, organization, and marketing) or service provider (either materially or through assistance and consultancy).

The intermediaries and professionals, where the conditions referred to in Article 35 of the AML decree obtain, may thus be subject to a dual obligation, albeit at different times, to the Revenue Agency and to the UIF. [62]

Some of the rules on communication to the Revenue Agency are as in Legislative Decree 231/2007 for STRs.[63] Some of the hallmarks of cross-border arrangements refer to operations that may be subject to STRs, in consideration among other things of the indications of the recently issued anomalous patterns of behaviour as regards tax violations, with special reference to international tax evasion consisting in the removal of domestic tax base through exploitation of differences in different national tax systems.

Implementation of Directive EU/2019/1153

The EU delegation law for 2019 was enacted (Law 53/2021), transposing a number of directives, including Directive (EU)/2019/1153, with provisions to facilitate the use of financial and other information for prevention, ascertainment, investigation or prosecution of serious criminal offences (the deadline for transposition was 1 August 2021).[64]

The implementation of the Directive concerns access to the UIF's financial information and analyses, hence the question of the Unit's cooperation with other institutions, which had already been raised on occasion of the AML reforms of 2017 and 2019.[65] The Unit's Director

---

[59] Effective from 26 August 2020; the implementing provisions were issued by the Ministry of Economy and Finance by a decree dated 17 November 2020 and by the Revenue Agency with a measure dated 26 November.

[60] The Directive is intended to provide tax authorities with timely, comprehensive and relevant information about potentially aggressive tax planning designed to reduce tax liabilities and transfer taxable earnings to jurisdictions with more favourable tax regimes.

[61] These are conditions relating to the criteria of tax residence of participants in the arrangement, the conduct of business by means of a permanent organization in a foreign jurisdiction or the possibility that the arrangement may distort the correct application of the procedures of automatic information exchange or identification of beneficial owners.

[62] The communication requirement vis-à-vis the Revenue Agency has a time limit of 30 days from the day after the cross-border arrangement becomes available for activation or that in which its activation is initiated or from the day after the assistance or consultancy for purposes of activation of the cross-border arrangement is provided.

[63] In particular, there is a possible exoneration analogous to that for STRs transmitted by professionals, and it is specified in any event that the communications to the Agency, where made for the purposes envisaged and in good faith, shall not constitute a violation of any contractual or legislative, regulatory or administrative restrictions on the divulgence of information and shall not entail liability of any kind.

[64] See UIF *Annual Report for 2019*, p. 105.

[65] See UIF *Annual Report for 2019*, p. 114.

spoke in favour of the broadening of information exchanges in testimony before the Parliamentary Anti-Mafia Commission on 16 July 2020. In the presentation he noted that the purposes of the new Directive extend beyond the regulations on money laundering. The intent, in fact, is to permit the use of financial intelligence, and specifically that in the possession of FIUs, by the authorities assigned to prevent and suppress serious criminal offences, and not only economic or financial crimes. This will require different choices in terms of the scope of information exchange; retaining the narrow set of authorities envisaged by the AML rules would threaten to result in a failure on Italy's part to transpose the new Directive. Given the existing institutional structure and AML competences, Article 21 of the Chamber of Deputies transposition bill (AC2757) contains no directive criteria that serve the need to designate a broad range of eligible authorities, in keeping with the purposes of the Directive.

Virtual assets

The UIF continues to follow regulatory developments regarding virtual assets, with a view to producing specific proposals for the institution of a uniform, effective AML/CFT regime in this area.

Regulatory initiatives on virtual assets

Global and European rules on virtual assets are being adapted to regulate an expanding sector that is frequently interconnected with the services provided by financial intermediaries (See Section 5.1, 'Inspections'), raising the need to protect consumers and investors and to safeguard market integrity.

In June 2020, the FATF released the *Report* of the contact group of countries engaged in promoting implementation of standards on virtual assets. The report recalls the main uses of virtual assets for illegal purposes and gives an overview of the state of implementation of the FATF's recommendations.

Also in June 2020 the FATF approved its *Report on so-called Stablecoins*, which highlights the need for monitoring of the emerging money-laundering risk of stablecoins that are: i) issued or utilized in jurisdictions where preventive safeguards are incomplete or wholly lacking; ii) based on decentralized operating systems not providing for the presence of AML-obliged entities; iii) transferred in peer-to-peer transactions via unhosted wallets, i.e. absent any entity that can apply AML/CFT safeguards.

In September 2020 the FATF published its 'Red Flag Indicators' for virtual assets in order to assist intermediaries, professionals, non-financial operators and virtual asset service providers (VASPs) in identifying suspicious conduct.

Relevant factors may be the size or frequency of transactions in virtual assets, certain transactions that are unusual or serve to maintain anonymity, as well as the recurrence of geographical risk.

A project team of which Italy is a member has been formed to revise and update the FATF Guidance published in 2019 for implementation of the AML/CFT defences in connection with virtual assets. The new guidelines will clarify the concept of virtual assets and VASPs, in part by means of practical examples, to make sure that no relevant cases escape application of the standards.

Within the European Union, on 24 September 2020 the Commission released a proposal for a Regulation on Markets in Crypto-assets (MiCA).[66] The regulation would contain provisions on: i) transparency and information requirements for issuance of crypto-assets and their listing for trading; ii) authorization and supervision of providers of crypto-asset services[67] and issuers of asset-referenced tokens[68] or e-money tokens;[69] iii) the management, organization and governance of the aforesaid crypto-asset issuers and service providers; iv) consumer protection as regards the issuance, trading, exchange and custody of crypto-assets; v) measures to prevent market abuses.

The proposed MiCA Regulation has no specific provisions regarding AML/CFT, although it 'should also contribute to the objective of combating money laundering and the financing of terrorism.'[70]

As far as Italian AML regulations are concerned, ad hoc legislative amendments are required to complete the adaptation of Legislative Decree 231/2007 and its implementing measures to the recommendations of the FATF. The main problem in connection with virtual asset services is the cross-border dimension of crypto-assets, which necessitates the extension of national defences also to foreign operators that do business in Italy online. In this regard, the preventive safeguards could be instituted with adequate machinery of enforcement, cooperation and information exchange among the various competent authorities.

9.3. Secondary legislation

New SARA instructions

On 25 August 2020, the UIF issued a Measure with new instructions for the transmission of Aggregated Anti-Money-Laundering Reports (SARA).[71] The technical documentation for the reports is posted on the UIF website as 'Communication of 16 December 2020' (only in Italian).[72]

The Measure modifies the Infostat-UIF membership form, revising the categories of entities subject to mandatory transmission of aggregated data specified in the reforms of 2017 and 2019, updated to take account of the Bank of Italy's 'Measure containing provisions

[66] The regulation would apply to persons involved in the issue of crypto-assets or that provide services in connection with crypto-assets within the EU; however, it would not cover those crypto-assets that correspond to legal notions already regulated at European level, such as financial instruments or electronic money.

[67] Any person whose occupation or activity consists in providing one or more services for crypto-assets to third parties on a professional basis.

[68] These crypto-assets are intended to maintain stable value by pegging to various fiduciary currencies that are legal tender, one or more commodities, one or more crypto-assets, or a combination of the foregoing.

[69] A type of crypto-asset whose main purpose is to gain use as a means of exchange and to maintain stable value by reference to the value of a currency that is legal tender.

[70] Recital (8).

[71] The Measure, which supplants the previous rules adopted by the UIF on 23 December 2013, was published in *Gazzetta Ufficiale* No. 223 of 8 September 2020. The new instructions apply starting with the reports on transactions in the month of January 2021, to be transmitted by 2 April 2021.

[72] See Section 6.1, 'Aggregated data'.

on organization, procedures and internal controls for purposes of preventing money laundering and the financing of terrorism' '(only in Italian)'.[73]

The SARA obligation is extended to fixed capital investment firms (SICAFs) and the central points of contact of providers of payment services and electronic money institutions with registered offices and central administration in another EU country.[74] The new rules also eliminate references to the Single Electronic Archive and set the threshold for aggregating transactions at €5,000 in order to ensure a more representative sample of the overall operations of the obliged entities' customers.[75] The transactions subject to aggregation do not include: i) those with obliged entities, except trust companies; ii) those with banks and financial intermediaries not subject to Community measures or with registered offices in a third country with low risk of money laundering and terrorist financing; iii) those with the persons specified in Legislative Decree 231/2007, Article 3(8) (securities depositories, market operating companies, etc.); iv) those with provincial treasuries of the central government or the Bank of Italy.

New anomaly patterns in tax matters

On 10 November 2020 the UIF published new patterns of anomalous tax behaviour (only in Italian) to assist obliged entities in meeting the requirements of active cooperation, with special reference to suspected tax offences. Four new patterns, developed together with the Finance Police and the Revenue Agency, are set out, updating and amplifying those adopted in 2010 and 2012. They relate to: A) the use or issue of invoices for non-existent transactions; B) intra-Community VAT frauds; C) international tax frauds and other forms of international tax evasion; and D) the transfer of fictitious tax credits and other improper uses.

New patterns of anomalous behaviour as regards transactions relating to tax offences

Tax evasion is one of the most frequent predicate offences for money laundering. However, the massive phenomenon of tax evasion in general comprises diverse cases with different degrees of complexity. Alongside established, recurrent patterns, there are innovative forms of evasion, often inserted in a broader criminal context so as to conceal the illegal origins of financial flows, sometimes cross-border. Some of the operations described in the Unit's patterns may therefore be closely related or complementary, constituting different phases in a single criminal design to commit tax crimes.

Pattern A, on the use or issue of invoices for non-existent transactions, hypothesizes cases of the total or partial non-existence of transactions, of over-invoicing, or of attribution of transactions to persons other than those actually involved. These types of fraudulent behaviour are often carried out through the instrumental use of 'paper mill' companies that have no staff or true operative structure, and which do not pay the taxes due.

Pattern B, on intra-EU VAT fraud (closely related to Pattern A), describes operations characterized by 'missing traders', entities often lacking an effective organization or

[73] See UIF, *Annual Report for 2019*, p. 121.

[74] UIF Measure of 25 August 2020, Article 2(1.h and 1.o).

[75] Aggregation of occasional transactions is also envisaged, with no threshold amount, for the provision of payment services and the issuance and distribution of electronic money through financial agents or through agents and persons under convention, without prejudice to the exception specified in Legislative Decree 231/2007, Article 44(3).

economic substance, constituted expressly for the operation and liquidated or discontinued shortly afterwards. In some cases, this form of fraud can be highly complex; the goods involved in an intra-Community purchase, after several transfers through buffer companies, are sold back to the original seller resident in an EU Member State, in a carousel fraud resulting in the creation of undue VAT credit positions.

Pattern C, on international tax fraud and other forms of international tax evasion, focuses on anomalous behaviour directed to the undue enjoyment of tax exemptions or reductions thanks to exploitation of international differences in tax legislation. The pattern highlights the transfer or holding of economic and financial assets abroad, fictitious residence in countries with more favourable tax regimes, and the artificial allocation of income-producing elements or their ownership to opaque jurisdictions.

Pattern D, on the transfer of fictitious tax credits and other improper uses, calls attention to the danger that the tax credits claimed may be the product of fraudulent conduct: the fictitious nature of the credits ceded, say, or their undue use to offset tax liabilities, social security liabilities and premiums effectively owed by the transferee firms.

On 11 February 2021, the UIF issued a new 'Communication' (only in Italian) for the prevention of financial crime in connection with the COVID-19 emergency. Recalling the predecessor Communication of 16 April 2020 (only in Italian),[76] it invites obliged entities to calibrate their preventive safeguards in the most effective possible manner, providing sufficient support in the rollout of the relief programmes for individuals and firms in difficulty, in an approach featuring the greatest possible active cooperation.

UIF initiatives in the COVID-19 emergency

As was anticipated by the UIF Director in his 'Testimony of 28 January 2021' (only in Italian) before the parliamentary Commission of Inquiry into mafias and other criminal organizations, including foreign organizations, the Unit's Communication of 11 February advised obliged entities of new risk factors and elements symptomatic of illicit operations that had come to light during the pandemic.

Emphasis is placed on the need for maximum synergy between the phase of application and disbursement and that of subsequent monitoring of the use made of the account credited, in consideration among other things of any constraints imposed by the relief programme.

The reporting entities' attention is also called to certain specific anomalies in connection with the supply of medical products or protective equipment, in particular the involvement of middlemen or entities linked with politically exposed persons, as well as to the fundamental importance of monitoring of public procedures and of fast-track awards of contracts.

The Communication also notes the risk of infiltration by organized crime, at times with efforts to win public procurement orders, and at times by direct or indirect management of enterprises active in economic sectors that are highly attractive or in difficulties owing to the pandemic (in addition to medicine and healthcare, other industries at risk are real estate,

[76] See UIF *Annual Report for 2019*, pp. 119-120.

construction, cleaning services, textiles, tourism, restaurants and sale of food products, funeral services and transport).

As regards IT activities, the Communication indicates illicit behaviour typical of online gaming but also offers specific warnings against operations carried out via 'advanced ATMs', payment instruments based on mobile apps, transactions on the dark web, and brokerage platforms or apps.

The Communication also cites the possible use of tax credits recognized under emergency legislation together with the danger of generalized transfers of the resulting tax credits with the aim of converting them into fungible assets.

The Communication highlights the risk of the credits themselves being fictitious, the presence of transferees using capital that may be of illegal origin, and the danger of improper conduct of financial business by unauthorized entities that carry out multiple acquisitions of credits from a broad range of transferors.

The UIF signed a memorandum of understanding with Cassa Depositi e Prestiti to support active cooperation in connection with the health emergency. The objective is to assist entities in performing their suspicious transaction reporting obligations in relation to management of the 'Patrimonio Rilancio' funds, thanks to a specific list of behavioural profiles at risk.

To enhance synergy among Italian institutions in respect of cases involving COVID-19, a procedure was introduced with the DNA for the rapid transmission of the names in the reports, so that the presence of persons known to the DNA can be detected promptly and any other elements of interest can be furnished to the National Anti-Mafia Prosecutor. The UIF also took part, along with the Finance Police and the Customs and Monopoly Agency, in ad hoc technical talks promoted by the Prosecutor for full mutual sharing of the initiatives undertaken in the course of the health emergency.

Finally, the Unit intensified dialogue with various public sector actors with a view to developing ways to make communications pursuant to Article 10 of Legislative Decree 231/2007 more effective and better targeted. Specifically, the UIF proposed that the preventive legal safeguards should include municipal information flows on business start-ups and transfers of ownership or management.

10. RESOURCES AND ORGANIZATION

10.1. Organization

The UIF is headed by the Director, who is assisted by the Deputy Director and a number of staff managers. It is structured as two Directorates: the Suspicious Transactions Directorate, for the financial analysis of suspicious transaction reports; and the Analysis and Institutional Relations Directorate, which is responsible for legislation, inspections, analysis of financial flows and cooperation with the judiciary and other domestic and foreign authorities, and also comprises the Unit's Secretariat.

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

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

The year under review was a crucial period for the organization of the Unit's work and processes. The major reorganization decided in 2019 had scarcely been implemented (in January) when the outbreak of the COVID-19 epidemic imposed another, equally sweeping organizational change, with the generalized introduction of remote working.

The new organizational structure,[77] which was put fully in place in January 2020, was designed to handle the Unit's growing work load and cope with the ever-increasing complexity of the phenomena analysed, permitting a better distribution of work assignments and responsibilities while also instituting new specialized divisions.

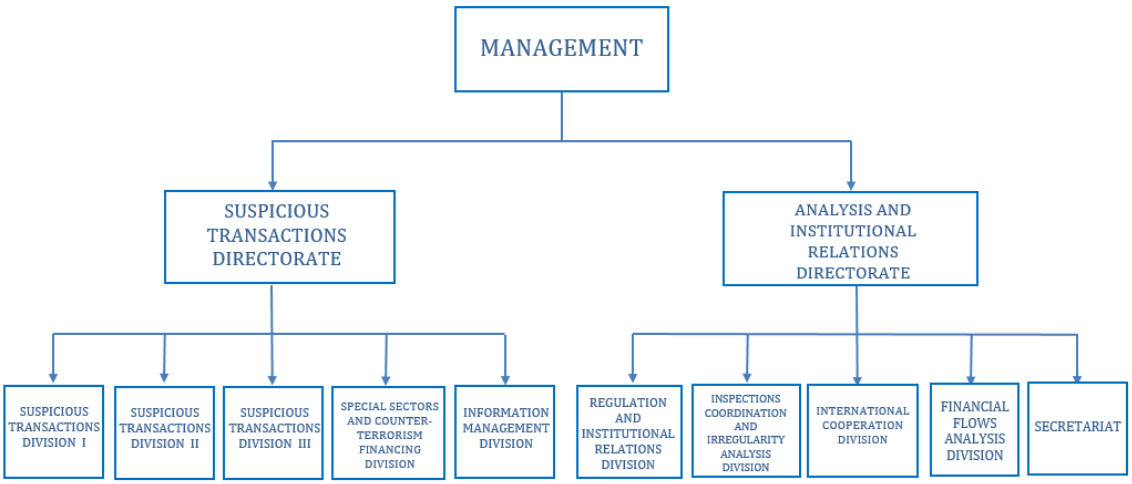
Apart from the creation of the position of Deputy for each Directorate, the main changes were the formation, within the Suspicious Transactions Directorate, of an additional Report Analysis Division and of the Special Sectors and Counter Terrorism Financing Division; and, within the Analysis and Institutional Relations Directorate, of the Inspections Coordination and Irregularity Analysis Division (Figure 10.1).[78]

The reorganization also involved the creation in 2020 of an IT Project and Technological Innovation Sector within the Information Management Division.

[77] See UIF, *Annual Report for 2019*, pp. 125-126.

[78] For the specific powers and duties assigned to the divisions of the two Directorates, see the UIF Organization Chart (only in Italian).

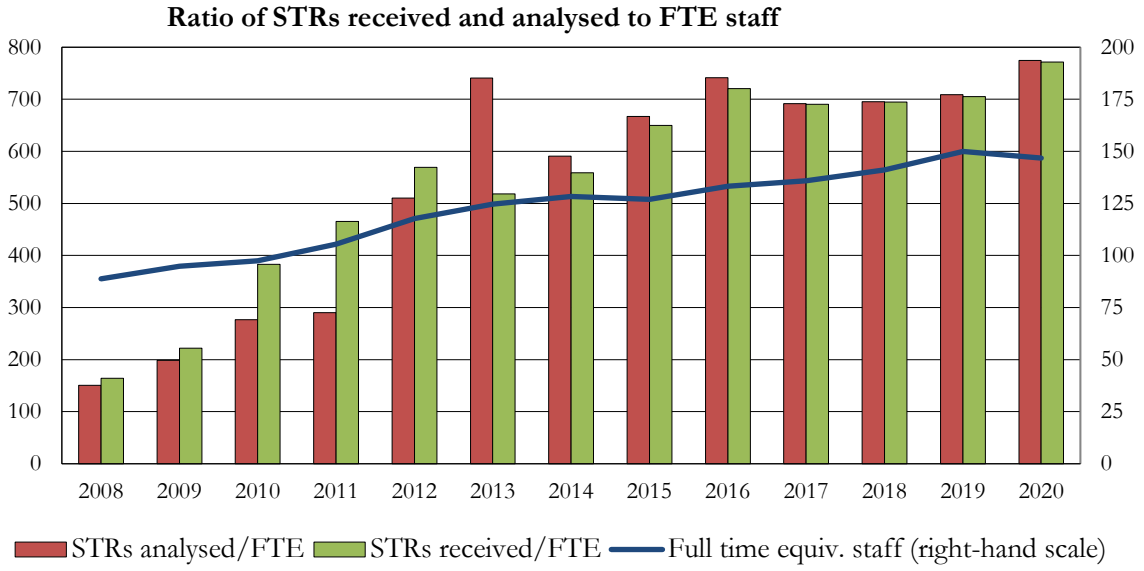
Figure 10.1



10.2. Performance indicators and Strategic Plan

In 2020, the Unit analysed 775 STRs per full-time equivalent employee (FTE), with a significant further improvement of 9.3 per cent in this indicator compared with 2019 (Figure 10.2). While staff remained broadly unchanged (see Section 10.3, 'Human resources'), the total number of days worked by UIF employees increased by 6.1 per cent. The backlog of cases was reduced again, and at the end of the year the number of reports still being processed was down to 3,329, or 35.3 per cent of the average monthly flow.

Figure 10.2



Definition of strategic guidelines

The UIF draws up its strategic action plan every three years. The 2017-19 Strategic Plan was concluded with full success, attaining all the objectives set.[79] The Plan for 2020-22 (Figure 10.3) lays out specific objectives that take account of the context of emerging risks in connection with the spread of new technologies and innovative payment instruments and the evolution of the European AML-CFT regulatory framework (see Chapter 9, 'The legislative framework'). The health and economic crisis triggered by the COVID-19 epidemic heightened the system's exposure to major risks of crime and the possible exploitation for illegal purposes of economic relief measures for households and firms.

To face these threats, it is essential for the Unit to make the processing of STRs still more efficient. A fundamental step towards attaining this objective is the adoption of a system of information exchange with the reporting entities for further analysis of the reports that guarantees both speed and maximum data confidentiality. In addition to making a start on renovating the RADAR infrastructure, greater use needs to be made of advanced information analysis techniques (machine learning, text and data mining, knowledge graphs), while the defences against cybercrime must be reinforced, among other things using tools for searching the dark web and exploring virtual asset blockchains. The new database of threshold-based communications on the use of cash will be exploited not only to analyse STRs but also to identify unreported suspicious operations and for strategic analysis.

The new Plan maintains the objective of stepped-up cooperation with the investigative bodies and the DNA, already intensified and enhanced in the course of 2020 in response to the COVID-19 pandemic (see Section 7.1, 'Cooperation with the judicial authorities'). In early 2021, a new memorandum of understanding with the DNA was signed for more efficient information sharing (see Section 10.4, 'IT resources'). Exchanges with foreign FIUs must also be increased, closer relations with public prosecutors must be forged, and cooperation with the Customs Agency must be developed to apply the new European rules on declarations on cross-border transports of cash pursuant to Regulation (EU)/1672/2018.[80]

Turning to relations with reporting entities, the Unit will proceed with its strategy of heightening their awareness and involvement in active cooperation – especially with sectors that are innovative or less mature in terms of incorporation of AML values – and feedback will be amplified. Since March 2020 the Unit has been working to heighten the obliged entities' awareness of the risks connected with the health emergency, such as improper use of public funds, fraud and corruption (mainly in the healthcare sector, private and public), and the financial support offered by organized crime to the worst-hit firms.

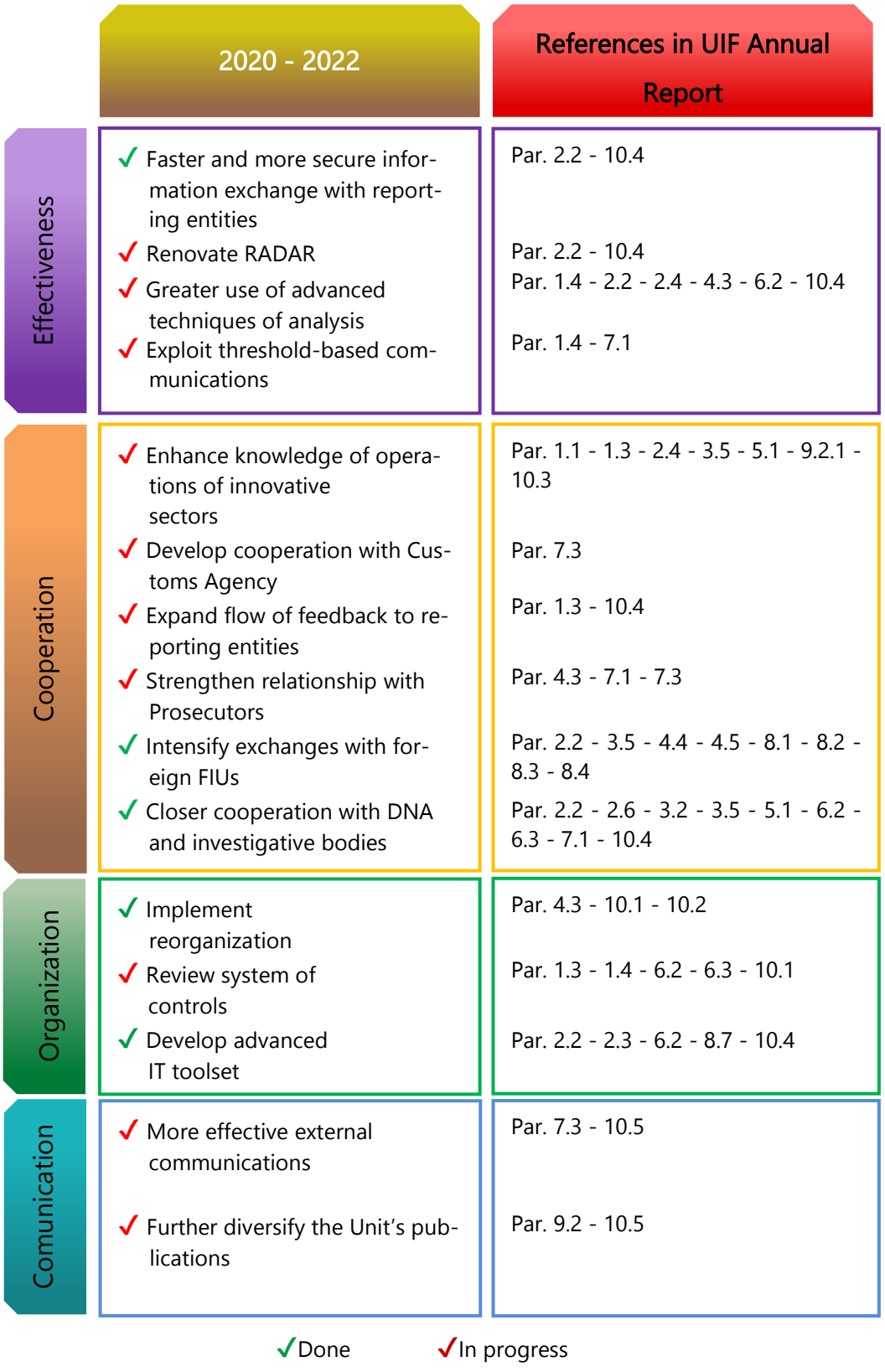
The reorganization adapted operational structures to the new tasks assigned to the UIF in recent years (threshold-based communications, cooperation with the DNA, cross-border STRs, transactions in virtual assets). In the next few years, further interventions may be planned to fully exploit the potential of the new divisions, possibly with the development of thematic poles of competence. Other lines of action will consist in adapting the system of controls to the new organizational structure and promoting innovation to build a more advanced set of IT tools for the analysis of STRs.

[79] See UIF *Annual Report for 2019*, p. 126.

[80] See UIF *Annual Report for 2018,* p. 104.

Figure 10.3

Strategic objectives and the results achieved



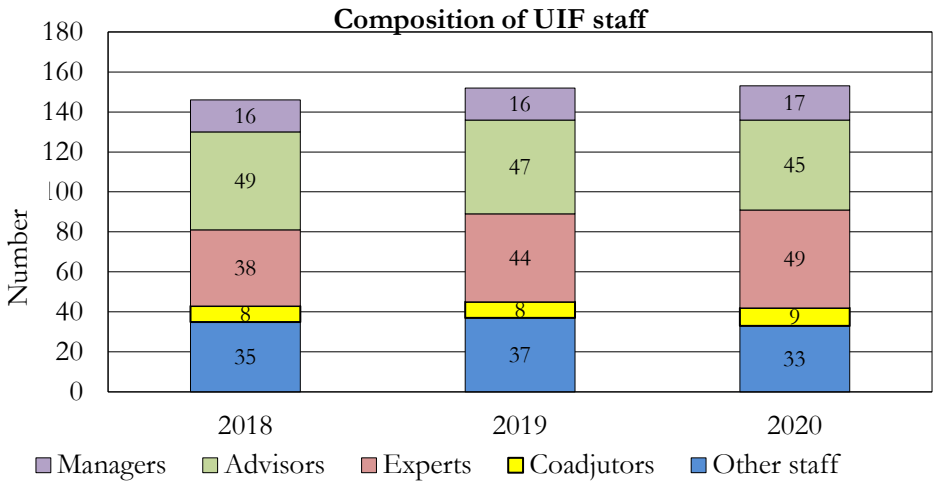
Lastly, the Strategic Plan calls for reinforcing the system of external communications, making the most of moments of contact not only with reporting entities but also with other institutions, the academic world and the press. A contribution in this regard can come from greater diversification of the issues treated and the readership for the Unit's publications (*Quaderni di analisi, Quaderni statistici, Raccolte di Casistiche, Newsletter),* also bearing in mind the interests of non-specialists.

10.3. Human resources

In 2020, the UIF's staff increased by one, from 152 to 153, with the exit of nine employees and the entry of 10, six new hires and four transfers from other Bank of Italy departments (Figure 10.4). The comparative youth of the new hires (average age, 32) resulted in a further lowering of the staff's average age to 44 at the end of the year. At 31 December, 90 staff members were assigned to the Suspicious Transactions Directorate (88 a year earlier) and 59 to the Analysis and Institutional Relations Directorate (60 a year earlier).

The negligible increase in staff in 2020 will have to be compensated for over the next two years to overcome the shortfall with respect to the 172 employees envisaged in the three-year plan for 2020-2022. The first five months of 2021 saw the entry of 12 new employees and the exit of three.

Figure 10.4



Starting in the second week of March, in response to the health emergency the UIF went over to generalized recourse to remote working, which had been tested previously in a very small number of cases and was possible thanks to the IT resources and technical assistance of the Bank of Italy. The portion of the Unit's personnel working on a remote basis was 92 per cent in the three months from March through May and stabilized at around 85 per cent for the rest of the year. The UIF continued to carry out its institutional tasks without a break and with no repercussions on productivity, which indeed improved significantly (see Section 10.2, 'Performance indicators and Strategic Plan').

The Unit continues to dedicate special attention to the capacities and professional growth of the staff. The health emergency, which necessitated strict limitation or, in some periods, the outright elimination of in-person activity, affected the Unit's investment in staff training only in its form, not its intensity. Thanks to the technology available, internal seminars were conducted on a remote basis (ten in 2020), with the involvement of the entire staff,

and participation was sustained in numerous other initiatives of the Bank of Italy and outside entities (some of them international). During the year, 70 UIF staff members took part in 39 training courses organized by the Bank, directed mainly to enabling employees to learn more about issues of institutional interest.

Attendance at training events organized by external entities (45 courses attended by 67 UIF staffers), instead, was oriented to strengthening expertise in matters of specific interest to the Unit, such as virtual assets, machine learning and deep learning techniques for data analysis, and cybercrime, also with reference to frauds perpetrated in spheres closely connected with the COVID-19 pandemic.

10.4. IT resources

In 2020, nearly ten years after the launch of its current IT architecture, the technological obsolescence of some components and the rapid evolution of the solutions available on the market prompted the Unit to set out on a course of thorough renewal of the infrastructures and applications used for the reception, analysis and dissemination of STRs. The new course initiated consists of a number of separate projects that will affect all the UIF's areas of activity.

The projects completed in 2020 were directed to improving data quality, strengthening security safegaurds and renovating some technological components. In the last quarter of 2020 and the first few months of 2021 the Unit began a series of wide-ranging projects to overhaul work processes both technologically and organizationally.

New controls on STRs

In January 2020 new controls on incoming STRs were released, to improve the quality of the data transmitted by obliged entities. Checks and monitoring of the anomalies observed were carried out, with a view to making the controls more incisive. Also, a new validation scheme was introduced, which does not necessarily block the report but offers the reporting entities suggestions on points where they can improve their information flow without impediment to reporting in the case of minor incongruities.

New STR transmission procedures for some types of reporting entity

The production release of the project 'New modalities for reports relating to payment cards, gaming and virtual assets'[81] presents new domain values for the compilation of STRs, permitting more accurate and detailed description of the transactions observed in those businesses, with their highly sector-specific operating modes.

Following a similar initiative addressed to money transfer firms in 2016, the project also took account of requests from a number of operators for functions that could reduce the reporting burden in sectors whose activities generally involve very large numbers of customers, transactions and accounts. In the first stage of the project, compilation of the STRs in 'data-entry' mode was made easier by the acquisition of a file compatible with a new, standardized data record, extended also to virtual asset operators. Thanks to cooperation with the entities involved, the data record and upload functions were further refined. The end result was to simplify the fulfilment of this requirement while at the same time obtaining more complete and detailed reports targeted to the specific field of interest.

Exchange of confidential data

On 17 February 2020 the first phase of the project 'Exchange of confidential data via the Infostat-UIF portal' was released. The new procedure significantly strengthens the security safeguards for information exchanges between the UIF and the obliged entities as

[81] See 'Comunicato UIF of 18 December 2019' (only in Italian).

regards analysis of STRs via the Infostat-UIF portal. During the year the realization of a new secure communications channel was completed, making possible the exchange of non-structured data; the successive steps will permit the exchange of structured data as well, thanks to the standardization of formats and the utilization of the data schema envisaged in the 'Financial investigations' project of the Revenue Agency, with which cooperation in this area has been initiated.

Feedback to reporting entities

In July the functionality for automatic generation and transmission of the feedback forms that the Unit sends to the largest reporters in the category 'banks and Poste Italiane' was made available. Until then, the forms had been processed using office automation products and transmitted one-by-one, customarily by certified email (see Section 1.3, 'The quality of active cooperation').

Threshold-based communications

The institution and implementation, in 2019, of threshold-based communications gave rise to problems of data quality in reporting entities' transmissions. In 2020, new types of check were developed for application in the data acquisition phase, such as to enhance the quality and accuracy of the data received. Studies were conducted on the application, in support of the Unit's analytical activity, of methodologies and indicators to detect anomalies in the use of cash even where they are not picked up by suspicious transaction reports. In addition, protocols and technical formats were devised together with the investigative bodies for exchanging the data contained in the threshold-based communications in cases where they are important for further investigation of the STRs.

Partner data-base

The project 'Managing the partner database' has the objective of designing a new IT procedure for managing the database of entities which, for various reasons, are required to transmit information to the UIF. Studies have been completed for the adoption of a more agile process for variation, verification and updating of the reporters' data, as well as better handling of other information and events relating to membership of a corporate group, such as mergers and acquisitions. In addition, a start was made on developing new electronic processes that will generate synergies and the integration of the database with the wealth of information at the Unit's disposal.

SAFE evolution

The 'SAFE evolution' project proceeded with its work towards automatic interaction between the Unit's internal SAFE system, which manages information exchanges with investigative bodies, judicial authorities and foreign FIUs, and the secure communication infrastructures used by foreign FIUs for international information exchange (Egmont Secure Web and FIU.NET). Specifically, work was begun on a plan for greater efficiency in the reception from foreign FIUs of information notes and structured data within the UIF's analysis platform, so as to reduce the manual processing of these flows with a view to full integration of FIU.NET and Egmont Secure Web with the SAFE platform.

Cross-border transmittion of STRs

At the same time, given the AML legislation, which requires the UIF to transmit to the FIUs of the other EU Member States the information on the STRs relevant to them,[82] technical measures were introduced to enable the information flows to take account of the relevant guidelines of the EU FIUs Platform,[83] thus launching the operational phase in the identification and transmission of these reports.

Information exchange with the DNA

For more effective cooperation between the UIF and the DNA under the updated memorandum of understanding between the two institutions (12 March 2021), information

[82] Art. 13-bis(4) of Legislative Decree 231/2007.

[83] Pursuant to Article 51 of Directive (EU)/2018/843.

exchange has been accelerated and the volume of data exchanged for name matching increased and also extended to some types of communications from foreign FIUs. In the second half of the year the automation of monthly data exchanges was completed and the data so received were consequently integrated into the STR handling process (see Section 2.2, 'The analysis process'). The data sharing is effected through a high-security web portal and uses exchange formats allowing for fully automatic data processing.

Technological migration

The obsolescence of parts of the IT platforms was a helpful stimulus for the complete overhaul of the applications the Unit uses. The technological migration of the components in support of the UIF's activity will proceed according to a detailed calendar for renewal of the IT infrastructures over a period of about 18 months, from the start of 2020 to June 2021. At the same time, revision has begun on the graphic interfaces of the applications, making available at the start of 2021 a new version of the portal for information exchange with the authorities, and by the end of the year will give users of the UIF website a new interface. Other innovative solutions will be integrated into a renovated IT platform in the medium term.

Evolution of RADAR

For comprehensive development of the IT components in support of the UIF's action, study has begun on the future evolution of work processes and support applications. Given the constantly changing operational framework and the continual increase in the number of reports received, the study is intended to identify new functions and technological assets that can support the process of analysis in the next few years. Within this strategic overview, several sectoral studies (described below) have focused on the main solutions for strengthening the process of financial analysis.

Improvement of name matching

Research continued towards a new system for matching entities within the Unit's database, which will help analysts in identifying recurrent parties and accounts and in reconstructing linkages between different spheres of financial operations.

New graph analysis system

At the end of 2020 study for a new system of graph analysis was begun. Combined with identity resolution, graph analysis will improve the efficiency of existing analysis processes and make possible new, more sophisticated modes of exploitation of the information in the Unit's possession.

The SARA database

The UIF's Measure on the storage and accessibility of documents, data and information for countering money laundering and terrorist financing (see Section 6.1, 'Aggregated data'), issued in August 2020, necessitated a series of actions to update and develop the IT procedures for reception, storage and treatment of SARA data.[84] The changes aligned the system with the new rules (in effect from January 2021) on transmission of reports and facilitated the introduction of additional controls on data quality.

Further, work began on developing an internal system for monitoring SARA reports to complement the one now in use, based on automatic statistical controls.[85] The new system exploits the information in the Unit's name databases together with some elaborations of the SARA data themselves in order to define, for each reporter, a structured profile of degree of compliance with the reporting requirements.[86]

---

[84] The series of interventions will presumably continue through June 2022.

[85] See *'Controlli statistici'* in the UIF website, relating to SARA reports.

[86] The system consists of 14 indicators concerning the information at the Unit's disposal as regards the internal organization of the reporting entities' AML function, the reliability of the data sent, and regularity in managing transmissions.

Lastly, in the course of the year, together with the work on the IT function, work proceeded on updating the dedicated platform for visual analysis and data mining to exploit the big data platform.[87] The new platform is now equipped with multiple integrated modules, making possible exploratory analysis of enormous masses of data and more efficient preparation of summary reports.

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 *Annual Report*, in which the UIF gives an account of its activities to the Government, to Parliament and to the general public, is presented officially every year to representatives of the institutions, financial intermediaries, operators and the professions, and is available on the UIF's website in both Italian and English. Last year, in compliance with the restrictions imposed owing to the health emergency, the presentation was conducted in remote mode.

The 'Testimony of the Director of the UIF' (only in Italian) before the parliamentary committee of inquiry into mafia and other criminal organizations, including foreign organizations, held in July 2020, focused on the initial impact of the ongoing health emergency on civil society and the economy, and on the consequent actions taken by the UIF to orient reporting entities towards cooperation in facing the related risks. In October, at his 'Testimony' (only in Italian) before a joint session of the Justice and Finance Committees dedicated to 'The European Commission's Action Plan of 7 May 2020: Evolution and prospects of the anti-money-laundering system,' the Director recalled the main policy lines set out by the Commission and highlighted the consequent implications for Italy. In January 2021, at another 'hearing' (only in Italian) held by the parliamentary committee of inquiry into mafia and other criminal organizations, the Director testified on prevention and suppression of predatory activity on the part of organized crime during the health emergency. Special attention was paid to international and national developments in countering crimes connected with the pandemic and other actions to assist AML-obliged entities in identifying the related risks.

The UIF's website reports the changes that have taken place; alongside a description of the work carried out, it gives an overview of the Italian and international AML-CFT system, with comprehensive and up-to-date information on regulatory and institutional aspects, initiatives and further research. The publication of the *UIF Newsletter* continued in 2020, offering brief updates on the Unit's activity and on anti-money laundering questions in general. The second issue of 2020 offered an overview of the data of the first eight months of threshold-based communications (April-November 2019). The third briefly set out the main areas of risk and the elements symptomatic of possible illegal operations, compiled by the UIF, other international institutions and some foreign FIUs for the identification of suspicious transactions in connect with the COVID-19 health emergency. In early 2021, two newsletters were published on the significant developments in the EU's AML framework, concerning among other things the final entry into force of Brexit and the developments in national and international measures to prevent money laundering in connection with the epidemic.

[87] See UIF *Annual Report for 2018*, pp. 75-76.

The UIF continues in its online publication of Quaderni dell'antiriciclaggio (only in Italian) on AML topics, divided into the series 'Statistics' and 'Analysis and studies'. The first series, published every six months, contains statistics on STRs, SARA data and gold declarations, plus a summary of the UIF's activities. The second gathers contributions on the subject of money laundering and the financing of terrorism; a study was published in 2020 on the development of a composite indicator for identifying 'paper mills' *(Quaderno No. 15 - only in Italian)*.

In the course of 2020, the UIF continued its work to heighten awareness and understanding among the public and various classes of obliged entities, and to work further with other authorities on the issues involved in money laundering and the financing of terrorism, by taking part in conferences, seminars and meetings. The health emergency reduced the number of these events, most sharply in the period between March and June. Subsequently, successful adaptation to the new working conditions enabled the organizers to create opportunities for meeting in remote mode.

In particular, UIF staff took part in more than 30 education and training initiatives addressed to other authorities and trade associations, at both national and international level. Prominent among these events were the courses organized by Istat, the Central Bank of the Bahamas, and the FIUs of Tunisia and the Philippines. The Unit also collaborated in training activities at the Higher Institute of Investigative Techniques of the Carabinieri and the Higher Police School. Cooperation continued with a number of universities, as well as training programmes involving associations of professionals and representatives of local authorities (municipalities, provinces 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, licenses or other permits, of any kind, vis-à-vis obliged entities, and the bodies responsible for verifying the possession of the requisites of professionalism and integrity, under the relevant sectoral rules. For the exclusive purposes set out in this Decree, the definition of administrations concerned includes: the Ministry of Economy and Finance as the authority responsible for supervising auditors and audit firms with no mandate to audit public-interest bodies or bodies under an intermediate regime, and the Ministry of Economic Development as the authority responsible for the supervision of trust companies not listed in the register under Article 106 of the TUB.

Anti-Mafia Investigation Department (Direzione Investigativa Antimafia - DIA)

A specialized interforce investigation bureau drawn from various police forces and having jurisdiction over the entire national territory. Set up within the Ministry of the Interior's Department of Public Security by Law 410/1991 this Department has the exclusive task of ensuring coordinated preventive investigations into organized crime, in all of its forms and connections, and of carrying out police enquiries into crimes of mafia-style association or crimes related thereto.

Beneficial owner

Pursuant to Article 1(2)(pp) of Legislative Decree 231/2007, the beneficial owner (or owners) is the natural person, other than the customer, who is the ultimate beneficiary on whose behalf the ongoing relationship is established, the professional service is provided or the transaction is carried out.

Central contact point

Pursuant to Article 1(2)(ii) of Legislative Decree 231/2007, this is a person or department, established in Italy, designated by the electronic money institutions, as defined in Article 2(1)(3) of Directive 2009/110/EC, and by payment service providers, as defined by Article 4(11), of Directive (EU) 2015/2366 with their registered office and head office in another Member State, and that operates without a branch office on national territory via accredited entities and agents.

Countries with strategic deficiencies in the fight against money laundering and financing of terrorism identified by the FATF

This group includes countries with weak safeguards against money laundering, as identified by the FATF in public statements that are issued three times a year. Based on these assessments (see *FATF High-Risk Jurisdictions subject to a Call for Action – February 2021* and *Jurisdictions under Increased Monitoring February 2021*), the following countries are not aligned with the legislation for combating anti-money laundering and terrorist financing: Albania, Barbados, Botswana, Burkina Faso, Cambodia, Cayman Islands, Democratic Republic of Korea, Ghana, Iran, Jamaica, Mauritius, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Senegal, Syria, Uganda, Yemen, Zimbabwe.

Cross-border report

This term refers to suspicious transaction reports received from an EU FIU that concern another Member State and which, pursuant to Article 53 (1) of the Fourth Directive, must be forwarded promptly to the relevant counterparties. These reports are identified based on a methodology developed within the EU FIUs Platform.

Designated entities

Pursuant to Article 1 (1) (l) of Legislative Decree 109/2007 designated entities means natural persons, legal persons, groups and entities designated as being subject to fund freezing based on EU regulations and national legislation.

Digital portfolio service providers

Pursuant to Article 1(2)(ff-bis) of Legislative Decree 231/2007, these are defined as natural or legal persons that provide to third parties, on a professional basis, including online, private cryptographic key safeguarding services on behalf of their own customers, for the purpose of holding, memorizing and transferring virtual currencies.

Egmont Group

An informal body set up in 1995 by a group of FIUs to further international cooperation and increase its benefits. The number of participating FIUs has grown steadily over time and it became an international organization in 2010, with its Secretariat in Toronto, Canada.

European FIU Platform

An EU body chaired by the European Commission and composed of the EU FIUs. Article 51 of the Fourth AML Directive formally recognized the role of the platform, in operation since 2006, and described its mandate in terms of developing stronger cooperation, exchanging opinions, and providing assistance in matters relating to the implementation of EU rules that apply to FIUs and reporting entities.

Financial Action Task Force (FATF)

An intergovernmental body set up within the OECD to devise and promote strategies to combat money laundering and the financing of terrorism at national and international level. In 1989, it issued 40 recommendations on monitoring money laundering, to which nine special recommendations were subsequently added on the financial fight against international terrorism. This area was fully reviewed in 2012, with the issuance of 40 new recommendations. The FATF also promotes the extension of anti-money laundering and counter-terrorism measures beyond the OECD's membership by cooperating with other international organizations and conducting inquiries into emerging trends and money laundering typologies.

Financial Intelligence Unit (FIU)

A central, national unit tasked, for the purpose of combating money laundering and the financing of terrorism, with receiving and analysing suspicious transaction reports and other information relevant to money laundering, the financing of terrorism and their predicate crimes, and disseminating the results of such analyses. Depending on the choices of national legislatures, the FIU may be an administrative authority, a specialized structure within a police force, or part of the judicial authority. In some countries, a mix of these models has been adopted.

Financial Security Committee (FSC)

Pursuant to Article 3 of Legislative Decree 109/2007, this is a committee established at the Ministry of Economy and Finance (MEF), chaired by the Director General of the Treasury, composed of 15 members and their respective delegates, appointed by MEF decree, upon designation by the Minister of the Interior, the Minister of Justice, the Minister of Foreign Affairs and International Cooperation, the Minister of Economic Development, the Bank of Italy, Consob, ISVAP (now IVASS) and the Financial Intelligence Unit. The Committee also includes an official in the service of the Ministry of Economy and Finance, an officer from the Guardia di Finanza (Finance Police), a manager or police officer of an equivalent rank under Article 16 of Law 121/1981, in the service of the Anti-Mafia Investigation Department, an officer of the Carabinieri, a manager of the 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 proliferation programmes

Under Article 1(1)(e) of Legislative Decree 109/2007, the financing of weapons of mass destruction proliferation programmes means the provision or collection of funds and economic resources, by any means, directly or indirectly instrumental in supporting or promoting all activities linked to the creation or carrying out of programmes to develop nuclear, chemical or biological weapons.

FIU.NET

A decentralized communication infrastructure for the Financial Intelligence Units of the European Union, permitting a structured, multilateral exchange of information, with standardized applications and immediate and secure information exchanges.

Freezing of funds

Pursuant to Article 1(1)(b) of Legislative Decree 109/2007, and in accordance with EU regulations and national legislation, this is a prohibition of the movement, transfer, modification, use or management of or access to funds, in such a way as to modify their volume, amount, collocation, ownership, possession, nature, purpose or any other change allowing for the use of the funds, including portfolio management.

General government entities

Pursuant to Article 1(2)(hh) of Legislative Decree 2007 these are general government entities under Article 1(2) of Legislative Decree 165/2001 and subsequent amendments, national public bodies, and companies owned by general government entities and their subsidiaries, pursuant to Article 2359 of the Italian Civil Code, limited to their activities of public interest governed by national law or by the European Union, as well as subjects responsible for tax collection at national or local level, regardless of the legal form.

High-risk third countries

Pursuant to Article 1(2)(bb) of Legislative Decree 231/2007, these are non-EU countries with strategic deficiencies in their national AML/CFT systems, as identified by the European Commission through its delegated Regulation (EU) 2016/1675 and subsequent amendments, in the exercise of its powers under Articles 9 and 64 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 as amended by Directive (EU) 2018/843.

Means of payment

Pursuant to Article 1(2)(s) of Legislative Decree 231/2007, means of payment are cash, bank and postal cheques, bankers' drafts and the like, postal money orders, credit transfers and payment orders, credit cards and other payment cards, transferable insurance policies, pawn tickets and every other instrument available making it possible to transfer, move or acquire, including by electronic means, funds, valuables or financial balances.

Money laundering

Article 648-bis of the Penal Code makes punishable for the crime of money laundering anyone who, aside from cases of complicity in the predicate crime, 'substitutes or transfers money, assets or other benefits deriving from a crime other than negligence, or who carries out other transactions in relation to them in such a way as to hamper the detection of their criminal provenance.' Article 648-ter makes punishable for illegal investment anyone who, aside from the cases of complicity in the predicate crime and the cases specified in Article 648

and 648-bis, 'invests in economic or financial assets moneys, goods or other assets deriving from crime.' Pursuant to Article 2(4) of Legislative Decree 231/2007, the following actions, if performed intentionally, constitute money laundering: (a) the conversion or transfer of property, carried out knowing that it constitutes the proceeds of criminal activity or of participation therein with the aim of hiding or dissimulating the illicit origin of the property or of helping any individual involved in such activity to avoid the legal consequences of his or her actions; (b) hiding or dissimulating the real nature, origin, location, arrangement, transfer or ownership of property or rights thereto, carried out in the knowledge that they constitute the proceeds of criminal activity or of participation therein; (c) the acquisition, detention or use of property, knowing at the time of receiving it that it constitutes the proceeds of criminal activity or of participation therein; and (d) participation in one of the actions referred to in the preceding subparagraphs, association with others to perform such actions, attempts to perform them, the act of helping, instigating or advising someone to perform them or the fact of facilitating their performance.

Moneyval (Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism)

Moneyval is a subcommittee of the European Committee on Crime Problems (CDPC) of the Council of Europe, established in September 1997. It serves as the Council's unit on money laundering, also taking account of FATF measures and making specific recommendations to the Member States. It evaluates the anti-money laundering measures adopted by Council of Europe member countries that are not FATF members. As a regional group, it has the status of Associate Member of the FATF. Under a thoroughly revised statute, Moneyval has served since January 2011 as an independent monitoring body of the Council of Europe in the fight against money laundering and the financing of terrorism; it reports directly to the Committee of Ministers, to which it submits an annual report.

National Anti-Corruption Authority (Autorità Nazionale Anticorruzione - ANAC)

Under Article 19 of Decree Law 90/2014, converted with amendments into Law 114/2014, this authority took over the functions and resources of the former authority for the supervision of public works, service and supply contracts (AVCP). The Authority is responsible for preventing corruption within general government, in state-owned, controlled and participated companies, also by implementing transparency in all management aspects, as well as through supervision activities for public contracts, appointments in any sector of public administration that could potentially be subject to corruption, while avoiding the aggravation of proceedings with negative consequences for citizens and businesses, by guiding the behaviour and activities of public employees, with interventions in advisory and regulatory settings, as well as through fact-finding activities.

National Anti-Mafia Directorate (Direzione Nazionale Antimafia - DNA)

The DNA, established as part of the General Prosecutor's Office at the Court of Cassation by Legislative Decree 367/1991, converted with amendments into Law 8/1992, has the task of coordinating the investigation of organized crime at national level. The jurisdiction of the DNA was extended to cover terrorism proceedings, including international ones, with Legislative Decree 7/2015, converted with amendments into Law 43/2015. Pursuant to Article 103 of Legislative Decree 159/2011, the DNA is managed by one magistrate with the functions of a national Public Prosecutor and two magistrates with functions of deputy prosecutors, together with magistrates that can substitute them, chosen from among those who have performed, also not continuously, the functions of a public prosecutor for at least ten years and that have specific aptitudes, organizational skills and experience in handling proceedings involving organized and terrorism-related crime.

Non-cooperative countries for tax purposes identified by the European Union

The following are on the EU list of non-cooperative jurisdictions for tax purposes: American Samoa, Fiji, Guam, Palau, Panama, Samoa, Seychelles, Trinidad and Tobago, US Virgin Islands, Vanuatu (*Council Conclusions 2021/C66/10, 26 February 2021).*

Office of Foreign Assets Control (OFAC)

This is an Office of the US Treasury Department, set up under the auspices of the State Secretary for the Treasury for terrorism and financial intelligence. The OFAC administers and enforces economic and trade sanctions, based on US foreign and security policy, against foreign nations, organizations and individuals.

Organization of Agents and Mediators (OAM)

Pursuant to Article 1(1)(q) of Legislative Decree 231/2007, this Organization is responsible for managing the lists of financial agents and loan brokers, pursuant to Article 128-undecies of the TUB (Consolidated Law on Banking). The OAM also holds: i) the currency exchange register, which has a special section for providers of virtual currency services (Article 17-bis, paragraph 8-bis, Legislative Decree 141/2010, added by Legislative Decree 90/2017 and amended by Article 5(1)(a) of Legislative Decree 125/2019; ii) the register of entities and agents under Article 45 of Legislative Decree 231/2007; and iii) the register of cash-for-gold traders under Article 1(1)(q) of Legislative Decree 92/2017.

Politically exposed persons

Pursuant to Article 1(2)(dd) of Legislative Decree 231/2007, these are natural persons that currently hold, or held important public offices up until less than one year ago, together with their immediate family members or persons known to be their close associates, and are listed as follows: 1) natural persons that hold or have held important public offices and are or have been: 1.1 President of the Italian Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, Regional President, Mayor of a provincial capital or metropolitan city, Mayor of a town with a population of at least 15,000, and similar positions in foreign countries; 1.2 a Member, Senator, Member of the European Parliament, regional councillor and similar posts in foreign states; 1.3 a member of the central governing bodies of political parties; 1.4 a Constitutional Court judge, a magistrate of the Court of Cassation or the Court of Auditors, a State Councillor or other component of the Administrative Justice Council for the region of Sicily, and similar positions in foreign countries; 1.5 a member of the decision-making bodies of central banks and independent authorities; 1.6 an ambassador, chargé d'affaires or equivalent positions in foreign states, high-ranking officers in the armed forces or similar ranks in foreign countries; 1.7 a member of the administrative, management or supervisory bodies of enterprises owned, also indirectly, by the Italian State or by a foreign State or owned, mainly or totally, by the regions, provincial capitals and metropolitan cities and by towns with a total population of not less than 15,000 inhabitants; 1.8 a general manager of an ASL (Local Health Authority) or a hospital or university hospital or other national health service entities; and 1.9 a director, deputy director, member of a management board or a person with an equivalent role in international organizations; 2) family members of PEPs include: the parents, the spouse or any person considered by national law as equivalent to the spouse, the children and their spouses or partners considered by national law as equivalent to the spouse; 3) persons who are known to be close associates of politically exposed persons include: 3.1 natural persons linked to PEPs because they have joint beneficial ownership of legal entities or other close business relationships; and 3.2 natural persons that only formally hold total control of an entity known to have been set up for the de facto benefit of a PEP.

Sectoral supervisory authorities

Pursuant to Article 1(2)(c) of Legislative Decree 231/2007, the Bank of Italy, Consob and IVASS are the authorities responsible for supervising and checking banking and financial intermediaries, auditors and audit firms with mandates to audit public-interest entities and entities under an intermediate regime. The Bank of Italy supervises and checks non-financial operators with cash-in-transit and valuable items transport companies that employ private security guards, and that have a licence under Article 134 of the TULPS (Consolidated Law on Public Security), limited to the handling of euro banknotes, and included on the list under Article 8 of Decree Law 350/2001, converted with amendments into Law 409/2001.

Self-laundering

Pursuant to Article 648-ter.1 of the Penal Code, 'whoever, having committed or attempted to commit a crime with criminal intent, uses, replaces or transfers money, assets or other utilities deriving from the commission of such a crime to economic, financial, entrepreneurial or speculative activities, in such a way as to actively hinder detection of their criminal origin' shall be punished for the crime of self-laundering. This rule was introduced by Article 3(3) of Law 186/2014.

Self-regulatory body

Pursuant to Article 1(2)(aa) of Legislative Decree 231/2007, this is a body that represents a professional category, including its various branches and the disciplinary boards on which the current legislation confers regulatory powers, supervisory powers, including checking compliance with the rules governing the exercise of the

profession and the powers to impose, via the mechanisms in place for this purpose, the sanctions applicable for the violation of such rules.

Special Foreign Exchange Unit (Nucleo Speciale di Polizia Valutaria - NSPV)

Established within the Finance Police (Guardia di Finanza), this unit combats money laundering, both as an investigative police body and as the administrative body responsible, together with the Bank of Italy and the Anti-Mafia Investigation Department, for controls on the financial intermediation sector.

Standardized archives

The files that make available the data and information envisaged in the provisions issued by the competent sectoral supervisory authorities pursuant to Article 34(3) of Legislative Decree 231/2007, in accordance with the technical standards and the analytical details referred to therein. They include the Single Electronic Archives (AUIs) already set up on the date of the entry into force of Legislative Decree 90/2017.

Tax havens and/or non-cooperative countries and territories

The blacklist of jurisdictions included in the decree of the Minister of Finance of 4 May 1999 (most recently amended by the ministerial decree of 12 February 2014) is as follows: Andorra, Anguilla, Antigua and Barbuda, Aruba, the Bahamas, Bahrein, Barbados, Belize, Bermuda, Bonaire, the British Virgin Islands, Brunei, the Cayman Islands, the Cook Islands, Costa Rica, Curaçao, Djibouti, Dominica, Ecuador, French Polynesia, Gibraltar, Grenada, Guernsey (including Alderney and Sark), Hong Kong, the Isle of Man, Jersey, Lebanon, Liberia, Liechtenstein, Macao, the Maldives, Malaysia, the Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Niue, Oman, Panama, the Philippines, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, the Seychelles, Singapore, Sint Eustatius and Saba, Sint Maarten (the Dutch part only), Switzerland, Taiwan, Tonga, the Turks and Caicos Islands, Tuvalu, the United Arab Emirates(Abu Dhabi, Ajman, Dubai, Fuijayrah, Ras El Khaimah, Sharjah and Umm Al Qaiwain), Uruguay and Vanuatu.

Trade-based money laundering

The term refers to the process of concealing the proceeds of crime and of transferring value through commercial transactions to seek to legitimize the illicit origin of such transactions.

Virtual asset service providers

Pursuant to Article 1(2)(ff) of Legislative Decree 231/2007, they are natural or legal persons that, as a business, provide third parties with services which are functional to the use, exchange and safekeeping of virtual currencies and their conversion from or into legal tender currencies or digital representations of value, including those convertible into other virtual currencies, as well as issuance, offering, transfer and clearing services and every other service functional to acquisition, trading or intermediation in the exchange of such currencies.

Virtual currency

Pursuant to Article 1(2)(qq) of Legislative Decree 231/2007, a virtual currency is a digital representation of value, not issued by a central bank or a public authority, not necessarily linked to a currency that is legal tender, and used as a medium of exchange for purchasing goods and services or for investment purposes, and transferred, stored and traded electronically.

ACRONYMS AND ABBREVIATIONS

ADM	Customs and Monopolies Agency (Agenzia delle Dogane e dei Monopoli)
ANAC	National Anti-Corruption Authority (Autorità Nazionale Anticorruzione)
ANCI	National Association of Italian Municipalities (Associazione Nazionale Comuni Italiani)
ATM	Automated Teller Machine
AUI	Single Electronic Archive (Archivio 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)
CRD-V	Capital Requirements Directive 5
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)
EBA	European Banking Authority
ECB	European Central Bank
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EDPS	European Data Protection Supervisor
EMI	Electronic Money Institution
ESA	European Supervisory Authority
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FSC	Financial Security Committee
FIU	Financial Intelligence Unit
G20	Group of 20
IAD	Independent ATM Deployer
ISIL	Islamic State of Iraq and the Levant

Istat	National Institute of Statistics (Istituto Nazionale di Statistica)
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
PSD2	Revised Payment Services Directive
RADAR	Collection and Analysis of AML Data (Raccolta e Analisi Dati AntiRiciclaggio)
SARA	Aggregate AML Reports (Segnalazioni AntiRiciclaggio Aggregate)
SACE	Italian Export Credit Agency
SGR	Asset management company
SICAF	Fixed capital investment company
SICAV	Variable capital 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
VASP	Virtual Asset Service Provider
VAT	Value Added Tax
VD	Voluntary Disclosure