



BANCA D'ITALIA  
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

# Annual Report 2022 Italy's Financial Intelligence Unit

Rome, May 2023

year 2022

number

15





BANCA D'ITALIA  
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

# Annual Report 2022 Italy's Financial Intelligence Unit

Rome, May 2023

*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, 2023**

**Unità di Informazione Finanziaria per l'Italia**

**Director**

Enzo Serata

**Address**

Largo Bastia, 35 00181 Rome -Italy

**Telephone**

+39 0647921

**Website**

<http://uif.bancaditalia.it>

ISSN 2385-1384 (print)

ISSN 2284-0613 (online)

Copyright

Reproduction allowed for educational or non-commercial purposes, on condition that the source is acknowledged.

## Index

<b>FOREWORD.....</b>	<b>5</b>
<b>1. ACTIVE COOPERATION .....</b>	<b>9</b>
1.1. Reporting flows .....	11
1.2. Suspicious transactions.....	15
1.3. The quality of active cooperation .....	19
<b>2. OPERATIONAL ANALYSIS.....</b>	<b>23</b>
2.1. The data.....	23
2.2. The analysis process .....	23
2.3. Risk assessment .....	25
2.4. Methodology.....	26
2.5. Suspension orders .....	28
2.6. Information flows of investigative interest and exchanges with the DNA.....	29
<b>3. RISK AREAS AND TYPOLOGIES .....</b>	<b>31</b>
3.1. Context factors .....	31
3.2. Tax evasion .....	32
3.3. Misappropriation of public funds and corruption .....	33
3.4. Organized crime.....	35
3.5. Further case studies .....	37
<b>4. COMBATING THE FINANCING OF TERRORISM.....</b>	<b>45</b>
4.1. Suspicious transaction reports .....	45
4.2. Typologies of transactions suspected of financing terrorism.....	48
4.3. The UIF's analyses.....	49
4.4. International activities .....	50
<b>5. THRESHOLD-BASED COMMUNICATIONS, SARA REPORTS, GOLD DECLARATIONS AND STRATEGIC ANALYSIS .....</b>	<b>53</b>
5.1. Threshold-based communications .....	53
5.2. SARA reports .....	59
5.3. Gold declarations .....	67
5.4. Strategic analysis.....	71
<b>6. CONTROLS .....</b>	<b>77</b>
6.1. Inspections and document audits.....	77
6.2. Sanction procedures .....	80
<b>7. COOPERATION WITH OTHER AUTHORITIES.....</b>	<b>83</b>
7.1. Cooperation with the judicial authorities .....	83
7.2. Cooperation with the MEF and the FSC .....	85
7.3. Cooperation with supervisory authorities and other institutions.....	87
<b>8. INTERNATIONAL COOPERATION.....</b>	<b>91</b>
8.1. Exchange of information with foreign FIUs .....	91
8.2. The state of cooperation between FIUs and the main findings of information exchange.....	94
8.3. The EU FIUs Platform.....	95
8.4. Developments in the FIU.NET .....	96
8.5. Relations with foreign counterparts and technical assistance.....	97

8.6. Participation in the FATF.....	97
8.7. Participation in other international organizations .....	100
8.8 Activities relating to the war in Ukraine .....	102
<b>9. THE LEGISLATIVE FRAMEWORK.....</b>	<b>105</b>
9.1. The global and European context .....	105
9.1.1. European regulatory developments.....	105
9.1.2. Further European and international initiatives .....	115
9.2. The Italian legislative and regulatory framework .....	117
9.2.1. Legislation.....	117
9.2.2. Regulatory and other measures .....	119
<b>10. RESOURCES AND ORGANIZATION .....</b>	<b>125</b>
10.1. Organization .....	125
10.3. Human resources .....	128
10.4. IT resources .....	129
10.5. External communication.....	131
<b>GLOSSARY.....</b>	<b>133</b>
<b>ACRONYMS AND ABBREVIATIONS.....</b>	<b>139</b>

---

#### List of boxes

Active cooperation of general government in the context of the NRRP	15
Communication to reporting entities of the outcome of low-risk STRs	20
Analysis of the STRs relating to the NRRP	33
Analysis of the STRs relating to the Culture Bonus	34
Studies on threshold-based communications	58
Indicators of compliance with the SARA reporting obligations	61
FAQs about gold	69
An indicator of opacity of Italian firms	72
Anomalous triangulations with Russia: an analysis on SARA and ORO data	74
Virtual IBANs: AML issues	79
A comparative analysis of failure to submit STRs	81
Memorandum of understanding with the DNA	84
Developments in cross-border reporting	92
The role of FIUs in asset recovery	98
International and Italian initiatives on crypto-assets	107
Establishment and host city of the AMLA: implementation and the impact on the UIF	109
AML aspects of the digital euro	116
The new anomaly indicators	119
The register of beneficial owners in the light of DM 55/2022 and the Court of Justice Judgment of 22 November 2022	120

---

## FOREWORD

The period covered by this Report proved to be another challenging year in the UIF's work of preventing and combating money laundering and economic and financial crime. The year registered a new all-time high in the number of suspicious transaction reports received (155,426, with growth of 11.4 per cent). As usual, the great majority of these STRs came from the banking and financial system, but there was also an increased contribution from gaming service providers and non-financial operators. The number of reports from general government entities remained negligible, even though the current period of massive public intervention in the economy heightens the necessity of safeguards for legality.

The increased reporting flow requires constant improvement and continuing innovation in processes and methodologies to produce prompt and accurate analyses despite the mounting operational pressures. The initiatives undertaken enabled the Unit to keep the number of STRs forwarded to the investigative bodies broadly in line with the number received, with only a modest increase in the backlog.

An innovative methodology for the selection and classification of reports marked by particular grounds for suspicion was introduced in 2022. The new method allows uniform assessments and treatment, which assists prompt transmission to institutional counterparties. Another step in this direction was the development of a procedure for assessment of the risk involved in situations characterized by pronounced fragmentation of transactions and large numbers of both transactions and persons – about a third of all STRs. These new approaches helped in the detection of implicit connections and more highly articulated situations, which were then subjected to network analysis, with a view to augmenting the value added for subsequent investigations. The outcomes of investigations and the feedback from the National Anti-Mafia Directorate (DNA) corroborate the efficacy of the Unit's analyses.

The upward trend in the flow of reports has not always been accompanied by improvement in their information content. In its constant commitment to enhance the quality of active cooperation, the Unit stepped up dialogue with the reporting entities and introduced new forms for sharing more detailed information on the outcomes of the STRs. Further studies and initiatives are planned to avoid a deterioration in the informational value added of the reports.

In 2023 the UIF released a complete revision of the indicators of anomaly. This brings together in a single, systematic regulatory act the typology of relevant cases, making it easier for all the obliged entities to evaluate the profiles of suspicion of money laundering or terrorist financing.

The long wave of the COVID-19 pandemic continued to produce operational cases connected with the aftershocks to the economy and the effects of the public policies of economic support. And, albeit to a lesser extent, the Russo-Ukraine crisis also impacted on the reporting flow, owing especially to the subjective, operational consequences of the EU and international sanctions against Russia.

The exploitation of the information on cash transactions acquired via threshold-based communications was intensified and extended both to cooperation with the investigative bodies and with the DNA and to the design and application of methodologies for the identification of the operating points of banking and financial intermediaries whose activities in cash exhibit significant anomalies. In this area, the UIF's strategy centres on closer partnership with the reporting entities for enhanced awareness of the risks of laundering in connection with the use of cash.

Strategic analysis concentrated on the study of indicators of opacity of Italian firms, the identification of firms at risk of infiltration by organized crime as signaled by financial statement indicators, and closer examination of cross-border flows to detect anomalous triangulations with Russia. The Aggregate Anti-Money Laundering Reports (SARA) and the gold declarations (ORO) were exploited still more intensely and systematically to develop analyses and context studies, devise indicators of risk in support of the supervisory authorities, and intercept emerging phenomena. The monitoring of SARA reporting entities was reinforced with the introduction of a new system for evaluating the degree of compliance with requirements. For the ORO declarations, which increased sharply by comparison with 2021, information to assist in their compilation was published.

The Unit's inspection and control activity continued at the same level as in 2021, directed to various types of entity, from pledge lenders to banks active in FinTech or factoring, from intermediaries involved in the securitization of impaired credits to virtual asset service providers.

After two years of considerable growth, the number of requests for information from the judiciary and law enforcement bodies returned to pre-pandemic levels, falling nearly 40 per cent. The new memorandum of understanding with the DNA seeks to improve the mechanism for data sharing and to strengthen other forms of cooperation.

Since the onset of the Russian military attack against Ukraine, the UIF has provided support to the Financial Security Committee, both by bringing the obliged entities up to date on the restrictive measures and by checking the availability at Italian intermediaries of funds traceable to the persons listed. On instructions from the Committee, the Unit also collected data on the deposits of Russian and Belarusian nationals and information on the presence of goods and assets subjected to freezes.

Information exchanges with foreign FIUs diminished modestly but continued to be important for financial analysis of STRs and for domestic cooperation. At European level, cross-border STRs received continued to increase at a rapid pace, with growth of over 200 per cent compared with 2021. However, the quality of this reporting flow suffers from the disparate approaches of different FIUs; a good part of it focuses on mere anomalies and is accordingly of scant use to analysis.

This shortcoming highlights the importance of coordination and of the tendency to more uniform contributions of the European FIUs, which will be powerfully stimulated by the AML Package now under discussion by the EU institutions and expected to be approved by the end of the year. Specifically, the creation of the AML Authority will result in better coordinated and more effective AML action within the Union.

The UIF is committed to active participation in the new supranational institutional framework and to laying the groundwork for the requisite coordination with the nascent Authority. At the operational level as well, the Unit has continued to make a major contribution to the working groups formed by the EU FIUs' Platform to standardize the formats and contents of cross-border STRs and thus enhance their usability, preparing the way for the future action of the AMLA within the framework of the Coordination Mechanism for FIUs.

The reorganization of the Unit, begun at the start of 2023, makes the most of the commitment, on every front, to the battle against money laundering and terrorist financing. The full implementation of the new structure and the related investments in human and IT resources constitute a necessary condition for carrying out the three-year plan for 2023-25, which focuses on increasing the efficacy of financial analysis, strengthening relations with the reporting entities to ensure high-quality reporting flows, closer cooperation with

institutional interlocutors, better external communications, and active participation in European institutional evolution.

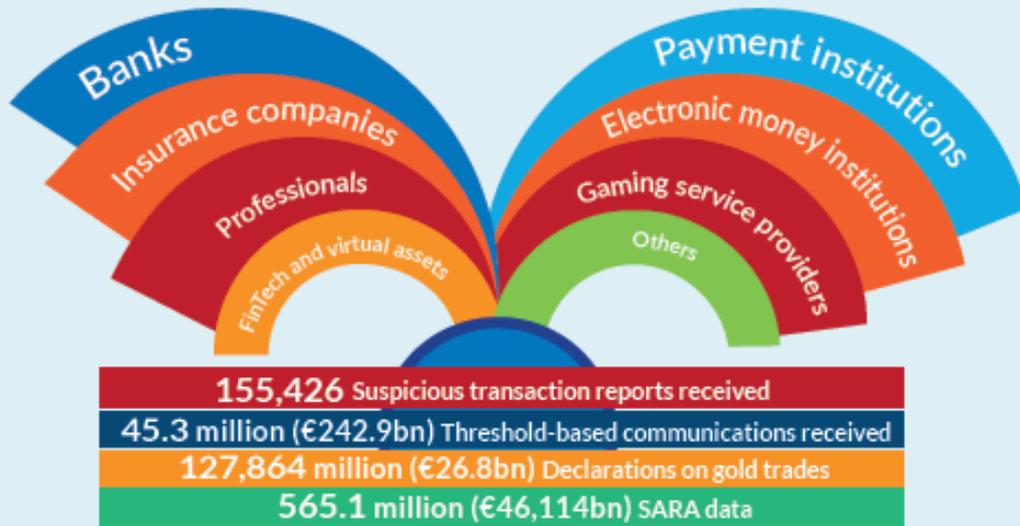
These goals are challenging but ineluctable in the changing landscape of risks, operating conditions, and the institutional and regulatory framework.

**The Director**

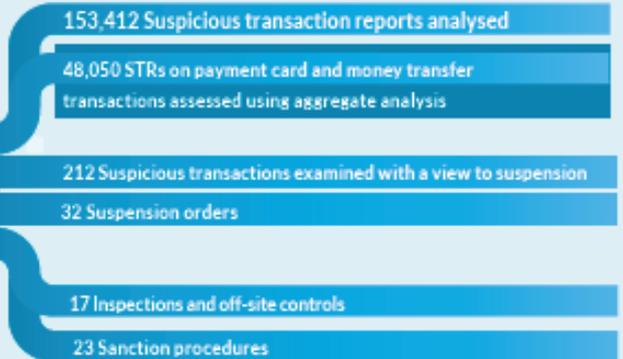
*Enzo Serata*

# ACTIVITY AT A GLANCE

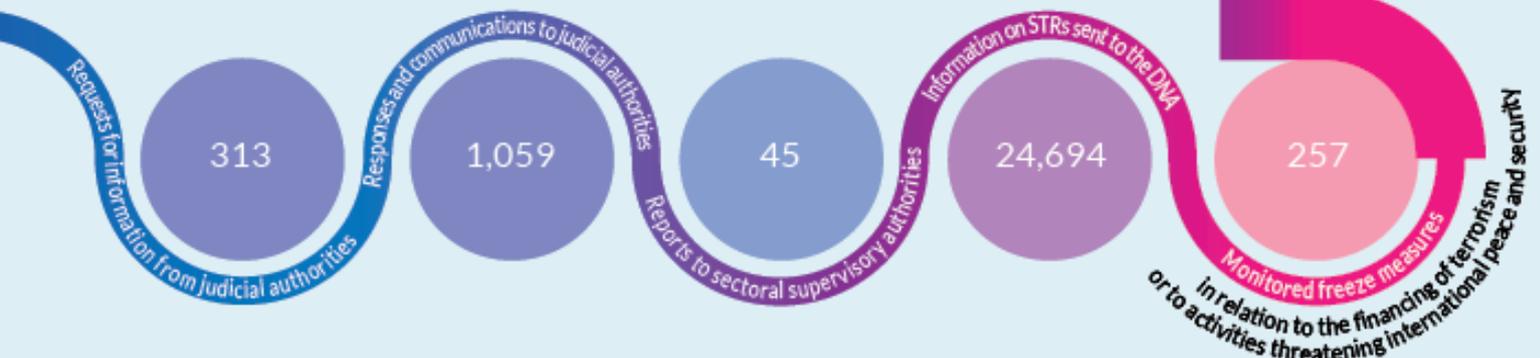
## Financial analysis



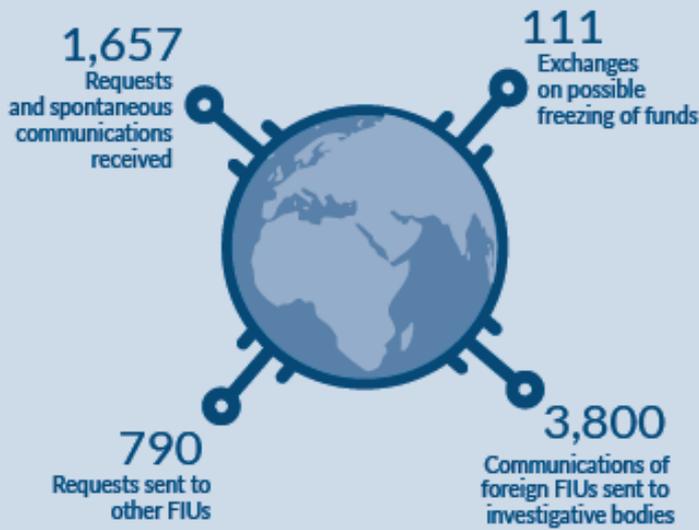
## Intelligence, dissemination and controls



## Cooperation with national investigative bodies and authorities



## FOREIGN FIUs



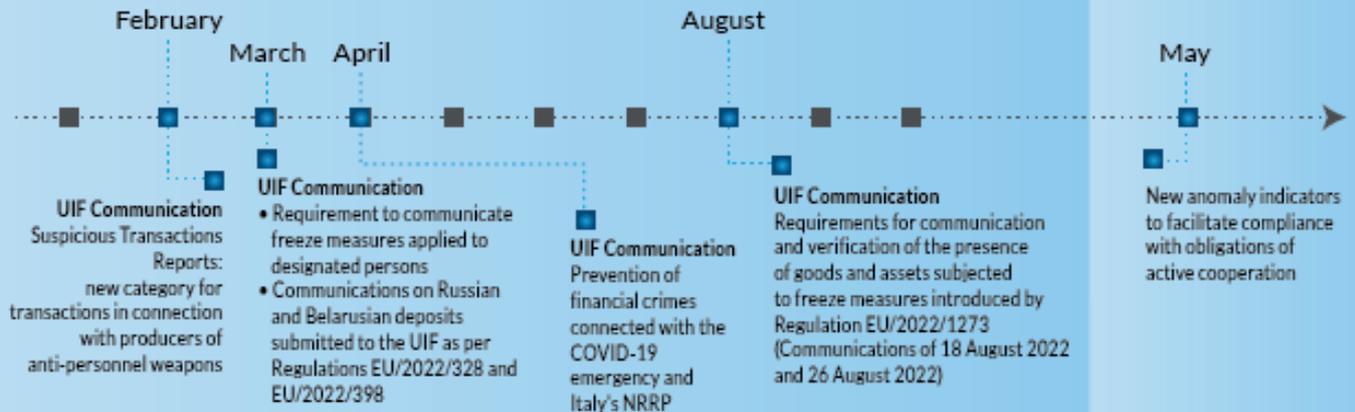
## DISSEMINATION

of knowledge about money laundering



## Secondary legislation and UIF communications

2022



## IT Infrastructure

Indicators for classifying and processing STRs

New tools for graph analysis

Automation tools for first level analysis

Innovation in the identity resolution system

New register of reporting entities



## 1. ACTIVE COOPERATION

The Unit is institutionally assigned to receive reports on transactions suspected of involving money laundering or the financing of terrorism and proliferation of weapons of mass destruction, which financial intermediaries, professionals and other qualified operators are required to identify, assess and report in a timely manner under the obligation of active cooperation.

Centralization of such reports at the UIF allows the Unit to conduct uniform and integrated evaluations of them capable of capturing subjective and objective links and networking dynamics, tracing financial flows even beyond Italy's borders with the contribution of information exchanged with foreign FIUs, and identifying innovative money laundering techniques and high-risk activities.

The UIF forwards the reports and its analyses to the Special Foreign Exchange Unit of the Finance Police (NSPV) and the Anti-Mafia Investigation Department (DIA) for investigative follow-up. It also sends reports and analyses to the judicial authorities in the event that information regarding crimes is found or upon their request. The results of analyses may be sent to the supervisory authorities if significant profiles are identified. The UIF sends data and information to the National Anti-Mafia Directorate (DNA) in order to check for the possible bearing of suspicious transaction reports on criminal contexts and enable prompt consequent action.

The body of information acquired by the Unit is also used to develop anomaly indicators and anomalous behaviour patterns for dissemination to reporting entities in order to guide and improve their ability to identify suspicious transactions.

### 1.1. Reporting flows

In 2022, the Unit received 155,426 suspicious transaction reports (STRs), 15,902 more than in the previous year (Table 1.1).<sup>1</sup> The growth rate, still high at 11.4 per cent after the exceptional jump of 23.3 per cent in 2021, was sustained by a significant increase in the number of reports sent in the second half of the year.

Table 1.1

	Reports received				
	2018	2019	2020	2021	2022
Number of reports	98,030	105,789	113,187	139,524	155,426
<i>Percentage change on previous year</i>	<i>4.5</i>	<i>7.9</i>	<i>7.0</i>	<i>23.3</i>	<i>11.4</i>

The increase for the year came chiefly from the growth of 11,948 in the number of reports transmitted by banks and Poste Italiane SpA (+15.5 per cent), whose share of the

<sup>1</sup> Detailed information on suspicious transaction reports can be found in [Quaderni dell'antiriciclaggio - Dati statistici](#), published on the UIF's website.

annual aggregate rose from 55.2 to 57.3 per cent, and from the contribution of electronic money institutions and the related EU contact points, STRs from which increased by 3,021, or 15.4 per cent. The number of reports transmitted by general government entities<sup>2</sup> remained limited, with two public sector companies accounting for 170 of the annual total of 179 (an increase of 51, or 39.8 per cent), mostly relating to requests for public financing drawing on resources of the National Recovery and Resilience Plan (NRRP). By contrast, the contributions of regional and local authorities (six reports) and of chambers of commerce (a single report) were marginal.

Table 1.2

<b>STRs by type of reporting entity</b>					
	<b>2021</b>		<b>2022</b>		<i>(% change on 2021)</i>
	<i>(number of reports)</i>	<i>(% share)</i>	<i>(number of reports)</i>	<i>(% share)</i>	
<b>Total</b>	<b>139,524</b>	<b>100.0</b>	<b>155,426</b>	<b>100.0</b>	<b>11.4</b>
<b>Banks and Poste Italiane SpA</b>	<b>77,086</b>	<b>55.2</b>	<b>89,034</b>	<b>57.3</b>	<b>15.5</b>
<b>Non-bank fin. intermediaries</b>	<b>46,618</b>	<b>33.4</b>	<b>46,888</b>	<b>30.2</b>	<b>0.6</b>
Electronic money institutions and points of contact of EU electronic money institutions	19,611	14.1	22,632	14.6	15.4
Payment institutions and points of contact of EU payment institutions	20,788	14.9	17,418	11.2	-16.2
Insurance companies	3,976	2.8	4,184	2.7	5.2
Financial intermediaries - Article 106 of the Consolidated Law on Banking	1,133	0.8	1,248	0.8	10.2
Asset management companies, SICAVs and SICAFs	405	0.3	383	0.2	-5.4
Trust companies - Article 106 of the Consolidated Law on Banking	255	0.2	230	0.1	-9.8
Investment firms	46	0.0	61	0.0	32.6
Intermediaries and other financial operators not specified above (1)	404	0.3	732	0.5	81.2
<b>Companies managing markets and financial instruments</b>	<b>10</b>	<b>0.0</b>	<b>6</b>	<b>0.0</b>	<b>-40.0</b>
<b>Professionals</b>	<b>5,121</b>	<b>3.7</b>	<b>5,667</b>	<b>3.6</b>	<b>10.7</b>
<b>Non-financial operators</b>	<b>2,902</b>	<b>2.1</b>	<b>4,386</b>	<b>2.8</b>	<b>51.1</b>
<b>Gaming service providers</b>	<b>7,659</b>	<b>5.5</b>	<b>9,266</b>	<b>6.0</b>	<b>21.0</b>
<b>General government entities</b>	<b>128</b>	<b>0.1</b>	<b>179</b>	<b>0.1</b>	<b>39.8</b>

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

<sup>2</sup> Since 4 July 2017 general government entities no longer figure among obliged reporting entities in that they are not included in Article 3 of Legislative Decree 231/2007 as amended by Legislative Decree 90/2017. The new rules, set out in Article 10(4), state: *For the purpose of enabling financial analyses aimed at bringing out phenomena of money laundering and terrorist financing, general government entities shall communicate to the UIF data and information concerning the suspicious transactions of which they become aware in the course of their institutional activity.*

Non-bank financial intermediaries again stood second among the categories of obliged entities by number of reports, with 46,888, or 30.2 per cent of the total. The number of STRs they sent rose by just 0.6 per cent, compared with 74.4 per cent in 2021, following a redistribution of the reporting flow within the category. In particular, the increase from 19,611 to 22,632 in STRs from electronic money institutions (EMIs) and the points of contact of EU EMIs, concentrated on three operators, was accompanied by a decline of 16.2 per cent in those filed by Italian payment institutions and the contact points of EU payment institutions, which fell from 20,788 to 17,418.

**Non-bank  
financial  
intermediaries**

The number of STRs from insurance companies grew again, rising by 5.2 per cent from 3,976 to 4,184, while those transmitted by asset management companies, SICAVs and SICAFs turned downwards by 5.4 per cent, from 405 to 383. STRs from trust companies under Article 106 of the Consolidated Law on Banking fell for the sixth consecutive year, though at decreasing rates, with the total for the year down by 9.8 per cent to 230. After slipping by 2.9 per cent in 2021, STRs from financial intermediaries under Article 106 of the Consolidated Law on Banking increased by 10.2 per cent, from 1,133 to 1,248.

To be noted, finally, is the growth in STRs from other intermediaries and financial operators not included in the above-mentioned categories (up by 81.2 per cent, from 404 to 732). It came largely from EU companies active in the insurance sector in Italy under the freedom to provide services, without a branch or point of contact, upon meeting the requirements set out in IVASS Measure 111/2021.

The annual flow of STRs from professionals showed a further increase (10.7 per cent, from 5,121 to 5,667), thanks to those from notaries (up by 13.1 per cent, from 4,688 to 5,304), which again accounted for the great majority of the sector's total (93.6 per cent; Table 1.3).

**Professionals**

Table 1.3

STRs received from professionals and non-financial operators					
	2021		2022		
	<i>(number of reports)</i>	<i>(% share)</i>	<i>(number of reports)</i>	<i>(% share)</i>	<i>(% change on 2021)</i>
<b>Non-financial obliged entities</b>	<b>15,682</b>	<b>100.0</b>	<b>19,319</b>	<b>100.0</b>	<b>23.2</b>
<b>Professionals</b>	<b>5,121</b>	<b>32.7</b>	<b>5,667</b>	<b>29.3</b>	<b>10.7</b>
Notaries and Nat'l Council of Notaries	4,688	29.9	5,304	27.5	13.1
Accountants, bookkeepers and employment consultants	242	1.5	166	0.9	-31.4
Auditing firms and auditors	77	0.5	80	0.4	3.9
Law firms, law and accounting firms and law practices	41	0.3	44	0.2	7.3
Lawyers	33	0.2	23	0.1	-30.3
Other professional service providers (1)	40	0.3	50	0.3	25.0
<b>Non-financial operators</b>	<b>2,902</b>	<b>18.5</b>	<b>4,386</b>	<b>22.7</b>	<b>51.1</b>
Cash/valuables-in-transit companies	1,630	10.4	2,204	11.4	35.2
Gold traders and manufacturers and traders of precious stones and metals	737	4.7	1,187	6.1	61.1
Virtual asset service providers (2)	326	2.1	826	4.3	153.4
Other non-financial operators (3)	209	1.3	169	0.9	-19.1
<b>Gaming service providers</b>	<b>7,659</b>	<b>48.8</b>	<b>9,266</b>	<b>48.0</b>	<b>21.0</b>

(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.

The number of reports submitted by accountants and lawyers fell by respectively 31.4 and 30.3 per cent, while those from the other professional categories, including auditing firms, law firms, law and accounting firms and law practices, showed increases. As in the previous years, practically all the STRs from notaries (98.4 per cent) were channelled through the National Council of Notaries, while the share of reports transmitted through the National Council of the Order of Accountants and Bookkeepers fell from 70.2 per cent in 2021 to 41.6 per cent owing to a suspension, ongoing at the start of 2023, of the STR forwarding service.

The growth in STRs submitted by non-financial operators (up by 51.1 per cent, from 2,902 to 4,386) reflected the positive contribution of all the main categories of the sector, notably cash/valuables in transit companies (+35.2 per cent, from 1,630 to 2,204), professional operators in gold and gold buyers<sup>3</sup> (+61.1 per cent, from 737 to 1,187) and virtual asset service providers (+153.4 per cent, from 326 to 826). The figure for the last-mentioned category, which is concentrated on three leading operators, possibly showed the positive impact of the obligatory registration of virtual asset service providers active in Italy in the registry, operative since 14 May 2022, kept by the Organization of Agents and Mediators.

STRs in the  
first four months of  
2023

The flow of STRs from gaming service providers grew again in 2022, rising by 21.0 per cent, from 7,659 to 9,266. In general, the uptrend for the sector could be linked to the rebound of activity due to the easing of the restrictive measures put in place during the health emergency.

In the first four months of 2023 the Unit received a total of 51,956 suspicious transaction reports, 8.2 per cent more than in the corresponding period of 2022. The number of STRs it forwarded to investigative bodies rose by 10.8 per cent.

New reporting  
entities

The growth in reports in 2022 went together with an increase in the number of reporting entities, thanks to 497 new registrations with the Infostat-UIF portal (compared with 353 in 2021). In line with the pattern of the last three years, most of the new registrations concerned professionals (270), including 168 accountants (33.8 per cent of all new registrations).<sup>4</sup> The increase in virtual asset service providers (19), all of them exchangers, benefited from the above-mentioned start-up of the census of virtual asset providers active in Italy. Of the new reporting entities, 27.4 per cent (28.3 per cent in 2021) transmitted at least one report, for a total of 848 STRs, up sharply from 373 the previous year. The bulk of these came from virtual asset service providers and from insurance companies operating in Italy under the freedom to provide services (276 and 317 STRs, respectively).

Twenty of the new registrations regard entities having their registered office in other European countries, including one non-EU country: six virtual asset service providers, eight financial intermediaries operating under the freedom to provide services, three online gaming service providers, one professional, one asset management company and one securities investment firm. As in recent years, the Italian region with the most newly registered entities was Lombardy (161), followed by Veneto and Emilia-Romagna (47 each) and Lazio (40).<sup>5</sup>

<sup>3</sup> In Table 1.3 the two types constitute 'Gold traders and manufacturers and traders of precious stones and metals'.

<sup>4</sup> The surge in new registrations is likely ascribable to the suspension of forwarding services by the National Council, since the total number of STRs from accountants diminished in spite of the increase in their registrations.

<sup>5</sup> For EU payment institutions and electronic money institutions, the office in Italy of the related point of contact was considered.

Active cooperation on the part of the 44 new reporting entities belonging to the public sector (chiefly municipalities) was negligible (4 STRs), especially considering the size of the related perimeter and the need to safeguard the public resources needed for the country's economic recovery.

AML legislation assigns a specific role to general government entities, calling upon them to identify, map and safeguard the areas of activity most exposed to the risk of money laundering and terrorist financing, and to report to the UIF any suspicious transactions of which they become aware in the course of their activity. As a whole, the administrative apparatus still does not seem to have grasped the scope of these duties, given that the number of STRs coming from general government entities continues to be very low, especially in relation to the scale of the illegal activities they can potentially intercept (sometimes linked to episodes of corruption) and the attractiveness of certain sectors of public activity, such as tenders and the various forms of public financing, for criminals.

### **Active cooperation of general government in the context of the NRRP**

The National Recovery and Resilience Plan offers extraordinary opportunities for relaunching Italy's economy. The Plan's diffuse governance makes it incumbent on the entire public sector not only to show a capacity for project design and a readiness to act, by streamlining and speeding up administrative procedures, but to activate in synergic fashion all the preventive safeguards and measures to strengthen integrity functional to the correct and legitimate allocation of the funds.

The legislative authority, conscious of the special role that the AML safeguards can play in the context of the NRRP, took this occasion to extend to the general government sector the application of one of the fundamental pillars of AML legislation, namely the task of performing due diligence on beneficial owners. Nevertheless, although there are no doubts as to the active role demanded of general government in the prevention of money laundering, the data collected by the UIF are not encouraging and indicate the need for the public sector to act swiftly to strengthen the preventive safeguards, particularly those against money laundering.

In this context, it is also urgent that the links between the prevention of corruption and the reporting of suspicious transactions, recalled by the National Anti-Corruption Authority in the National Anti-Corruption Plan for 2022-24, be turned fully to account. Coordination among the agents of prevention and of the protection of the integrity of general government entities is in fact one of the key factors to ensure integrated management of the risks of criminal infiltration of public activity.

The UIF, in collaboration with the National School of Administration, the National Anti-Corruption Authority and the Department of Public Administration, is working to raise the public sector's awareness of the need for an integrated approach to prevention and to the protection of legality. At the centre of the initiatives are training regarding the risks and the elements warranting communication of suspicious transactions and the creation of special 'communities of practice' for discussion among the administrations, exchange of experiences, and the identification and dissemination of best practices.

## **1.2. Suspicious transactions**

As in the preceding years, nearly all of the suspicious transaction reports received in 2022 – 99.8 per cent of the total – concerned money laundering, while a limited number,

41.0 per cent fewer than in 2021, bore on terrorist financing (see Chapter 4, ‘Combating the financing of terrorism’). The number of STRs on instances of suspected financing of the proliferation of weapons of mass destruction remained residual (8 in 2021, 16 in 2022).<sup>6</sup>

The regional distribution of STRs showed no significant changes: Lombardy again accounted for the largest share (17.8 per cent), followed by Lazio (12.4 per cent) and Campania (11,8 per cent; Table 1.4).<sup>7</sup> In relation to the resident population, instead, the largest contribution in terms of active cooperation came from Lazio, followed by Campania and Lombardy.

Table 1.4

<b>Distribution of STRs received by region of transaction</b>					
	<b>2021</b>		<b>2022</b>		<i>(% change on 2021)</i>
	<i>(number of reports)</i>	<i>(% share)</i>	<i>(number of reports)</i>	<i>(% share)</i>	
Lombardy	25,447	18.2	27,651	17.8	8.7
Lazio	17,236	12.4	19,255	12.4	11.7
Campania	15,728	11.3	18,305	11.8	16.4
Veneto	10,253	7.3	11,437	7.4	11.5
Emilia-Romagna	9,570	6.9	9,477	6.1	-1.0
Piedmont	8,295	5.9	9,001	5.8	8.5
Tuscany	8,206	5.9	8,971	5.8	9.3
Sicily	9,283	6.7	8,936	5.7	-3.7
Puglia	7,702	5.5	8,115	5.2	5.4
Calabria	3,826	2.7	4,125	2.7	7.8
Liguria	3,198	2.3	3,621	2.3	13.2
Marche	2,897	2.1	3,097	2.0	6.9
Trentino-Alto Adige	2,378	1.7	2,691	1.7	13.2
Friuli Venezia Giulia	2,264	1.6	2,426	1.6	7.2
Abruzzo	1,990	1.4	2,334	1.5	17.3
Sardinia	1,880	1.3	2,239	1.4	19.1
Umbria	1,283	0.9	1,354	0.9	5.5
Basilicata	867	0.6	900	0.6	3.8
Molise	559	0.4	603	0.4	7.9
Valle d’Aosta	245	0.2	327	0.2	33.5
Abroad	1,412	1.0	3,056	2.0	116.4
Online	5,005	3.6	7,505	4.8	50.0
<b>Total</b>	<b>139,524</b>	<b>100.0</b>	<b>155,426</b>	<b>100.0</b>	<b>11.4</b>

In general, increases were recorded for the STRs referring to transactions carried out in all the regions except Emilia-Romagna and Sicily (down by 1.0 and 3.7 per cent, respectively). Among the top regions by number of STRs received, those with the largest increments were Campania (+16.4 per cent), Lazio (+11.7 per cent) and Veneto (+11.5 per cent). Though at lower levels, noteworthy increases were also recorded in Valle d’Aosta (+33.5 per cent), Sardinia (+19.1 per cent) and Abruzzo (+17.3 per cent). Milan, Prato, Rome and Naples were

<sup>6</sup> From February 2022 onwards the category also includes STRs on transactions connected with the activity of firms producing anti-personnel mines and cluster munitions and submunitions; see UIF Communication of 3 February 2022 ([only in Italian](#)).

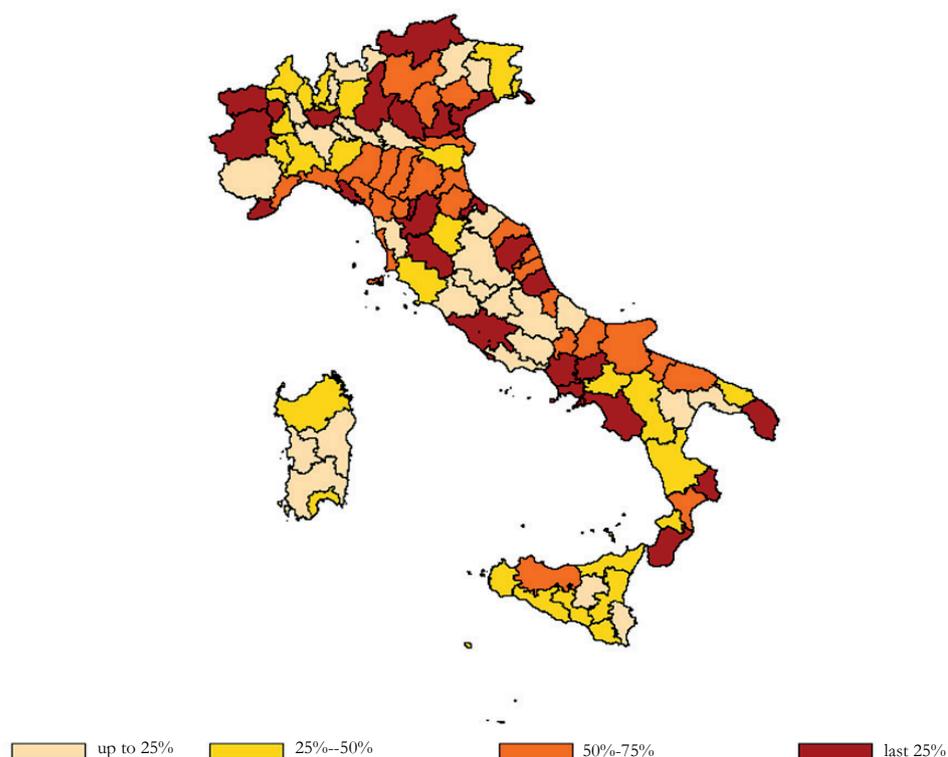
<sup>7</sup> By convention, reports are assigned to the region of the first suspicious transaction reported in the STR.

again the leading provinces of transaction for STRs in relation to the population (Figure 1.1), with flows of between 378 and 469 STRs each per 100,000 inhabitants, while fewer than 100 STRs referred to the province of Sud Sardegna.

The year under review also saw a 50 per cent jump in STRs not indicating a physical place of execution because the transactions were carried out ‘online’, further evidence that that operating practice is by now well-established. The main categories of reporting entities submitting STRs on online transactions were electronic money institutions (44.8 per cent of the total, with 3,360 STRs) and gaming service providers (41.1 per cent, with 3,085 STRs). The number of STRs referring to cross-border operations more than doubled, rising by 116.4 per cent, from 1,412 to 3,056.

Figure 1.1

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

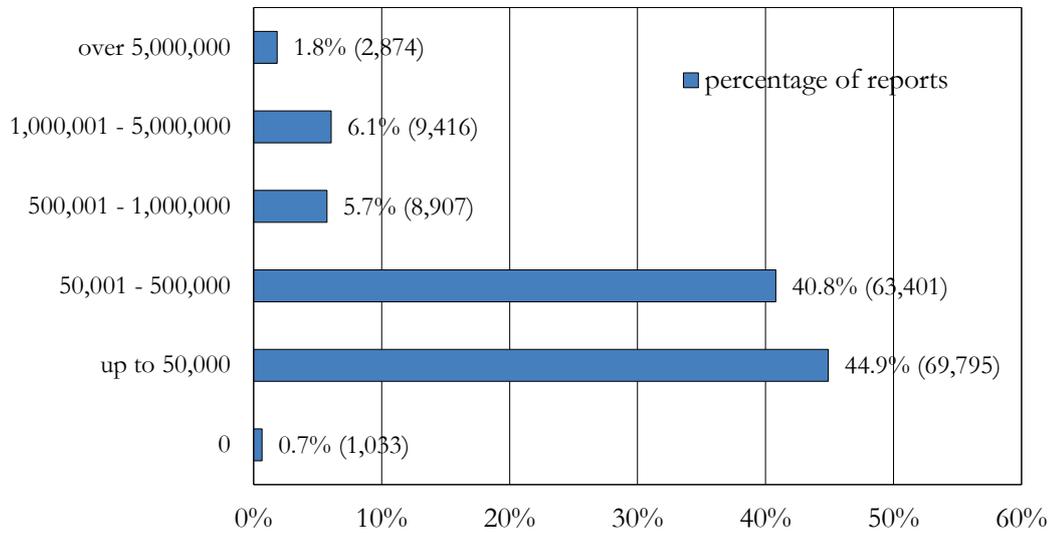


The STRs received in 2022 regarded executed transactions totalling €94.9 billion (€83.7 billion in the previous year). Adding in suspicious transactions that were attempted but not executed, whose value fell from €7.8 billion to €5.0 billion, the overall value of the flow came to €99.9 billion in 2022, up from €91.4 billion in 2021.

No significant changes occurred in the distribution of STRs by amount classes: 44.9 per cent of the STRs in 2022 (47.3 per cent in 2021) referred to transactions of €50,000 or less (Figure 1.2), followed by STRs on transactions worth between €50,001 and €500,000 (40.8 per cent of the total, up from 39.4 per cent in 2021).

Figure 1.2

**Distribution of STRs received by transaction amount**  
(in euros)

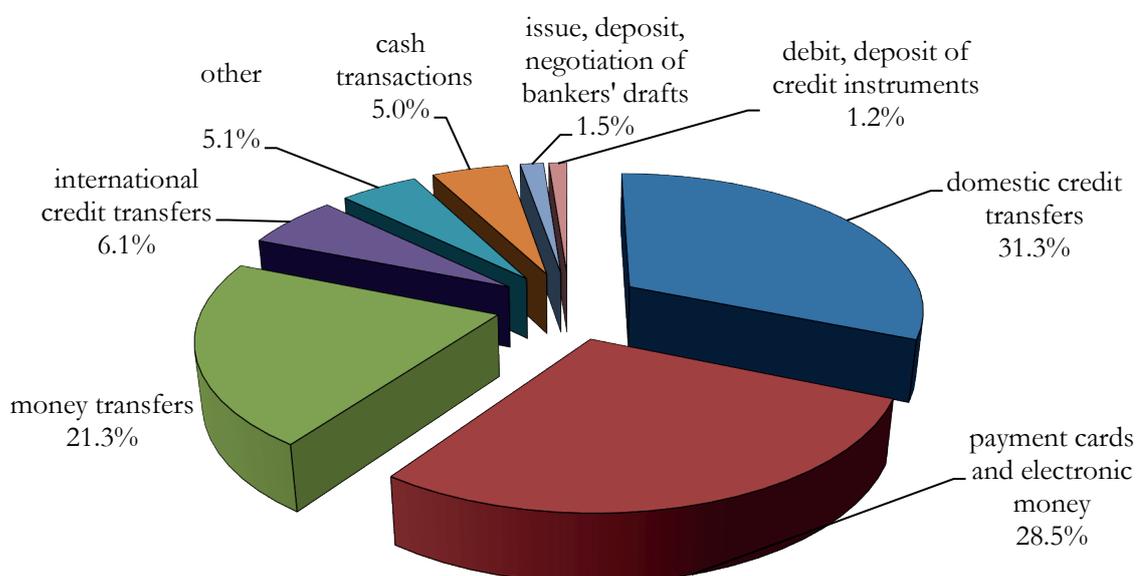


**Types of transactions reported**

The breakdown of reported transactions according to their technical form shows a sharp growth in credit transfers, whose overall share came to 37.4 per cent, with increases in both the domestic and the cross-border components (from 22.5 to 31.3 per cent and from 4.6 to 6.1 per cent, respectively). There was a further growth in transactions via payment cards and electronic money instruments (from 27.2 to 28.5 per cent), set against a decline in money transfers (from 33.4 to 21.3 per cent). The share of cash transactions was broadly unchanged, edging up from 4.8 to 5.0 per cent (Figure 1.3).

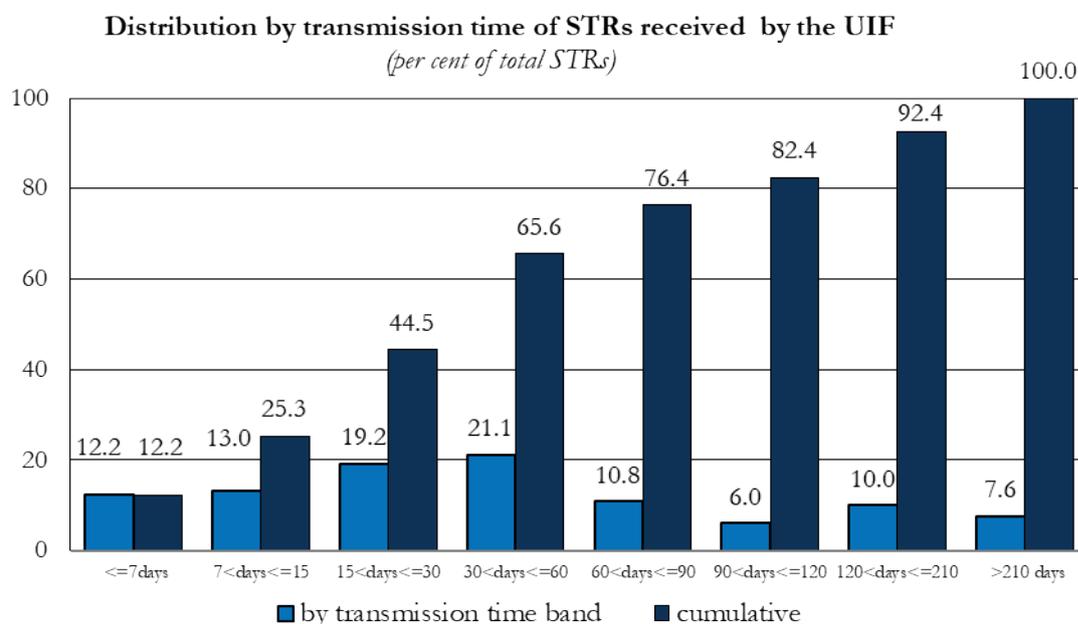
Figure 1.3

**Main technical forms of reported transactions**  
(percentage shares)



In 2022, 44.5 per cent of STRs were received within one month of the transaction, compared with 44.0 per cent in 2021, while 65.6 per cent were received within two and 76.4 per cent within three months, against 63.2 and 76.2 per cent, respectively, the previous year (Figure 1.4).

Figure 1.4



The share of reports sent to the UIF within 30 days increased for intermediaries and other financial operators (from 34.7 to 43.6 per cent) and, to a lesser extent, for professionals (from 74.0 to 76.9 per cent) and non-financial operators (from 44.0 to 47.7 per cent). By contrast, there was a slight lengthening of STR transmission times for banks and Poste Italiane SpA, with the share forwarded within 30 days contracting from 47.5 to 45.1 per cent. A sharper decline was registered for gaming service providers, whose percentage of STRs transmitted within 30 days fell from 46.1 to 22.7 per cent. A similar development was recorded for reports transmitted by general government, whose transmission times doubled in all time bands up to 90 days.

### 1.3. The quality of active cooperation

The added value of active cooperation depends above all on the ability to identify emerging phenomena and forms of money laundering and terrorist financing and to portray them in an effective, complete and timely manner. To this end, in addition to having adequate organizational safeguards and complying with the rules, reporting entities also need to adopt research tools and work processes for suspicion identification that can generate high-quality information able to open paths of analysis by the authorities charged with prevention and the investigative bodies. In recent years, however, the rapid growth in the flow of reports has gone together with a worsening in their quality: a large and increasing number of STRs are based exclusively on anomalies – generic, at times episodic – or on the mere resubmission of already reported information in the absence of additional grounds for suspicion, not indicating the subjective and objective circumstances found or even the evaluations conducted in order to single out the suspicion.

Reports with such scant justification may sometimes stem partly from the massive use of automatic detection tools whose results are not subsequently tested further for the simultaneous presence of objective and subjective grounds for suspicion and money laundering risk factors before transmission to the UIF.

Consequently, the Unit has stepped up its work to offer reporting entities useful elements for sharing an evaluation of active cooperation and thereby improving the quality of reports. In 2022 two important innovations were made in the feedback to reporting entities on STRs considered to feature a low level of money laundering risk, divided into two macro categories:

- type A STRs, for which sufficient risk elements were not found to support the suspicion of money laundering or terrorist financing;
- type B STRs, for which the UIF database contains some information supporting the suspicion but which, also taking account of the facts communicated by the reporting entity, were classified as low-risk.

Such information can help reporting entities to refine suspicious transaction selection and evaluation processes, and to check that they have not omitted significant information that might have led to a different evaluation on the part of the Unit. The transmission of these types of feedback, in fact, aims at creating a virtuous dialogue between the UIF and the reporting entities, who are invited to send a new STR upon the emergence of new or previously overlooked information. In any case, low-risk STRs are also the object of dissemination to the investigative bodies and suspicions may always be reassessed by the Unit upon the detection of connected contexts and new distinguishing features.

### **Communication to reporting entities of the outcome of low-risk STRs**

The new approach to selecting low-risk STRs implements Article 41(2) of Legislative Decree 231/2007, which requires the UIF periodically to communicate to reporting entities the outcomes of the risk evaluations conducted on the suspicious transaction reports transmitted by each of them, and is in line with the FATF guidelines for communicating the investigative outcomes of STRs to reporting entities.

The new criteria made it possible to give reporting entities feedback on a much higher number of reports and with a greater granularity of information.

The current outcome report on low-risk STRs replaces the UIF communications on reports requiring no further action, a process terminated because no longer in conformity with the law. It takes account of the practices and criteria used by the UIF for the risk-based selection of incoming reports, including the elements of evaluation furnished by the investigative bodies and by the DNA,<sup>8</sup> acquired both *ex ante* (possible investigative relevance of persons and contexts reported) and *ex post* (possible outcomes of investigations).

It must be underlined that the acquisition of these elements of information is conducted entirely online, through the portal for information exchange with the investigative bodies. The outcome reports are released when all the elements of assessment, including the investigative ones, are in the possession of the UIF; they are, therefore, communicated at the conclusion of the STR evaluation cycle, every six months.

In parallel, a revision of the summary feedback reports on the essential elements of STRs is under study. These reports measure the individual reporting entity's active

<sup>8</sup> See UIF, *Annual Report for 2021*, p. 36.

cooperation in terms of timeliness, completeness and exhaustiveness of the portrayal of reported contexts both in absolute terms for the individual reporting entity and relative to the cluster to which it belongs.

Based on data available as of mid-March 2023, in 2022 type A STRs – those lacking sufficient risk scenarios – made up about 9 per cent of the total; the share rises to more than 10 per cent for the category consisting of banks and Poste Italiane SpA and to about 12 per cent for gaming service providers. Type B STRs, distinguished by weak investigative and other grounds to support the suspicion, made up just under 20 per cent of the total, again with higher percentages for some categories, such as professionals (about 23 per cent) and gaming serving providers (more than 31 per cent).

Among the remaining STRs, one in four was considered high-risk, that is to say based on recognized high-risk money laundering and terrorist financing scenarios, with consistent findings of interest in the realm of financial and/or investigative analysis. The share of STRs of this type differs across categories of reporting entity: it is lower for non-financial operators and gaming service providers than for banks and Poste Italiane SpA.

Pending improvements to the qualitative feedback reports, the Unit looked into the time it took reporting parties to transmit the supplementary information requested by the UIF during analysis of STRs, the completeness of such information and the exhaustiveness of the replies provided. Considering that this interlocution with reporting entities serves, in general, for deeper examination of the STRs, it was found that about 55 per cent of the inquiries relating to STRs for 2022 and closed by January 2023 were concluded within 15 days while more than 14 per cent exceeded 30 days.

Monitoring of reporting entities

There are differences across categories of reporting entity. Speed of response was greater for banks and Poste Italiane SpA and for other financial intermediaries, although there were still 111 reporting entities (out of 344) for which a third of inquiries lasted beyond 30 days. The inquiries addressed to gaming service providers, general government entities and the self-regulatory bodies of professional orders were especially prolonged, with 57, 43 and 38 per cent, respectively, taking more than 30 days to be concluded.

By and large, reporting entities' response times to the UIF's supplementary requests for further examination of their own or others' STRs, are similar to the STR transmission times, so it appears that the system is responding efficaciously to the UIF's requests, albeit with ample room for improvement. In particular, there is the case of professionals, who report either in their own name or by means of the professional orders' reporting channel, and who generally are only asked for data concerning the STRs they themselves have sent, and that of non-financial operators, who must be reminded repeatedly before responding. Response times are also slow on the part of general government entities, which in many cases are involved for the analysis of contexts reported by other entities.

Ensuring reporting flows of high quality requires a constant dialogue between reporting entities and the Unit. The Unit promoted several encounters in order to clarify its own information needs.

The UIF also promoted a venue for discussion with the AML officers of some of the delegated offices of general government entities, in order to draw their attention again to the importance of the suspicious transaction report as a tool of prevention. The initiative, in which 69 AML officers representing 23 entities took part, aimed essentially at bringing out possible scope for improvement of the reporting model and proposals for modifying it to better portray the operations typical of public administrations. Although explicit contributions were not received within the agreed time period, many areas for improvement

did emerge and can be explored in bilateral meetings with some of more cooperative administrations.

**Technical  
assistance to  
reporting  
entities**

Lastly, the UIF provides reporting entities with constant technical assistance along the entire STR production chain, from registration with the system to the most critical phases of the preparation of reports (from changes to the ID data of AML officers to the solution of interpretative queries). In 2022, the Unit received more than 2,900 requests for assistance, in line with the previous year, when some problems arose due to the updating of the Infostat-UIF portal's computation infrastructure. The demand for assistance was affected by the suspension, still ongoing, of the centralized service offered by the National Council of Accountants and Bookkeepers, which diverted to the UIF an additional flow of queries on the part of professionals who found themselves having to transmit suspicious transaction reports.

With regard to the registration of reporting entities and requests for changes in the information supplied, the UIF launched an initiative to simplify compliance by obliged entities and shorten the time for validation of changes. The new functionalities are expected to be released before the end of 2023 and will be made known to the interested parties with suitable advance notice through the customary communication procedures.

## 2. OPERATIONAL ANALYSIS

The financial analysis performed by the UIF is aimed at identifying transactions and situations attributable to money laundering or terrorist financing. 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 described in the report, identify parties and relationships, and reconstruct the financial flows underlying the operations described.

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

### 2.1. The data

The UIF analysed and transmitted to the investigative bodies 153,412 suspicious transaction reports in 2022, 10.8 per cent more than in 2021 (Table 2.1).

Table 2.1

	Reports analysed				
	2018	2019	2020	2021	2022
Number of reports	98,117	106,318	113,643	138,482	153,412
<i>Percentage change on previous year</i>	<i>4.4</i>	<i>8.4</i>	<i>6.9</i>	<i>21.9</i>	<i>10.8</i>

Despite this marked increase, the number of reports analysed and transmitted to the Special Foreign Exchange Unit of the Finance Police and the Anti-Mafia Investigation Department was slightly less (98.7 per cent) than the number received.

### 2.2. The analysis process

The collection and handling of STRs are supported by RADAR, a 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 system that also encompasses the acquisition of supplementary documentation for the analysis of STRs and the investigative outcomes.

One of RADAR's basic functions is the risk-based classification of each report, to which a system rating is assigned, thus providing an initial tool for selecting flows and ranking priorities.

**Processing times**

The UIF worked to ensure that the considerable growth in STRs did not compromise the efficiency and accuracy of the analysis process. STR processing took an average of 14 days in 2022, as in the previous year, while the share of those sent to the investigative bodies within 30 days rose from 88.3 to 91.3 per cent. Of the STRs featuring higher risk, 49.7 per cent were analysed and forwarded within 7 days and 90.3 percent within 30 days of their reception.

**Automatic classification of STRs**

Operational pressures made it necessary to search for new approaches and to try out new process, technological and organizational solutions, both in order to cope with the increasing inflow of STRs and to improve the quality of analysis, by favouring the standardization of procedures and speeding up the processes for classifying and selecting the cases with the highest risk of money laundering or terrorist financing.

Accordingly, the Unit developed two parallel systems. The first (CLAUT, an acronym standing for Automatic Classification of STRs), based on the integration of rule-based algorithms, risk indicators and handling indicators derived from shared operating practices, classifies reports that lend themselves to a uniform process of assessment (first and foremost, those involving only persons under investigation or transactions mainly in cash). The second selection system (LASER, Assisted Reading of STRs for Risk Calculation) was developed with reference to the reports of the special sectors (casinos, gaming, money transfers and virtual currencies) marked by a high number of transactions and counterparties: through an information scoring system, it provides an evaluation according to the financial and investigative riskiness of the context and a classification based on many of the elements available in the RADAR system. The algorithm evaluates both the distinguishing features of the transactions reported and the elements derivable from all the matches with the Unit's dataset, employing indicators, based on scores weighted by the cumulative experience of analysis over the years, that select the most significant links and information.

Both systems have proved highly effective in selecting and classifying a growing number of reports. CLAUT has had a positive impact by ensuring better quality of in-depth analysis. For its part, LASER has made it possible to inaugurate aggregate and network methods of analysis, bringing out implicit links between contexts reported even at some distance in time and by different obliged entities.

While analysis of STRs is no doubt a delicate process entrusted to the judgement and expertise of analysts, who are ultimately responsible for the phenomenological classification of STRs, adjustments are being made to integrate the two new systems to achieve uniform classification of all STRs.

**Interventions necessitated by the NPRR**

In a near-term perspective, the approval of the NPRR and its unfolding implementation required vigilant monitoring of correct and prompt compliance with the active cooperation obligations by the targets of AML legislation in order to assist the identification of possible risk situations that could jeopardize the attainment of the Plan's objectives. In this framework, a specific taxonomy was introduced (phenomenon 'PN1 – Anomalies connected with the implementation of the NPRR') for the categorization of reports showing risk situations linked to such contexts (see the box 'The analysis of STRs referring to the NPRR' in Chapter 3). To this end, the Unit developed automatic tools that assist analysts in promptly intercepting STRs that report improper use of the resources allocated, with a view to determining the most appropriate way to handle them and to make them quickly available to the investigative bodies.

### 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 five-tier scale.

As soon as the STR arrives at the Unit, it receives an automatic rating, again on a five-tier scale, 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 the reporting entity's assessment into account, but it may diverge from the latter owing to the wider array of information used. Its accuracy depends in part on correct and complete compilation of the STR by the reporting entity.

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.

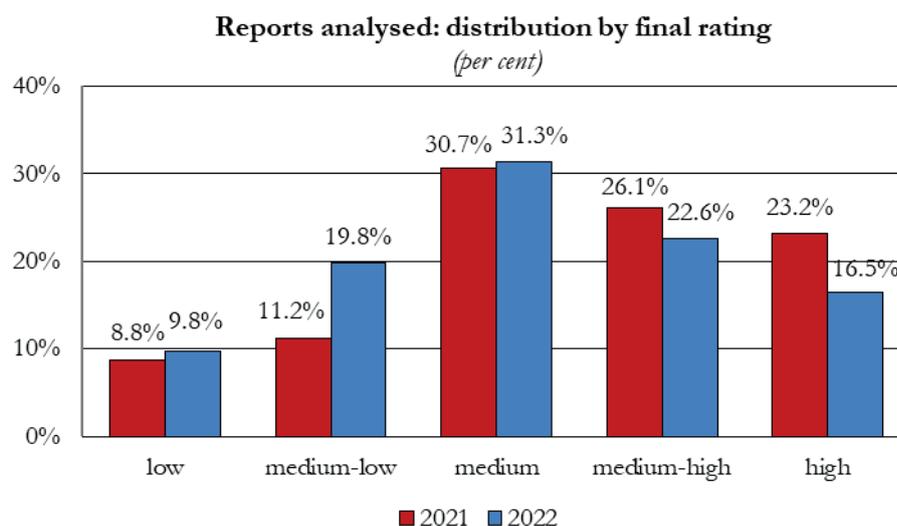
In the course of 2022, the Unit adjusted its internal rules for STR risk assessment in order to obtain a more balanced distribution among the five risk classes and facilitate the prioritization of analyses. In addition, new parameters were defined for the assessment of STRs belonging to the two low-risk classes (ratings R1 and R2) so as to take due account of the ever expanding data set supporting analysis, including information supplied by the investigative bodies and the DNA.

This revision also affected the assignment of final ratings to the reports analysed and processed, making it possible, among other things, to give the reporting entities more granular feedback on the reports they sent, starting with those of low money-laundering risk.

In the year under review, the distribution of final ratings showed a reduction in those at the higher end of the scale (Figure 2.1): 39.1 per cent of the reports were evaluated as medium-high or high risk, compared with 49.3 per cent in 2021. Those rated as medium-risk was about the same (31.3 per cent, against 30.7 per cent in 2021), while the share of reports rated as medium-low or low risk rose to 29.6 per cent (20.0 per cent in 2021).

Risk reclassifications downstream of analysis (final rating) primarily concerned STRs whose risk the reporting entities had rated low or medium-low: 32.9 per cent of such STRs were assigned a final rating of medium risk, while 19.0 per cent were reclassified as medium-high or high risk, compared with 37.3 and 33.3 per cent, respectively, in 2021. In the opposite direction, 24.9 per cent of reports initially rated as medium-high or high risk received a final rating of medium risk and 9.5 per cent one of low risk, up from 20.1 and 7.6 per cent, respectively, in the previous year.

Figure 2.1



The risk rating of STRs by reporting entities coincides to a high degree with the final ratings assigned by the UIF. In 2022, 48 per cent of STRs received a final rating in line with the score indicated by the reporting entity, compared with 39.1 per cent in 2021; of these, some 40 per cent regarded low and medium-low risk reports (Table 2.2).

Table 2.2

**Comparison for each STR between the risk indicated by the reporting entity and final rating assigned by the UIF**  
(percentage composition)

		Risk indicated by the reporting entity			Total
		Low and medium-low	Medium	Medium-high and high	
UIF rating	Low and medium-low	19.8	7.4	2.4	29.6
	Medium	13.5	11.5	6.3	31.3
	Medium-high and high	7.8	14.6	16.7	39.1
Total		41.2	33.4	25.5	100.0

## 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 data enrichment or from other sources, the grounds for suspicion of money laundering or terrorist financing and the need for further action are evaluated.

If certain conditions are met (the transaction and the grounds for suspicion are described thoroughly, the case can be traced to a known typology, it has proved impossible to proceed with further investigation, a rapid sharing of information with the investigative bodies is advisable) the STR can be accompanied by a simplified report, thus optimizing

its processing.

When further scrutiny is needed to track and reconstruct the financial path 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 reconstruction and the results of the financial checks performed. At this stage of processing, the Unit's analysts have multiple options and tools of inquiry at their disposal. The legislation governing the sector empowers the UIF to contact the reporting party or other obliged entities to acquire additional information of use for further inquiry or serving to clarify the operational perimeter of the suspicion. The Unit may also consult the data of the Revenue Agency, query the international network of FIUs, and avail itself of all the information that can be extracted from the UIF database and are integrated in the RADAR application or deriving from other sources.

The STR analysis process also envisages a third level of evaluation, on an aggregate basis, for some report typologies (at present, money transfer, payment card and gaming sector reports). This procedure collates large sets of reports characterized by a multiplicity of small-value transactions, a large number of parties involved and geographical dispersion. The LASER selector helps to bring out significant links and patterns even where the transactions, taken individually, appear insignificant.

In 2022 the Unit had increased recourse to 'third-level' analysis, with which the reports falling within a defined temporal and/or sectoral perimeter are batch processed and aggregated on the basis of differentiated criteria.

**Aggregate analysis**

A first approach envisages the construction of specific risk indicators based on the characteristics of the operations found and their subsequent aggregation in a composite indicator. This methodology was applied, for example, to the money transfer and videolottery sector. A second criterion (pattern matching) takes into consideration the reports traceable to specific phenomena in which common features and operational recurrences can be identified, with the aim of framing possible patterns of anomalous conduct for the future identification of contexts with the same characteristics. Finally, the use of network metrics based on social network analysis and the production of graphs with data visualization tools make it possible to delimit groups of reports displaying objective statistical indicators of interrelation. The process of selecting potentially significant networks follows a risk-based approach, using a methodology developed ad hoc to reconstruct clusters of connected reports, which are identified taking into account the number of persons in common and the related financial importance, measured by number and value of transactions. Subsequently, the networks distinguished by the highest risk and, as such, warranting further inquiry are determined by associating each cluster with a series of structural, financial and investigative risk indicators.

Payment cards are shown again to be one of the sectors that inherently lend themselves most readily to network analysis, in that the related reports are distinguished by high transaction fragmentation and a large number of persons and accounts, often present in other STRs, not infrequently with identical characteristics. In 2022 the Unit scrutinized some 1,500 reports aggregated in networks with the above-described criteria, involving transactions potentially traceable to the exploitation of prostitution, frauds, unlicensed commercial activities, and the use of payment cards in countries at variance with the provenance of the user.

Since 1 September 2022 the UIF has been using the new System for Forensic Analysis of Virtual Currencies (see Section 10.5, 'IT resources'). This tool, clustering virtual currency

**System for Forensic Analysis of Virtual Currencies**

addresses<sup>9</sup> and exploiting information external to the blockchains (mainly Open Source Intelligence – OSINT), enables different addresses to be aggregated and, in some cases, to be traced to the entities that manage them (for example, virtual currency exchangers, terrorist organizations, listed persons, etc.). The introduction of this system enhances the UIF’s intelligence capabilities in the virtual currency sector.

## 2.5. Suspension orders

The UIF, at 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 is not prejudicial to 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 still to be executed or in response to unsolicited preliminary communications from intermediaries supplying advance information on the contents of STRs.

This is an incisive power, particularly effective for delaying the execution of suspicious transactions for a limited period of time pending subsequent precautionary measures by the judiciary.

In 2022 the Unit initiated 212 administrative proceedings with a view to the possible issue of suspension orders for suspicious transactions worth a total of €154 million (55.3 per cent more than in 2021). In 99 cases, a link to organized crime was discerned and, accordingly, the related information was shared not only with the Special Foreign Exchange Unit of the Finance Police, but also with the Anti-Mafia Investigation Department

The Unit undertook the inquiry at its own initiative in 90 cases, up from 67 in 2021 thanks in part to its exploitation of information on unexecuted transactions. On average, suspension proceedings were concluded within five days of their inception.

Altogether, 32 suspension orders were adopted, very close to the number of the previous year, but the value of the transactions suspended was far higher, much of it ascribable to a single measure (Table 2.3).

Table 2.3

	Suspensions				
	2018	2019	2020	2021	2022
Number of orders	47	43	37	30	32
Total value of suspended transactions ( <i>millions of euros</i> )	38.8	11.4	13.0	18.0	108.7

As in 2021, the majority of the evaluations regarded insurance companies, which accounted for 78 per cent of the total, while the share concerning banks fell from 17 to 12 per cent. The prevalent typology of transactions scrutinized for suspension remained policy

<sup>9</sup> Random alphanumeric strings that, at a first approximation, stand for the IBANs on which the network users’ virtual currencies are held in the blockchain.

surrenders or payouts at maturity traceable to natural persons under criminal investigation or close to organized crime.

One case evaluated with a view to suspension concerned a credit transfer initially requested of the intermediary by a company that was already the object of a complex financial examination on the part of the Unit, which found it to be involved in an extensive scheme of fraud to the detriment of several banks. Pending the suspension, seeing that the credit transfer had not been executed, the company's legal representative attempted to transfer the funds by means of a different bank transaction. Thanks to the exchange of information with the investigative bodies, the interest of the judiciary was promptly secured and the UIF consequently issued the suspension order, which was followed by a preventive seizure order.

## 2.6. Information flows of investigative interest and exchanges with the DNA

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

Coordination with the National Anti-Mafia and Anti-Terrorist Directorate (DNA) takes place through an exchange of personal ID data and other information stored in the respective databases.

The feedback on the investigative interest of the reports disseminated is particularly important for the UIF, allowing it to derive indications to gauge the efficacy of the activity performed and guide its choices regarding the handling of future reporting flows. For the reports sent to the investigative bodies in the two years 2021-22, at mid-March 2023 the Finance Police had sent more than 53,400 positive feedback reports, 83.5 per cent of them regarding STRs rated as high or medium-high risk; just 2.7 per cent of the positive feedback regarded low-risk or medium-low-risk STRs. In the same period, the Anti-Mafia Investigation Department (DIA) sent 224 positive feedback reports, of which 94.6 per cent in regard to STRs rated as high or medium-high risk.

The information exchanges with the DNA consist in cross-checks of personal ID data acquired preventively by the Unit on the reported persons (so-called name matching pursuant to Article 8(1), letter a, of Legislative Decree 231/2007) and feedback reports of interest on the data of the reports sent to the DNA pursuant to Article 40 of the Decree. As a result of this collaboration (see the box 'Memorandum of understanding with the DNA' in Section 7.2), the data in the UIF's possession has been enriched with information on persons under investigation belonging or close to mafia-style organizations. In particular, name matching – the only feedback received by the UIF on individual persons – makes possible ex ante orientation of the analysis with regard to the role played by the persons in the context reported and to widen the perspective and perimeter of analysis through the development of relational and financial networks cutting across the individual reporting flows. Like the feedback flow from the investigative bodies, the feedback reports from the DNA on STRs' investigative interest enable the UIF to make more efficacious choices for handling subsequent reports. Given the pronounced usefulness of such information in the different phases of analysis, work is proceeding for the complete integration of the outcomes of these exchanges into the handling of STRs, including through the construction of indicators that combine the risk levels of the feedback reports from the DNA with the data in the Unit's possession. For the STRs received in 2022, about 41,000 names, recorded in some 25,000 STRs, were found to be present in the DNA's archives.



### 3. RISK AREAS AND TYPOLOGIES

The UIF's operational analysis of suspicious transaction reports identifies typologies characterized by recurring elements material to the assessment of the risks of money laundering or terrorist financing, enabling the Unit to classify the reports and to disseminate updated guidance facilitating the obliged entities' identification of suspicious transactions.

#### 3.1. Context factors

In the course of 2022, active cooperation continued to be affected by the long wave of the COVID-19 pandemic, reflecting the economic and financial system's adjustment and the effects of the support measures taken over time. On the quantitative plane, the Unit analysed and transmitted to the investigative bodies 7,345 suspicious transaction reports referring to risk contexts linked to the pandemic and to the support measures, for a total value of more than €9 billion. Although 36.9 per cent more numerous than in 2021, these STRs did not reflect significant new underlying phenomena. The cases that did emerge were mostly variants of known phenomena and indicative of a progressive refinement of criminal activities, which could also be interpreted as a direct response to the efficacy of the preventive, investigative and repressive action undertaken in recent years and substantiated by the outcomes of many judicial inquiries.

Although to a lesser extent, the Russia-Ukraine crisis also had repercussions on the reporting flow. These stemmed from the gradual, massive expansion of the sanctions imposed on Russia by the European Union and the international community with the aim of weakening its economic fundamentals and significantly curtailing its ability to finance the conflict. The contents of the relevant reports received by the Unit – some 400 since the start of the war – are heterogeneous but can be classified, broadly, in three categories: often, they are motivated solely by the nationality or provenance of the parties involved and lack specific elements of objective anomaly; in some cases, though referring to transactions inherently devoid of significant risks, they regard natural persons listed or other entities designated following the issue of Community regulations and analogous international measures; in other cases, the transactions reported appear directed to circumventing the restrictive measures envisaged by the various packages of sanctions.

The consequences of the altered geopolitical context, starting from the energy crisis, have had a considerable impact on the economic situation of households and firms, protracting and sometimes aggravating their weakness in the wake of the pandemic and their resulting vulnerability to criminal financial activity. Meanwhile, the implementation of the NRRP has laid the groundwork for a speedy recovery capable, hopefully, of triggering stable growth with a battery of reforms and investments. The risks potentially connected to these factors reverberated, with varying degrees of intensity, on the reporting flow during the year under review.

Cases involving tax evasion, corruption and misappropriation of public funds, alongside those potentially traceable to organized crime, continue to be of central importance in the sphere of active cooperation, focusing the Unit's attention on the related contexts in view of the risk traditionally associated with them – a risk magnified by the typical promiscuity of these threats, which often makes clearly distinguishing them difficult.

### 3.2. Tax evasion

Reports of suspicious transactions relating to taxation were again one of the main components of the overall reporting flow. They accounted for more than a fifth of STRs in 2022 (20.2 per cent, against 16.8 per cent in 2021), drawing the Unit's attention to conduct suspected of being directed at tax evasion or reflecting strategies designed to avoid tax obligations.

Again in 2022 presumed invoicing fraud schemes made up more than a quarter of the STRs in question. The share relating to traditionally detected phenomena (such as funds transfers between connected natural and legal persons and the use of personal instead of company accounts) diminished slightly, while that concerning anomalous transfers of tax positions grew considerably. Among the latter, noteworthy were STRs on transfers of tax credits under Decree Law 34/2020 (the 'Relaunch Decree'), comprising 9.0 per cent of the total reporting flow for this risk area, the classification of which was facilitated by the introduction of a specific taxonomy to distinguish, within the broader category of anomalous transfers of tax credits and liabilities, the component ascribable to the post-pandemic measures, starting with the Relaunch Decree.

#### Transfers of tax credits

Many of the reports received during the year relating to anomalous transfers of tax credits evidenced transaction typologies already examined in depth by the Unit. The outcomes of these inquiries, known and largely typified, enabled the Unit to flank well-established analytical models with new methodological approaches, aimed at enhancing the added value of financial examinations and producing more robust investigative hypotheses for subsequent inquiries by the responsible bodies. An example is recourse, including in the context in question, to 'third-level' aggregate analysis, especially well-suited to more effective description and examination of complex phenomena in both objective and subjective terms.

An inquiry of this kind concerned 62 suspicious transaction reports grouped by recurrence of parties such as to indicate that they could be traced to the same operational perimeter. It focused primarily on credit transfers, whose counterparties were modelled as nodes of the network. The latter, considered as a whole, represented some 1,600 natural or legal persons to whom transactions worth more than €270 million were ascribable. A significant correlation was found, in amounts and timing, between collection of the payments for tax credits and the transfer of the credited funds to accounts abroad, predominantly in Asia (China, Hong Kong) and, less often, in Eastern Europe (Slovenia, Bulgaria), although the latter, according to Unit's analytical experience, often constitutes a mere transit point for the amounts to be ultimately transferred to Chinese territory.

Moving financial resources out of the country proved to be a common *modus operandi* not only of the subjects who transferred the ownership of the tax credits but also of the persons ('collectors'), who did not directly transfer any tax credits but acted exclusively as hubs for distributing the funds received from those who did. In general, these are firms which, even though recently created, have already gone or are about to go out of business; they operate in sundry sectors that cannot easily be reconciled with activities generating tax credits and at times they represent the last link of the chain, as beneficiaries of the repatriation to Italy of amounts initially transferred abroad. As to the 'collectors', the evidence acquired demonstrates frequent financial exchanges with persons flagged by cross-checking names with the databases of the DNA or with banks located in tax havens that also are crypto-asset service providers.

#### Other transaction typologies

In 2022 active cooperation again brought to light transactions potentially constituting attempts to circumvent tax law by interposing non-resident persons in the receipt of remuneration by beneficial owners so as to shield the latter from taxation in Italy.

In one case that the Unit examined, a sports club concluded an agreement for the early termination of a contract with a professional athlete, conferring on an agent resident abroad a mandate to finalize the agreement and stipulating the payment of a substantial fee in the event of a positive outcome of the engagement. The mandate was executed successfully and very quickly, with the consequent termination of the contract between the sports club and the athlete, who received an incongruously small sweetener by comparison with the fee payable to the agent. The latter initially received a non-taxable payment, being a non-resident and operating in Italy without a fixed base, and then transferred nearly the entire amount to a foreign company which, in turn, had engaged him to act as mediator in the termination of the same contract. This *modus operandi*, also found in similar contractual affairs with other athletes, enabled the Unit to identify the foreign company as the final beneficiary of the fee, most likely in the interest of the professional athlete, who thereby benefited from an otherwise undue tax exemption for the amounts received under the contractual relationship outstanding with the sports club.

### 3.3. Misappropriation of public funds and corruption

In the framework of the institutional measures deployed to cope with the post-pandemic crisis and impart impetus to a sustainable and lasting recovery, a crucial role is played by the NRRP, whose governance and implementation machinery hinge on the general government sector. The latter, given the huge volume of public resources to be allocated, the large number of projects and, often, their nature and complexity, is required to put in place effective safeguards, including informing the UIF of possible suspicious transactions detected in the various stages of project execution.

For the second consecutive year, the communications transmitted by general government entities pursuant to Article 10 of Legislative Decree 231/2007 registered a sharp percentage increase (+39.8 per cent), even though their number was negligible as a fraction of the total resulting from active cooperation (see Section 1.1, ‘Reporting flows’) and, for that matter, included a substantial share tied to the implementation of the NRRP.

#### Analysis of the STRs relating to the NRRP

With its Communication (*only in Italian*) of 11 April 2022, the UIF called attention to the risk factors connected with implementation of the NRRP and the need to adopt specific AML safeguards to prevent possible distortions in the use of public funds also by organized crime; it stressed the importance of making the best possible use of the AML system in the public sector, in view of the sector’s prominent role in the Plan’s implementation, and the need for the utmost speed in transmitting STRs, so as to enable the Unit to activate international cooperation and, possibly, exercise its power to suspend transactions.

With its subsequent Communication (*only in Italian*) of 31 May 2022, the Unit disseminated the new taxonomy to facilitate the active cooperation of obliged entities and thus enable the prompt identification of STRs showing aspects of anomaly during the procurement of access to the support measures or in the use of the funds made available (see Section 2.2, ‘The analysis process’).

In 2022 the Unit received 152 STRs classified as relating to the NRRP (of which 27 per cent concerning contexts potentially traceable to organized crime), for transactions worth a total of more than €264 million. About half of these STRs came from the general government sector, the rest mainly from banks and Poste Italiane SpA.

As was often seen with the public incentives connected with COVID-19, or, more recently, the measures to support Italian exporters hurt by the conflict in Ukraine, here, too, the Unit detected the widespread presence of networks of businesses that unduly procured access to subsidized financing and/or made improper use of the funds, which were frequently transferred abroad (particularly to China) to the benefit of corporate counterparties, including businesses traceable to persons flagged as in name matching with the DNA's databases. Often, the entities of the network are firms recently taken over by persons fronting for organized crime. At virtually the same time as they apply for the subsidies, these firms record changes in the scope of their business, especially in connection with measures directed at promoting specific sectors, or of their registered office, when a given geographical location serves to increase the sinking-fund component.

Professionals such as lawyers, accountants or consultants play a key role in the network, acting in all likelihood on behalf of specific central interests. These professional 'facilitators' assist the firms both in gaining access to the support measures, for example by providing the requisite attestations (often forged), and during disbursement, handling the opening of dedicated accounts (in many cases at the same bank branches, sometimes far from the business's headquarters). Analysis of these cases found that it was crucial for reporting entities to take a proactive approach to using their internal information resources and cooperating with the Unit in identifying the network or expanding its perimeter, through queries and responses or meetings for sharing detailed information on their vetting of applications and monitoring of activities.

Other patterns of illegal conduct involving public financial resources emerged from a number of STRs regarding anomalies in the receipt of the subsidies envisaged by the 'Culture Bonus'.

### **Analysis of the STRs relating to the Culture Bonus**

The Culture Bonus is a contribution of €500 introduced by Law 208/2015 for individuals just turning age 18 and resident in Italy. It can be spent at approved businesses only for specific cultural products and activities. It cannot be cashed or exchanged, and the amounts are disbursed through a platform, '18 app', subject to registration of the persons entitled and the merchants.

The reports relating to this measure were triggered by the finding of anomalies in the transactions recorded on the bank accounts of some interconnected merchants. Examination of them brought to light an apparently concerted operation designed to appropriate unduly received contribution reimbursements. The latter, ordered by the public body responsible for managing the funds, were largely withdrawn in cash, including via recharges of recently activated prepaid cards held by natural persons, often common counterparties of the businesses themselves. The remaining funds were paid by credit transfer to persons under investigation, gaming companies and firms traceable to names close to members of organized crime.

The cases intercepted appear to involve the purchase of bonuses through the recruitment of persons entitled (often by means of social networks or simply by word of mouth) and their subsequent conversion into cash through the sham sale of books or other products allowed by the law. This hypothesis would appear to be borne out by the absence on the businesses' accounts of transactions relating to the sale of goods and/or services linked to the subsidy and by some subjective circumstances pertaining to the firms, such as non-registration with the chambers of commerce or having minimum income scheme

beneficiaries as beneficial owners.

Other STRs regarded reimbursements of the Culture Bonus to businesses that sell IT goods, which may not be purchased with the Bonus, or whose activity is incompatible with the product categories contemplated by the measure.

The cases examined by the Unit, substantiated by investigative and judicial outcomes, delineate a picture in which the rules governing subsidies are circumvented at the time of their payment. The retention of such measures, albeit with some different features,<sup>10</sup> therefore makes it imperative for general government to tighten controls and for obliged entities to be made aware of the need for careful assessment of transactions for reporting purposes both upon the opening and during the monitoring of accounts to which payments by public entities under bonus schemes are credited.

The suspicious transaction reports involving corruption that the Unit received in 2022 show that the related dynamics, though unfolding in the secrecy of the relationships between corrupters and corrupted, do not impede obliged entities from detecting, within their sphere of operation, even latent signs of concealment of an exchange of favours. The fact, equally well established, that the actors move within variable schemes which are only in part recognizable and identifiable for reporting purposes makes the phenomenon worthy of the special attention that the UIF has always directed to it.

STRs generated by whistleblowing under the relevant laws and regulations proved to be of special interest for their implications with regard to corruption. While they do not concern distinctive or especially complex transactions, these reports have a common denominator in the grounds for suspicion, which mention the existence of communications by the whistleblower regarding irregularities, unlawful acts or crimes committed in public or private entities. In the cases of this kind examined in 2022, the whistleblowing communications mentioned in the STRs concerned presumed episodes of corruption of substantial importance both for the amounts at stake and for the nature of the natural and legal persons involved.

Whistleblowing

To give an example, there was a case involving payments approved by high-level managers on behalf of a company even though they were apparently unrelated to the company's ordinary operations and no services or goods had been supplied by the counterparty; these circumstances, considered together with the whistleblowing report, gave rise to the suspicion that the manager may have benefited from some form of utility in exchange for the unmotivated and unusual approval of payments. In another case, the Unit received a report concerning financial operations traceable to politically exposed persons, giving rise to the suspicion that the funds may have had an illegal origin in the form of bribes from companies tendering for works executed on behalf of regional or local authorities.

### 3.4. Organized crime

Continuing work begun in previous years, in 2022 the Unit refined the criteria for identifying and classifying suspicious transactions associated with the organized-crime risk area, on the basis of indicators derived from various internal processes of analysis and from regular information exchange with the DNA pursuant to Article 8 of Legislative Decree

<sup>10</sup> The 2023 Budget Law (Law 197/2022) provides that from 2024 the Culture Bonus will be replaced with two new €500 bonuses with a cumulative benefit cap of €1,000: the Youth Culture Card, for 18-year-olds belonging to households with Equivalent Economic Situation Indicator (ISEE) income of at most €35,000; and the Merit Card, for persons aged 18 who get the top mark in their high-school graduation exam.

231/2007. The Unit also undertook initiatives aimed at strengthening its ability to select cases and operating contexts which, though not directly ascribable to organized crime, are the visible expression of relational networks intended to further criminal interests. In this framework, a set of risk indicators to support inquiries is being defined, based on quantitative, qualitative and discretionary factors of evaluation.

As to the numbers, more than 18 per cent of the STRs received were classified as potentially traceable to the interests of organized crime, and 6.5 per cent were subjected to second-level analysis. In some cases, where required by the specific context, the Unit conducted third-level analysis in the form of social network analysis, enabling it to reconstruct complete relational and operating schemes.

In one important case, the UIF mapped a network of persons engaged in the monetization and appropriation of funds whose *modus operandi* suggested the existence of a central command. The funds targeted for misappropriation originated partly from the transfer of tax credits under the 'Relaunch Decree' and, to a larger extent, from transfers ordered by companies active in the metals sector. The Unit traced recurring financial channels, some of them pre-dating the transfer of tax credits, used to launder substantial amounts of funds potentially deriving from various crimes most of which apparently involved violations of tax law. These resources were transferred abroad, above all to China, at the end of swirling movements of funds among numerous persons, often with the intervention of recently created single proprietorships based mostly in Campania. Worthy of note was the involvement, with a central role, of numerous names already in the sights of some Anti-Mafia District Directorates, as well as of persons who were flagged as positive in name matching with the DNA's databases.

There was little change with respect to 2021 in the percentage of positive feedback reports from the investigative bodies on the STRs of the category in question, which remained at rather high levels (22.6 per cent). Of considerable impact was the reporting flow including names matching with the DNA's databases, amounting to 86 per cent of the STRs of this kind; the related feedback of interest from the DNA also added value to the information dataset.

The year saw an increase in the incidence of communications for the purpose of suspending transactions deemed to be connected to organized crime on the basis of the information provided by the reporting entities or derived from the Unit's archives or from information exchanges with the DNA (46.7 per cent of the cases examined).

As in the past, the geographical distribution of reports shows a strong correlation with the mappings of organized crime's bases as presented by the DIA and the DNA in their respective reports. In particular, 19.8 per cent of the reports regarded Campania, followed by Lazio (14.4 per cent) and Lombardy (14.1 per cent); after them came Sicily (8.1 per cent), Puglia (6.4 per cent), Calabria (5.3 per cent) and Emilia-Romagna (5.1 per cent). Rome, Naples and Milan were again, in that order, the three provinces with the highest volumes of transactions potentially traceable to the interests of organized crime, with an overall incidence of 32.9 per cent.

As regards typology, the operating schemes reported resembled those recorded in past years: a good part of the reports were found to reflect tax manoeuvres (22.2 per cent) and a significant share documented the foreign provenance or destination of flows whose reconstruction was possible thanks to international cooperation.

Some of the reports analysed confirmed the propensity of mafia-like organizations to seize on the vulnerabilities and opportunities for profit arising from crisis situations and the support measures taken to cope with them. Of the reports of suspicious transactions

potentially traceable to organized crime, 5.8 per cent bore on the risk area connected with the pandemic and the related economic support measures. The analyses performed by the UIF in this area mainly concerned cases of undue receipt of financing under the emergency legislation or misuse of such funds, also with reference to resources allocated under the NRRP.

With regard to the award of public contracts connected with the implementation of the NRRP, important provisions include measures to simplify the access process and the procedures for acquiring and presenting anti-mafia certification provided for by the legislation in force (Decree Law 13/2023 converted by Law 41/2023).

Indicative is the case of a group of connected companies, based in the same region, engaged in municipal solid waste disposal for local authorities and traceable to names detected in the check performed pursuant to Article 8 of Legislative Decree 231/2007, already involved in judicial proceedings for mafia-like crimes, and suspected of having links with the local criminal clans. The scheme the Unit reconstructed would appear to be potentially directed at circumventing the restrictions imposed by anti-mafia interdictions on the possibility of doing business with the general government sector. This was to be achieved by reorganizing the activities of the company subject to the ban, leasing a branch of the business to a new company, formally outside the group but with evident financial and personal ties to it.

The results of the financial analyses also confirmed the interest of organized crime in the gaming and betting sector – these STRs accounted for 8.5 per cent of those attributable to the risk area in question – not only as a direct and immediate channel for laundering funds of illegal provenance but also through the establishment abroad of financial intermediaries with funds deriving from companies of the sector.

With regard to the latter point, international cooperation made it possible to trace the beneficial ownership of an EU electronic money institution to Italian parties linked to a Camorra clan already in control of a foreign group specialized in off-shore tax planning and the opening of anonymous bank accounts, which presumably directs its customers to the electronic money institution in question.

### 3.5. Further case studies

A recurring type of case among the STRs connected with the Russia-Ukraine crisis, especially in the early phase of the conflict, concerned numerous cash withdrawals from ATMs at branches of several Italian intermediaries with credit/debit cards issued by Russian banks, some of them under sanctions. The transactions in question were recurrent, involve amounts that were modest individually but substantial in the aggregate, and were carried out again and again within the span of a few minutes or with a high daily frequency, by means of repeated and rotating use of the same cards. Reconstructing the information contained in the related identifying codes enabled the Unit to trace the payment instruments to persons unknown to the branches where the transactions were executed in that they were not customers of the reporting intermediaries. The fact that the latter did not receive requests for reversal of debits or complaints for card fraud or cloning by third parties corroborated the suspicion that the operations might constitute a withdrawal of foreign funds in the light of the financial restrictions in place, which entailed, among other things, the blocking of access to international circuits (SWIFT) for some Russian and Belarusian banks. Potentially confirming this hypothesis was the unusual timeframe of the phenomenon, which erupted before the introduction of sanctions and abated rapidly in the subsequent days.

Russia-Ukraine  
crisis

Other STRs concerned more or less evident diversion schemes in connection with the various fund-raising initiatives promoted to assist the population of Ukraine in the humanitarian crisis precipitated by the conflict.

Emblematic is the case of a minister who, exploiting mandates to transact business on the bank accounts of charitable and religious entities, diverted a large part of the funds deposited, deriving from a multitude of donations from individuals, to gaming accounts managed by concession-holders through online platforms. The unlawful appropriation of the funds was completed through multiple credit transfers in round amounts, for different stated reasons, after they had been moved to the reported individual's personal accounts.

The Unit likewise received a number of reports relating to payments triangulation, carried out, for the most part, in order to permit the conclusion of business deals between Italian and Russian counterparties by circumventing the restrictions imposed by sanctions (see the box 'Anomalous triangulations with Russia: an analysis on SARA and ORO data' in Section 5.4). In general, these involve exports whose payment is managed by third parties, on the basis of presumed agreements that justify the delegation of payment, through recourse to intermediaries in a variety of locations (Turkey, Kazakhstan, etc.) that channel the funds to the seller. Some cases of special interest regarded transactions relating to luxury goods (with typical made-in-Italy characteristics) and items that can be used for both civilian and military purposes ('dual-use').

The same pattern of financial movements also concerned private customers, most of them born in Russia or resident there, for the payment of ostensible purchases of high-value goods or services, especially in real estate. Not infrequently the credit transfers were ordered via companies having an opaque corporate structure, with a view to making it complicated to reconstruct the transactions and trace them to the customers and, ultimately, to avoiding application of funds freeze or similar measures.

#### Works of art

In 2022 the Unit continued its exploration of the art market, whose large volume of business makes it attractive for criminal economic activity and especially for money laundering, not least in view of the inverse proportion between size and value and the ease of transfer that often distinguishes art. During the year the Unit received several STRs concerning possibly illegal utilization of artworks; these came not only from art market operators but, above all, from banks and financial intermediaries, through which payments for sales are routed, and trust companies, which step in for the customary purposes of title of ownership and administration of the assets.

The cases reported most often involved anomalies in the mechanisms for setting prices, which seem entirely random, arbitrary and detached from ordinary standards of reasonableness: for example, reporting entities found incongruences between the market price at which the sale was concluded and the higher/lower prices quoted on specialized online portals or those applied to previous sales of the very same works. Suspicions were also raised by multiple changes of ownership of the same work of art, which, plausibly, were not the fruit of normal market negotiations but, on the contrary, reflected the intention of the parties to dissimulate their illegal origin. Another element common to many reports concerned prejudicial information on buyers, sellers, intermediaries, persons involved in one way or another in the transfer of the goods and persons connected to these actors, generally for crimes relating to commerce in artworks, such as forgery, fencing and money laundering, but also for association with organized crime. Likewise, it was frequently found that third parties wholly extraneous to the reciprocal undertakings inherent in the contracts between the counterparties for sale and purchase intervened in the settlement of the transactions, suggesting likely recourse to fronts, especially in the absence of adequate documentation justifying their intercession. Not least in importance among the STRs the Unit received were

those reporting manoeuvres carried out for illegal tax purposes, such as evading the tax on donations by declaring in a public instrument, the fruit of fraudulent misrepresentation, a value well below the market value, or the evasion of other direct and indirect taxes in the case of transactions concluded by collectors or occasional speculators who actually are habitually engaged in a business activity.

Noteworthy among the cases examined was that of a company that approved a resolution for a share capital increase which the shareholders paid in via the contribution of a work of art of great value as determined by an ad hoc appraisal. To allow third-party investors to participate in the business project launched with the new financial resources acquired, the company issued a proprietary virtual asset with a total value equal to a fraction of the share capital and an exchange rate anchored to an existing well-known stablecoin. Especially suspicious was the procedure whereby the shareholders purchased the work of art, as it was impossible to accurately trace the transaction, which had taken place years earlier at a price considerably lower than the estimated value of the reported transactions.

The STRs concerning possible abuses in the management of crowdlending platforms, popular portals that facilitate the matching of supply and demand for financing to back specific business projects, were of special importance considering, among other things, their potential repercussions on the peer-to-peer credit market. The analyses performed by the Unit turned up methods of operation potentially involving uses of the funds raised inconsistent with the projects financed by the borrowers. The companies financed, most of them in the real estate sector, used the funds raised to repay other crowdlending loans that had been granted either to companies belonging to their group, by means of dedicated online platforms operated by intermediaries based in northern Europe and tied to them via ownership and/or management, or to their corporate officers, for subsequent employment in highly speculative investments (including derivatives and crypto-assets).

**Crowdlending**

Given the methods by which they were carried out and the persons involved, some with criminal records or involved in typically anomalous tax-related behaviour, the transactions in question appear to be part of a larger pyramidal, multilevel, fraudulent investment scheme (a so-called Ponzi scheme): the misuse of the funds with respect to the avowed purposes presumably does not allow the platforms to receive the expected cash flows from the projects financed, making it necessary to recruit additional investors to make up for the shortfall, with the possible reiteration of the mechanism until it collapses due to the impossibility of procuring new investors.

The Unit continued to receive a regular flow of reports of presumed fraud perpetrated by natural persons in the performance of professional activities or tasks inherent in the positions they hold.

**Embezzlement**

An emblematic case involved a conservator, appointed by a court under Law 6/2004 to protect a person whose ability to act is limited or impaired by physical or mental illness or disability. In detail, the conservator made substantial cash withdrawals from the bank account of the person under protection, followed shortly, in the same municipality, by cash deposits to a private account used for personal expenditures. Despite the normal margin of uncertainty as to the destination of the sums withdrawn and the origin of those deposited, the compatibility in amount and the timing of the transactions suggested that the conservator, abusing his office, may have embezzled funds belonging to the natural person under his protection.

More broadly, similar operations were found involving persons of advanced years who gave a third-party mandate on their bank accounts to individuals with whom they had no apparent family or legal relationship, who then transferred the funds on those accounts to personal accounts or used them for substantial withdrawals of cash.

Another example concerns the operations carried out by a professional, appointed by a court as a public official under Article 59-bis of the Code of Civil Procedure, to manage property sales as part of enforcement procedures. The analyses performed by the Unit found behaviour on the part of the professional aimed at appropriating funds to the detriment of an enforcement procedure on whose bank account the same professional had a third-party mandate. The funds, deposited by others as security for participation in a real estate auction, were swiftly transferred, at the end of a series of intermediate movements, to connected persons, some of whom, moreover, were flagged as positive in name matching with the databases of the DNA, or else were used for private investments.

#### Insider trading

During the year the Unit received several suspicious transaction reports relating to shares traded on regulated markets in Italy or other EU countries, in which the suspicion involved possible instances of money laundering tied to the abuse of privileged information by the persons ordering the trades. Usually, these involved transactions, already brought up in the envisaged communications to CONSOB, carried out by natural persons (of high standing, with appropriate financial culture and experience, or else devoid of elements of subjective anomaly) who prove to be directly or indirectly linked to the issuer of the securities by virtue of relationships that, in theory, could give them access to information on listed companies (corporate strategies, earnings estimates, etc.) not yet divulged to the market and which, if made public, would be likely to have an appreciable impact on the prices at which the shares are traded.

The trades in question are apparently carried out to profit from the short-term fluctuations of share prices generated by the publication of price-sensitive information. Usually, they involve purchases ordered just before rises in share prices; less often, sales of shares already held in the days immediately preceding the divulgence of adverse information on the issuer. Other recurring circumstances are the priority demanded by the traders in forwarding the orders, the inconsistency of the orders with the traders' transaction history, and the incompatibility of the trades requested with the principle of portfolio diversification as a risk management strategy, given that trades often involve large investments in a single equity security.

#### Scams via SDD and virtual IBANs

Some reports received in 2022 described operating schemes already known to the Unit,<sup>11</sup> bringing to light a novel variant capable of facilitating their execution by making their fraudulent nature less readily apparent and recognizable. The reference is to scams carried out by means of SEPA Direct Debit (SDD), the electronic preauthorized debit collection service widely used by both private and corporate customers for settling recurring transactions. In the usual versions, the mandates to authorize use of the service are based on presumed business relationships between counterparties likely in connivance, who intervene in the role of debtor and creditor companies. The latter, exploiting the lag of the interbank clearing system, present multiple SDD claims to the banks and, once they have received the advance payments subject to successful completion, immediately empty the accounts to which the advances have been credited, generally via domestic or cross-border credit transfers to natural and legal persons of doubtful repute, before the notices of payment failure reach the banks.

An addition to this mechanism is the use of so-called virtual IBANs (vIBANs), an innovative service whereby one or more 'digital' IBAN codes can be associated with a single 'physical' bank account or payment account, offering customers automatic reconciliation in real time of banking transactions by means of dedicated IT platforms (see the box 'Virtual IBANs: AML issues' in Section 6.1). Availing themselves of vIBANs, the creditor companies present the SDD claims, indicating the vIBANs generated at a third-party intermediary and

<sup>11</sup> UIF, *Annual Report for 2017*, p. 60, and *Annual Report for 2019*, p. 47.

formally associated with the names of presumed debtors who in fact do not match the holder of the 'physical account' and are sometimes totally unaware of being involved in the scam. Magnifying the complexity of the schemes is the intervention of companies that interpose themselves between the creditors and the debtors by requesting activation of the vIBAN service on existing or new accounts and whose names are unknown to the scammed intermediaries.

The vIBANs, that is, enable the designers of the criminal scheme to create a further stratification of operations that conceals it from the view of the defrauded banks, impeding identification of the holders of the 'physical' accounts to which the failed payments should ultimately be debited. Furthermore, the 'one-to-many' association of accounts that characterizes the vIBAN service allows the fraudsters to limit the number of 'physical' accounts they have to open in order to perpetrate the scam while being able to count on a large number of vIBANs associated with debtor companies for communication to the banks targeted by the scam, thus raising fewer suspicions on the part of the latter and consequently triggering less stringent controls.

The frauds described above, though perpetrated against several different banks, were traced to the same operating perimeter thanks to the subjective recurrences (creditors/debtors, directors, beneficial owners, etc.) and objective recurrences (contracts underlying the SDD mandates, Device IDs of the devices for connecting to Internet banking services, etc.) during financial analyses, whose investigative developments led the judiciary to issue freeze measures.

Other instances of fraud concerned mortgage loans granted and disbursed to individuals for the purchase of their principal residence. The financial analyses performed were triggered by several STRs on transactions concentrated on a small number of neighbouring branches of the same bank and featuring the intervention of the same notary for the conveyance of title, giving rise to the suspicion that the granting of the mortgages could be part of a context in which ramified mafia-like organizations exploit the mechanisms of loan disbursement by exploiting specific professional competences of affiliates, associates or persons close to them to pursue illegal ends. Heightening these suspicions were the properties involved (often dilapidated or else located in run-down urban areas), the agreed sale price (substantially above market value), the impossibility of contacting the borrowers upon non-payment of loan instalments and the adverse finding regarding the persons involved in the transactions in various capacities.

Frauds on mortgage loans ...

One group of reports concerned the disbursement of mortgage loans with a loan-to-value ratio of up to 160 per cent through an expedient constituting the linchpin of the fraud and underlying probable collusion among the different parties involved: the indication, in the final instrument of conveyance, of a price well below the amount borrowed, which had been determined during the loan examination and was correlated to the price stated in the preliminary agreement, the appraisal value and the price indicated in the draft conveyance instrument given by the bank to the notary before the closing. The borrowers withdrew a part of the excess of the loan over the price of the property in cash and transferred it to persons connected to the notary with a series of small cheques drawn on accounts at intermediaries, other than the lending bank, to which part of the extra funds received with the loan had been transferred beforehand.

Other cases were distinguished by the transfer of most of the funds credited to borrowers to the benefit of a person who acted as the sellers' attorney in the conclusion of the final agreement of sale, as well as by the partial repayment of the mortgage instalments with funds made available by the attorney or created with credit transfers in respect of presumed emoluments by companies whose names recur in the various STRs analysed.

Upstream of these operations, during the loan examination the applicants presented the defrauded banks with forged ID documents or untruthful information concerning their income status, stating, for example, that they had employment contracts with companies that subsequently denied that the applicants were employees of theirs.

In addition, the financial analyses performed with reference to the end beneficiaries of the amounts borrowed sometimes brought to light transfers compatible in many respects with the operating methods of usury.

#### ... and in the automotive sector

Several reports regarded a wide-ranging scam in the automotive sector, set up by creating companies or sole proprietorships with business names similar to those of known franchises or dealers, inducing third parties to trust their identity. The buyers were thus misled into making credit transfers for their purchases to the benefit of the scammers, who, once the amounts were credited, immediately transferred the funds to other accounts, often located abroad, or withdrew them in their entirety without delivering the vehicles.

These operations were detected as a result of the multiple requests by transferors to revoke payment orders or the complaints of fraud they submitted to their banks. Upstream, it was found that the self-styled dealers had usurped the data on vehicles up for sale (technical fact-sheets, photos, price lists, estimated values, etc.), published them on their own websites with logos and graphics copying those of the actual companies of the sector, and offered the cars at advantageous prices without actually having them available.

#### Crypto-assets

Reports concerning virtual assets show a progressively rising trend.<sup>12</sup> The most common grounds for suspicion bear on the origin of the funds used to purchase the assets, often related to possible violations of tax law, phishing or episodes of ransomware. Suspected cases of fraud were detected in online trading and investment carried out on foreign platforms, many of them unauthorized, by the victims following persistent telephone calls or with the intervention of self-styled financial consultants; usually, by virtue of presumed partnerships with the principal exchangers, low commissions are requested for the investment in crypto-assets.

Other frequent cases regard the offering of exchanger services without adequate organizational safeguards for customers and failure to comply with the AML rules; or, further, financial flows that are part of schemes designed to cheat the tax authorities by means of transfers of fictitious tax credits deriving from construction expenses, whose amounts are withdrawn in cash or used to buy crypto-assets and gold bars. Functional to these activities are the services of ‘decentralized finance’ (DeFi),<sup>13</sup> which pose new challenges for the application of AML/CFT safeguards, particularly as regards identification of the service providers.

#### Gaming and betting

The gaming and betting sector continues to display shadow areas that could favour money laundering. A number of reports transmitted by online gaming service providers drew the Unit’s attention to presumable chip dumping arrangements<sup>14</sup> that their internal anti-fraud procedures had picked up. The scheme envisages the channelling of funds of illegal origin to gaming accounts, transfers made to seem legitimate by recourse to chip dumping, followed by the collection of those amounts in cash by presenting vouchers at recurring sales points located in the same geographical area. The fact that the players reside in the same area and

<sup>12</sup> See UIF, *Newsletter*, no. 5, 2022.

<sup>13</sup> Applications, developed by means of smart contracts (computer programs executed in decentralized mode by the web), that make it possible to realize more or less disintermediated business models, e.g., exchangers, loan platforms and stablecoins.

<sup>14</sup> A form of collusion between players enabling them to transfer money between themselves by rigging the outcome of a game.

that transactions are carried out on adjacent dates suggests the existence of a more far-flung network of persons involved, directly or merely as fronts, in collusive behaviour directed at laundering illegal proceeds of phishing, payment card cloning and scams of various kinds.

A peculiar characteristic brought up in reports was the finding that, during due diligence, many individuals provided ID data which were similar, illogical or inconsistent (different and/or geographically distant places of birth and residence, non-existent addresses, wrong postal codes, etc.), suggesting that the transactions were ascribable to a single natural person acting under different false names. This hypothesis was borne out by the use of the same responses to the 'secret questions' used for the recovery of passwords to gaming accounts. In addition, the examinations of the transactions effected at the sales points most extensively involved did not rule out complicity on the part of the merchants, who were in a position to allow the vouchers to be cashed by persons other than the applicants.

Lastly, there were instances of some gaming outlets promoting games, without the concession-holder knowing, on websites not authorized by the Customs and Monopolies Agency (included in the list of sites subject to interdiction) by means of unallowed procedures, e.g., collecting bets on events not included in schedule made available by the Agency or having video terminals not in conformity with the provisions of Articles 110(6) and 110(7) of the Consolidated Law on Public Security. These circumstances delineate an unauthorized conduct of gaming or betting business and favour money laundering through operations that are untraced and outside the control of both the concession-holder and the responsible authorities.



## 4. COMBATING THE FINANCING OF TERRORISM

Analysis of suspicious transaction reports relating to terrorist financing follows the same sequence of phases as analysis of money laundering reports. As the suspicion in this case concerns organizations or persons that could plan and carry out terrorist attacks, first-level analysis of the reports is crucial and is conducted as rapidly as possible to ensure that their information contents are promptly shared with the investigative bodies.

The examination of terrorist financing STRs, in which the subjective element of the actors involved carries fundamental weight, serves to reconstruct 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.

The perception of the risk of terrorist financing that emerged from suspicious transaction reports in 2022 remained largely associated with the jihadi threat. In the European context, that threat still mainly concerns the danger of violent attacks carried out by small groups ('cells') or isolated individuals ('lone wolves') with means that do not require significant organizational or financial resources.

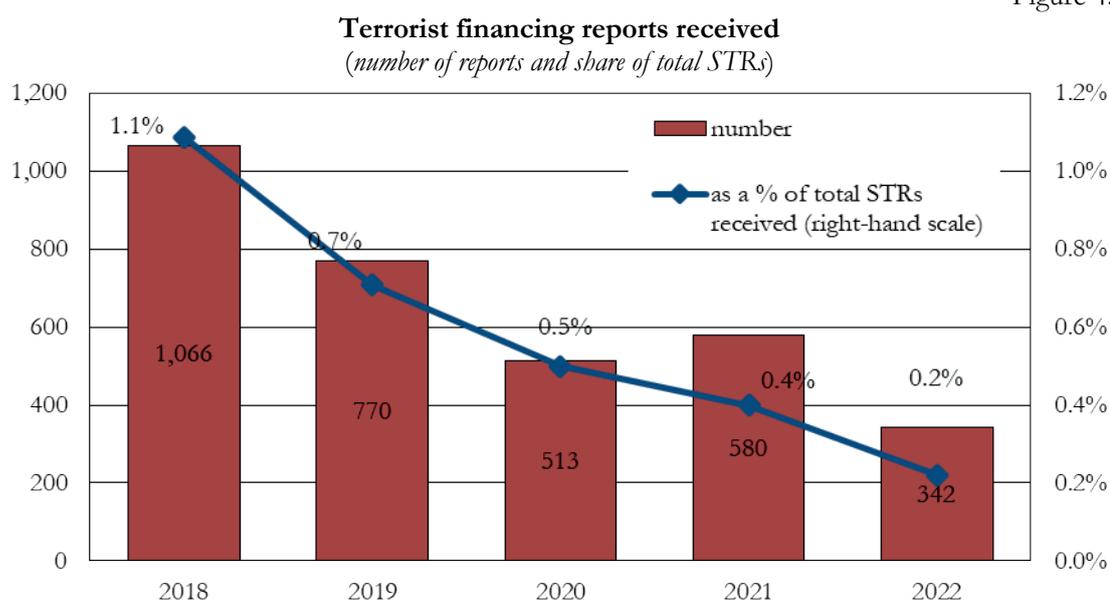
Against this background, from February 2022 onwards the outbreak of the Russia-Ukraine conflict gave rise to suspicions on the part of reporting entities relating to profiles of terrorism potentially associated with that event. Partly shaping this perception were reports in the mass media about Italian nationals or residents who had supposedly joined the fighters on both sides of the conflict. In some cases, these referred to persons already scrutinized in the past by the investigative bodies for their involvement in groups espousing radicalism and violence.

### 4.1. Suspicious transaction reports

The Unit received 342 reports regarding terrorist financing, 41 per cent fewer than in 2021 (Figure 4.1), with the incidence of such reports in the total reporting flow diminishing further, to 0.2 per cent. The UIF forwarded a total of 392 terrorist financing STRs to the investigative bodies in 2022, including STRs that the reporting entities had flagged for possible money laundering but which the UIF also profiled for terrorist financing.

The overall decline in the number of reports left the distribution by type of reporting entity broadly unchanged (Table 4.1): money transfer agents transmitted the largest share (47.7 per cent, up slightly from the previous year), followed by banks and electronic money institutions (30.7 and 14.0 per cent, respectively), less in both cases than in 2021. Non-financial entities, though continuing to play a marginal role compared with banks and financial intermediaries, accounted for almost 5 per cent, reflecting, in particular, the contribution of some auditing firms regarding natural or legal persons sanctioned by the European Union in relation to the Russia-Ukraine conflict.

Figure 4.1



The number of transactions reported fell along with the number of reports, but less sharply, from nearly 60,000 in 2021 to about 42,300 in 2022, a drop of just under 30 per cent.

Table 4.1

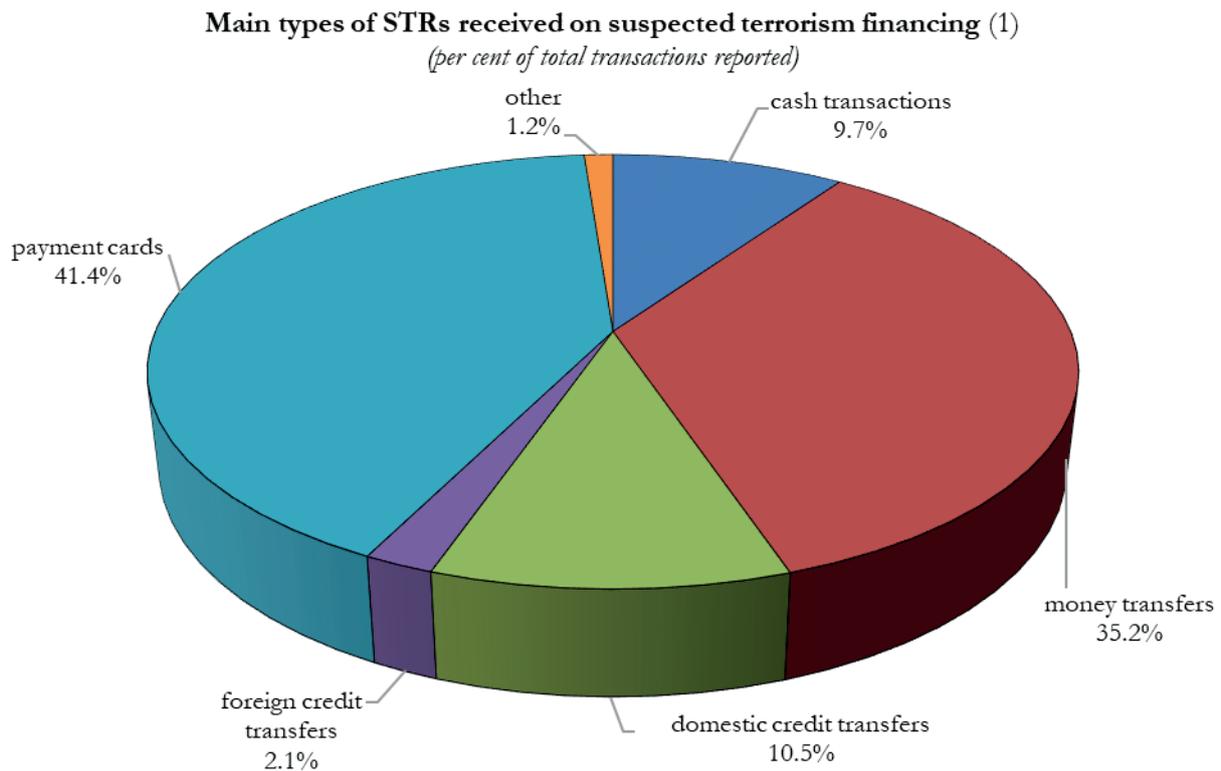
#### Terrorist financing reports by type of reporting entity

	2021		2022	
	(number of reports)	(share %)	(number of reports)	(share %)
<b>Banking and financial intermediaries</b>	<b>569</b>	<b>98.1</b>	<b>326</b>	<b>95.3</b>
Payment institutions and contact points	271	46.7	163	47.7
Banks and Poste Italiane SpA	196	33.8	105	30.7
EMIs and contact points	96	16.6	48	14.0
Other (1)	6	1.0	10	2.9
<b>Non-financial obliged entities</b>	<b>11</b>	<b>1.9</b>	<b>16</b>	<b>4.7</b>
Notaries and Nat. Council of Notaries	9	1.6	8	2.3
Other (2)	2	0.3	8	2.3
<b>Total</b>	<b>580</b>	<b>100.0</b>	<b>342</b>	<b>100.0</b>

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

The distribution of suspicious transactions by technical form displays a significant inversion compared with the previous year: those carried out with payment cards rose to 41.4 per cent, overtaking money transfers (35.2 per cent) as the leading method of transaction. The procedure made available by the UIF for reporting networking arrangements continues to assist the transmission of STRs capable of depicting contexts that are highly fragmented across innumerable transactions. The UIF examines these highly useful reports with social network analysis techniques (see Section 2.4, 'Methodology'). Credit transfers and cash transactions again accounted for roughly one tenth of the total each (12.6 and 9.7 per cent, respectively; Figure 4.2).

Figure 4.2



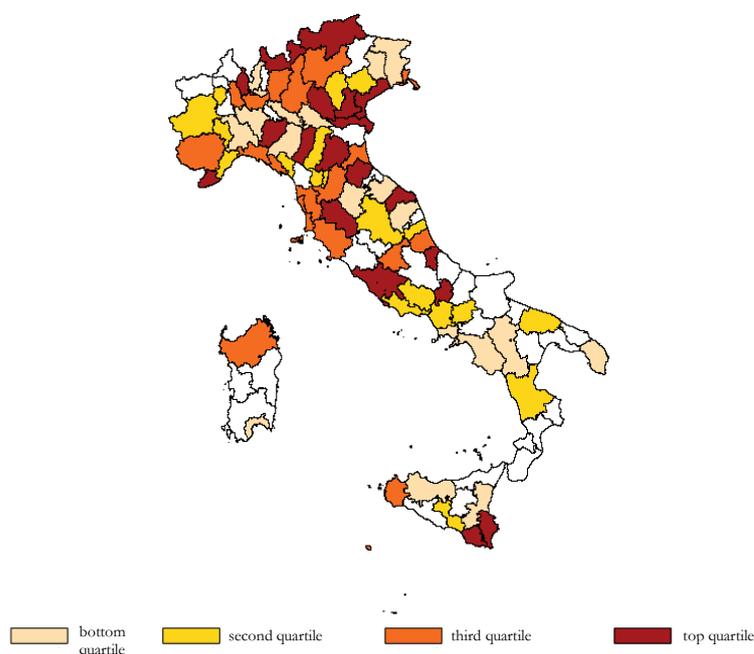
(1) The data are calculated taking into account the actual number of transactions, including those reported in aggregate.

The geographical distribution of the reports was similar to that of the three preceding years (Figure 4.3). Overall, once again the regions of the Centre and North predominate and the highest concentration is found in four geographical areas: (a) the northern provinces having border crossings with France (Imperia), Switzerland (Varese, Sondrio) or Austria (Bolzano); (b) the Po Valley, especially the parts lying in Emilia-Romagna (Piacenza, Reggio Emilia, Bologna, Forlì-Cesena) and Veneto (Rovigo, Verona, Padua, Venice); (c) central Italy, with the provinces of Siena, Ancona and Rome (and off-shoots in those of Pescara and Isernia); (d) coastal zones of southern Sicily (particularly the eastern provinces of Siracusa and Ragusa).

**Geographical distribution**

### Terrorist financing reports received by province

(number of reports per 100,000 inhabitants)



This confirms the reading the Unit proposed in the previous years, which ascribes the higher perception of risk to the geographical areas most attractive to immigrant groups for settlement - specified above at points (b) and (c) - or most convenient for transit traffic, like those indicated at points (a) and (b).

#### 4.2. Typologies of transactions suspected of financing terrorism

The partial change in the risk landscape referred to at the beginning of this chapter manifested itself in the transmission of a significant number of terrorist financing STRs (about 10 per cent of the total) triggered by the detection of persons subject to financial sanctions in connection with the Russia-Ukraine conflict. This produced a further increase in the share of reports with ‘subjective’ triggers, already traditionally predominant with respect to those prompted by financial transaction anomalies.

In broader terms, these two macro-categories (‘subjective’ versus ‘financial’ grounds for suspicion) still serve to frame the whole spectrum of contexts reported in 2022, regardless of whether the suspicion of terrorist financing refers to the jihadi ideology or to the conflict between Russia and Ukraine. The first macro-category embraces the STRs relating to customers – most often natural persons, but also firms or non-profit entities – whose ID data correspond to those of persons whose possible connections with terrorism have been identified by national or international authorities and communicated to obliged entities by means of procedures that vary depending on the degree of confidentiality required by the nature of the information source.

In this regard, there are two main information procedures. The first consists in confidential requests from an investigative authority to one or more obliged entities for information on some of their customers currently under investigation. The second turns on the lists of designation that some organizations (the United Nations, the EU, OFAC) publish

on their open-access websites to make known to the broadest possible public the ID data of the persons subject to financial sanctions for carrying out or financing terrorist activities. The sanctions for the persons designated by such lists typically call for the freezing of any funds deposited with financial intermediaries.

Corresponding to these two different channels of communication is a different distribution of STRs by category of reporting entity. In particular, the indication of confidential requests for information as the origin of the report is especially frequent in the case of money transfer agents. Given the global scale of their operations, in fact, they receive requests from both Italian and foreign investigative bodies, based on which they reconstruct networks at global level, sharing the resulting information with the FIUs concerned with the transactions identified.

By contrast, most of the STRs regarding persons possibly included in public lists of designation continue to come from banks and electronic money institutions, thanks to their updating of due diligence and continuous monitoring. It comes as no surprise, therefore, that most of the reports relating to the Russia-Ukraine conflict have come from these two types of reporting entity, added to which are notaries and auditing firms that, in the course of their professional activity of identifying ownership structures and beneficial ownership, detect the presence of natural or legal persons targeted by the European Union’s sanction regulations.

In the second macro-category, instead, the suspicion stems from the presence of purely financial anomalies already evidenced in operating schemes linked to the financing of terrorism. These usually include various kinds of information – sector of economic activity, stated reason for the transactions, manner of execution and payment instruments used – that typically can be acquired only by intermediaries with which customers have lasting financial relations, such as banks and EMIs, which in fact make the principal contribution to this class of reports.

Lastly, banks are responsible for almost all of the reports concerning non-profit entities suspected of involvement in terrorist financing, which numbered 32 in 2022, down by 15.8 per cent compared with the previous year, and accounted for 8.2 per cent of all the terrorist financing STRs (Table 4.2). The contexts reported continued to refer to possible connections with the jihadi threat or with the more general situation in the Middle East; analogous suspicions have not emerged, to date, in relation to the Russia-Ukraine conflict.

Table 4.2

<b>Reports on non-profit religious entities (1)</b>					
	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>
Number of reports	71	54	38	38	32
As a percentage of the total reports classified as financing of terrorism	6.0	6.5	6.9	6.1	8.2

(1) Reports sent to the investigative bodies in the year of reference. The number and percentage share include STRs originally filed on grounds of suspicion of money laundering.

### 4.3. The UIF’s analyses

The information input of the STRs exhibited a broad similarity with the suspected transaction typologies identified in the preceding years, so the UIF continued to follow well-established analytical approaches in examining them. The reports relating to the Russia-Ukraine conflict have had a rather limited impact in this respect, given their scant information

content. To date, the mere occurrence of names that appear in the lists of persons subject to sanctions, in the absence of anomalies indicating possible involvement in terrorist activities, has only sporadically provided a sufficient basis for developing financial analyses from the terrorist financing perspective, proving to be of greater use for probing cases of suspected money laundering in connection with tax evasion and for identifying figureheads.

More generally, the drop in the number of terrorist financing STRs did not significantly affect the typology of contexts reported, which showed a broadly unchanged proportion between reports relating to anomalous financial transactions on lasting accounts and those relating to transactions not involving movements on such accounts in that they consist of sequences of occasional operations (as in the case of remittances via money transfer services or recharges of payment cards).

For the first group of reports, the identification of the potentially significant aspects from the standpoint of terrorist financing turns on acquiring the documentation that the customer has provided over time to the different intermediaries involved, using the same methods of analyses employed for money laundering STRs, in order to ascertain if the reasons stated for the transactions reported as anomalous are compatible with their financial characteristics and, if they are not, to verify whether there are elements such as to suggest that the funds may ultimately be used for the benefit of organizations engaged in terrorism or ideologically contaminated by violent radicalism. For the reports in the second group, instead, the definition of the subjective profile often can only draw on elements that can be derived from the databases available to the Unit (especially the tax registry). In the absence of key information on the nature of the transactions, determining the paths of inquiry hinges on reconstructing the network of links by cross-checking the information in the Unit's possession with the information requested of additional intermediaries, identified thanks to the Registry of Financial Accounts.

The employment of these well-established methods of analysis, classification and assessment of the risk level of STRs found corroboration in the flow of feedback reports of interest from the investigative bodies, which corresponded to about 59 per cent of the STRs transmitted by the UIF for reasons of suspected terrorist financing, of which 29 per cent presented at least one name match with the databases of the DNA.

#### 4.4. International activities

The FATF has updated its analyses of ISIL's ability to generate revenues, now further diminished following its loss of territorial control. Its chief sources of financing continue to consist in criminal activities, above all kidnapping for ransom, trafficking in human beings and trafficking in cultural assets looted from archaeological sites, as well as in donations from sympathizers and from relatives of foreign fighters. In 2022, more extensive use of virtual assets by ISIL, Al-Qaeda and its affiliates was detected. In some cases, these terrorist groups collected and transferred funds by simulating charitable activities carried out in theatres of conflict. Money transfer agents and *hawala* networks<sup>15</sup> continue to be the channels most often used to transfer funds to activities located in conflict zones and to foreign fighters. In April 2022, the FATF published a report on the risks of money laundering and terrorist financing connected with the trafficking of migrants. Although clear evidence of systematic cooperation between terrorist networks and migrant trafficking has not emerged, in some cases payments to local terrorist groups have been found in the form of 'tolls' to facilitate the movement of people along migratory routes, especially in Africa.

<sup>15</sup> See UIF, *Annual Report for 2018*, p. 58.

During the year the UIF received 184 requests and spontaneous communications from foreign FIUs regarding terrorist financing. Although this was a considerable jump compared with the previous year, a large part (135) referred to cross-border transactions flagged in a single European country as anomalous on the basis of automatic screening criteria rather than specific suspicions tied to the subjective and operating profile of the individuals involved.

Most of the requests and spontaneous communications that the UIF examined regarded networks of remittances (particularly on-line transactions) by possible facilitators of terrorists, often identified on the basis of requests that the intermediaries had previously received from Italian or foreign investigative bodies. In a few scattered cases, the information received from abroad concerned the purchase, on e-commerce platforms, of material that could be used to make explosives.

All the information bearing on cases potentially linked to the financing of terrorism were shared with the investigative bodies on a priority basis. The UIF submitted nine requests during the year, most of them to FIUs of European countries: in two cases, the activation of foreign FIUs was requested in the framework of cooperation with the judiciary to ascertain the possible use for terrorist purposes of flows of money deriving from international smuggling.



## 5. THRESHOLD-BASED COMMUNICATIONS, SARA REPORTS, GOLD DECLARATIONS AND STRATEGIC ANALYSIS

### 5.1. Threshold-based communications

Article 47 of the Anti-Money Laundering Decree requires periodic transmission to the UIF of data and information identified on the basis of objective criteria concerning transactions at risk of money laundering or terrorist financing (so-called threshold-based communications). These data are used to enrich the body of information at the Unit's disposal for the examination of suspicious transactions and to initiate specific analyses of potentially anomalous financial flows.

The communications requirement – governed by UIF Measure of 28 March 2019 (*only in Italian*) – applies to banks, 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 in the form of occasional operations, including by way of single transactions of €1,000 or more. These communications must be submitted to the UIF monthly through the Infostat-UIF portal by the 15th day of the second month following the reference month.

Threshold-based communications constitute an important database on which the UIF draws for the performance of its institutional functions. It is a unique source of information, making available details on the actors and transaction characteristics of all cash movements carried out in Italy above the pre-set reporting threshold.

The UIF's decision to focus on cash reflects the particular risks bound up with that instrument. The ease of using cash and the untraceability of cash transactions can facilitate the laundering of illicit funds. 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 monitor cash transactions for the purpose of preventing money laundering.

Threshold-based communications relating to 2022 reported 45.3 million transactions worth a total of €242.9 billion, up by 4.8 and 7.7 per cent, respectively, from the previous year. The bulk of this increase came in the period from January to May, when the number of transactions grew by 12.8 per cent and their value by 17.6 per cent compared with the year-earlier period.

The monthly average was 3.8 million transactions (some 240,000 withdrawals and 3.5 million deposits) amounting to €20.2 billion, slightly more than in 2021 (Figure 5.1).<sup>16</sup> Deposits again far outweighed withdrawals, accounting for 93.6 per cent of the number and 95.5 per cent of the value of total transactions, owing to large-value transactions by businesses and particularly by major distributors.

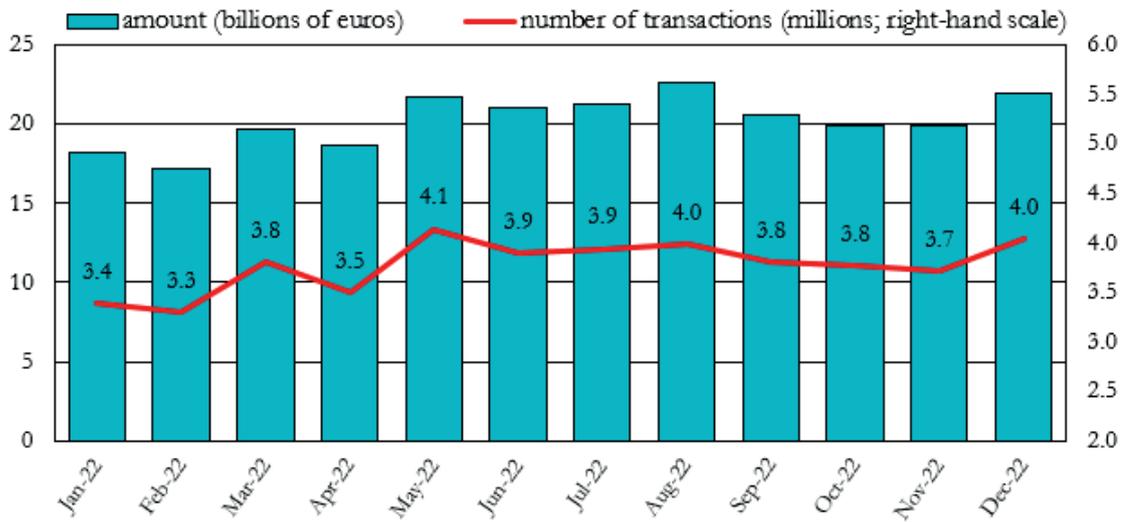
The average amount per transaction remained stable at about €5,470 for deposits and €3,790 for withdrawals, with median values of €3,270 and €1,950, respectively. There was a rising trend between January and May (amounts up by 19.4 per cent and number of transactions by 22.3 per cent), with brief interruptions in February and April, when the volume of cash transactions contracted slightly. From June onwards the number of transactions and the related value held steady, with August and December peaks confirming

<sup>16</sup> The data are subject to rectification by the reporting entities. The statistics published here are based on data available at 20 March 2023.

the influence of seasonal factors in the use of cash.

Figure 5.1

**Threshold-based communications**

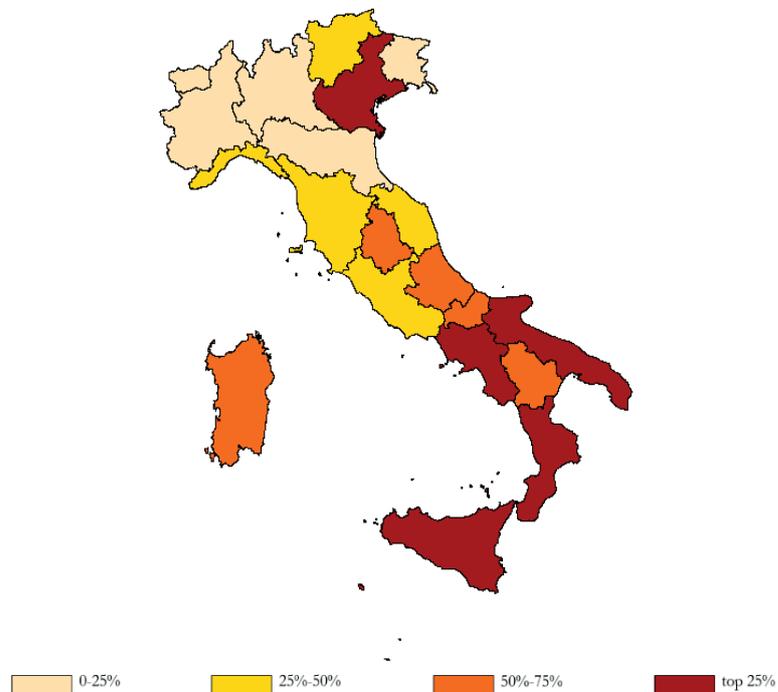


**Regional distribution**

At regional level, the overall value of transactions was highest in Lombardy, Veneto, Lazio, Campania and Emilia-Romagna, which together accounted for 57.7 per cent of the total. In relation to nominal GDP (in 2021), instead, the largest amounts were recorded in Veneto, Campania, Puglia, Calabria and Sicily (Figure 5.2).

Figure 5.2

**Threshold-based communications: amounts by region**  
(as a percentage of nominal GDP; quartiles)

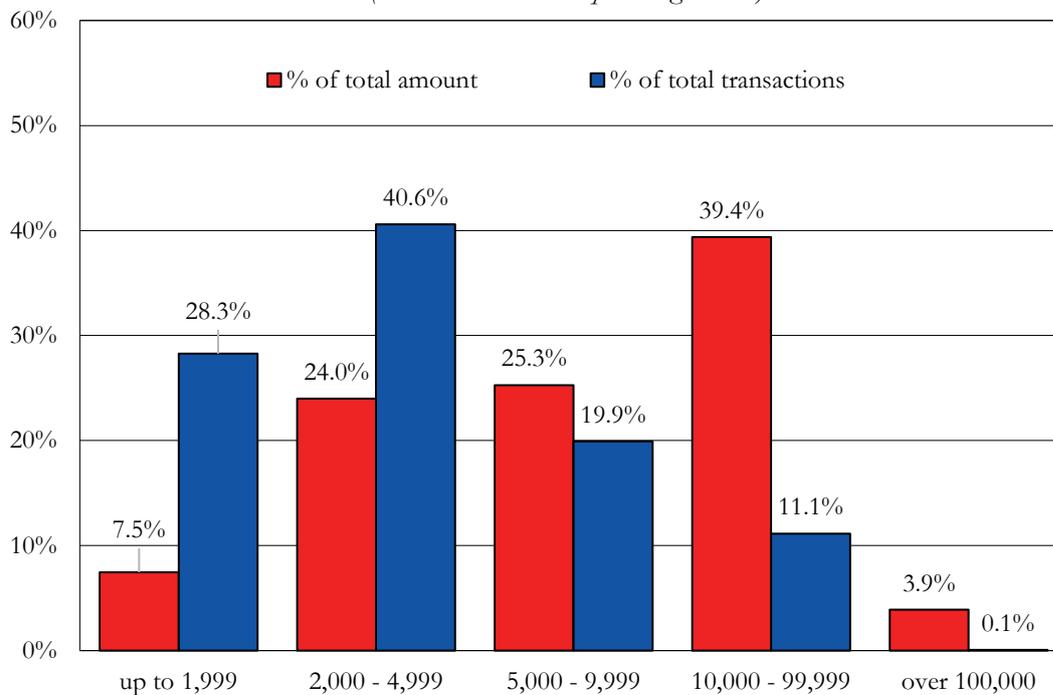


The data show a concentration of the number of transactions in the size class €2,000-€4,999 and of their value in the size class €10,00-€99,999, in line with the percentages of previous years (Figure 5.3). By contrast, transactions worth more than €100,000 grew by 17.5 per cent in number to 36,401 and by 16.2 per cent in total value to about €9.5 billion.

Distribution by size of transaction

Figure 5.3

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



Regarding the distribution of the amounts by type of transaction, cash deposits via ATMs or night safes, over-the-counter deposits and deposits with professional cash handlers remained prevalent, with percentages similar to those registered for 2021 (Figure 5.4).<sup>17</sup>

Transaction typologies

Most of the withdrawals (83.4 per cent) referred again to transactions by way of branch withdrawal forms or from cash handlers or from savings books (Figure 5.5).

At the end of 2022 there were 537 registered reporting entities. Banks, which accounted for 99.2 per cent of the total value of transactions surveyed in threshold-based communications, made up the vast majority of active reporting entities (351 out of 370; Table 5.1).<sup>18</sup> The communications of the top five banks accounted for 62.3 per cent of the total amount reported.

Reporting entities

Other types of operators (payment institutions and electronic money institutions) are responsible for less than 1 per cent of the total amount, not least because restrictive policies keep their cash transactions generally below the reporting threshold.

<sup>17</sup> Outgoing credit transfers shown in Figure 5.4 refer to operations in which the funds for the transaction do not come from a bank account but are delivered over-the-counter in cash.

<sup>18</sup> Inactive reporting entities are those that have requested to be exempted from transmitting monthly communications because they do not do business in cash or only handle cash transactions for amounts below the reporting threshold. Among them are many payment institutions and electronic money institutions, about 80 per cent of which have requested exemption.

Figure 5.4

**Threshold-based communications - deposit amounts**  
*(per cent of total deposits)*

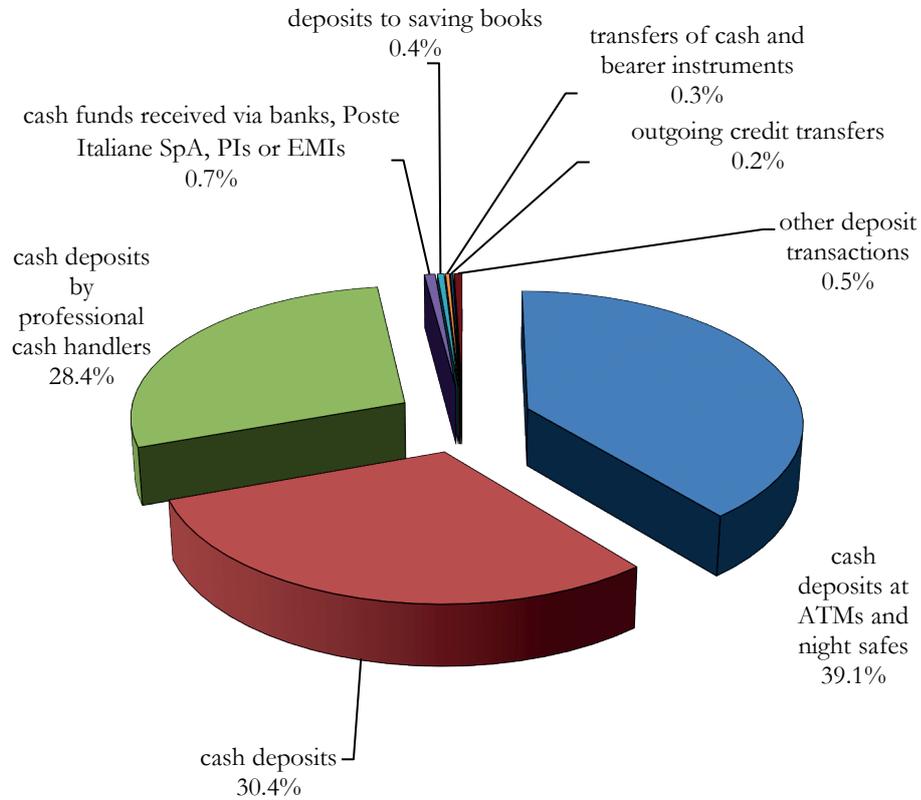


Figure 5.5

**Threshold-based communications: withdrawal amounts**  
*(per cent of total withdrawals)*

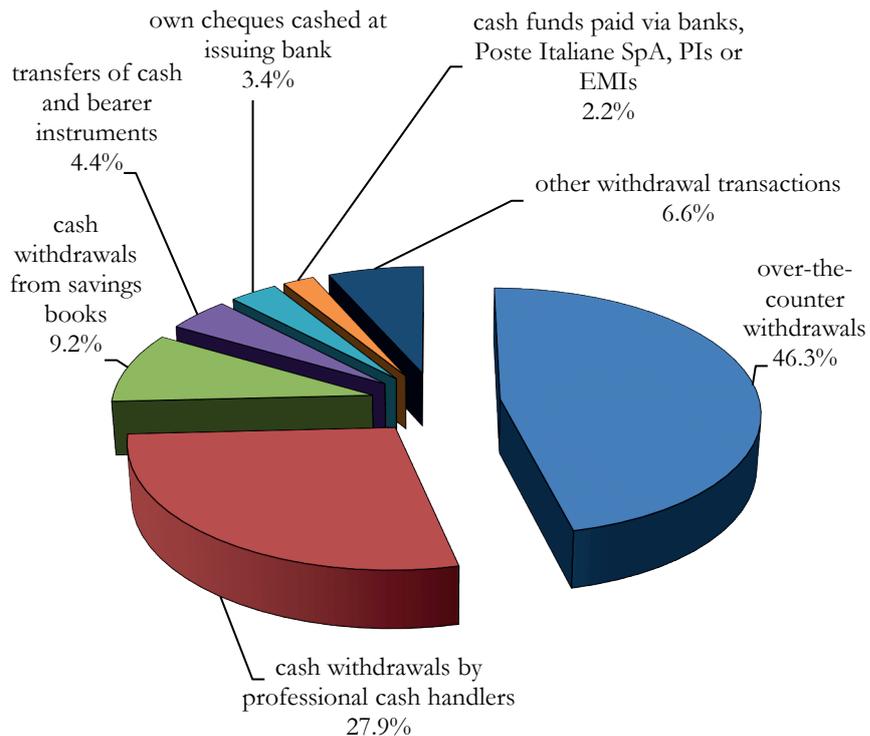


Table 5.1

	Amounts		Number of transactions	Average amount
	(millions of euros)	(% share)		
			(thousands)	(euros)
<b>Total</b>	<b>242,932</b>	<b>100.0</b>	<b>45,282</b>	<b>5,365</b>
<b>Banks and Poste Italiane SpA</b>	<b>241,050</b>	<b>99.2</b>	<b>44,868</b>	<b>5,372</b>
Top 5 reporting entities	151,260	62.3	28,014	5,399
Other obliged entities	89,790	37.0	16,854	5,327
<b>Payment institutions and contact points of EU payment institutions</b>	<b>1,500</b>	<b>0.6</b>	<b>294</b>	<b>5,106</b>
<b>Electronic money institutions and contact points of EU electronic money institutions</b>	<b>382</b>	<b>0.2</b>	<b>120</b>	<b>3,170</b>

The Unit has constantly monitored the quality of threshold-based communications since their inception in April 2019, finding widespread weaknesses in the capability of obliged entities to correctly record and report the data requested.

Quality of threshold-based communications

Although continual dialogue with the largest reporting entities has succeeded in identifying and rectifying the main anomalies found, other shortcomings persist and require remediation. The most common problems concern the complete and correct reporting of the place of execution of transactions, with special reference to the indication of the local unit at which withdrawals and deposits are made, sometimes omitted or else erroneously indicated as the intermediary's head office. In some cases, the error regards the municipality where the transaction took place, thus impeding correct identification of its location.

Additional problems regard the reporting of transactions in virtual cash,<sup>19</sup> failure to record in threshold-based communications cash transactions reported in STRs (even though the reporting threshold was exceeded) and omission of some attributes of the persons involved (e.g. customer's economic activity).

In the light of these findings, during the year the UIF stepped up its interaction with obliged entities and introduced further controls to identify reporting errors and foster their prompt correction. The actual effort exerted by operators to remedy these shortcomings will be monitored over time and also checked in the course of inspections.

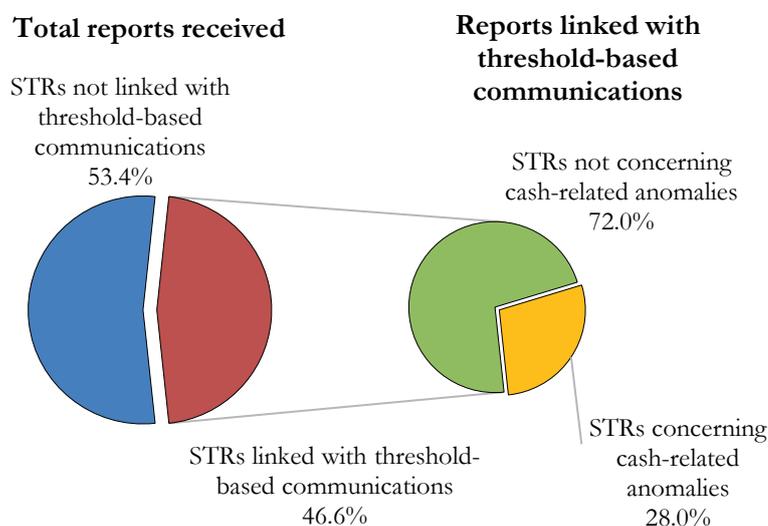
A total of 46.6 per cent of the suspicious transaction reports received in 2022 contain matches with threshold-based communications. This figure, somewhat lower than in 2021, could reflect an improvement in reporting entities' ability to identify potentially anomalous situations and distinguish them from the mere use of cash in the absence of further grounds for suspicion. In fact, only 28.0 per cent of the STRs received in 2022 matching threshold-based communications referred to instances of anomalous use of cash, while the remaining 72.0 per cent brought out different possible irregularities (Figure 5.6). Of the STRs that do not match the data of threshold-based communications (53.4 per cent of the total), those regarding anomalous use of cash amount to 20.7 per cent, down slightly with respect to 2021.

Matches with STRs

<sup>19</sup> Virtual cash transactions are simultaneous transactions of opposite sign that are carried out by the same person at the same intermediary and recorded as two cash transactions but which in reality do not involve actual physical movements of money. For example, the same person simultaneously making a withdrawal from a bank account and a deposit on a different account constitutes a virtual cash transaction and should therefore not be registered in threshold-based communications.

Figure 5.6

**Suspicious transaction reports received  
and links with threshold-based communications**  
*(per cent)*



During the year, with a view to examining some areas of interest in depth more closely and analysing new phenomena at risk of money laundering or terrorist financing, the Unit carried out a series of studies both for internal use and as part of its cooperation with the investigative bodies and the judiciary. The methods of inquiry and objectives of research were defined based on their ability to distinguish between situations in which cash may actually prove to be a factor of anomaly and situations in which it is a means of exchange in normal economic activity.

**Studies on threshold-based communications**

In 2022 the UIF, also in collaboration with some institutional organizations charged with fighting crime, conducted three main studies, identifying some contexts that warrant closer examination for the particularly anomalous procedures found in the use of cash.

A first study examined a set of transactions in cash relating to a specific territory indicated by the NSPV, using the links between the persons involved in the same cash transactions to bring out a wider activity also extending into non-adjacent areas. This approach made possible to conduct an overall examination of the actors and study their roles with intersecting information. Some of the persons involved appeared to be hubs of larger operations, while others turned out to be mere executors. Lastly, some individuals acted as linkages between different centres of interests.

The second study investigated the transactions of persons of foreign origin potentially involved in criminal activities, indicated by the DNA. It considered only the transactions carried out by executors of cash withdrawals, which represent a minority of the transactions contained in threshold-based communications but may be pointers to anomalous uses of cash. Several distinct profiles of anomaly were identified. For the natives of a certain Asian country, there emerged massive withdrawals from accounts held by companies, the funding of which seemingly refers to commercial activity in the clothing sector but which could conceal the intent of monetizing the company's account for illicit use. For the natives of an African country, instead, the largest cash withdrawals were made on accounts attributable to persons of Italian origin, for whom the executors presumably act as figureheads, thus cloaking the intention to dissemble the operation.

The third study compared different operating points of banks grouped in homogeneous clusters by size in a given territory of Italy, in order to highlight, also for possible inspection purposes, those characterized by anomalies in cash activity. In particular, the incidence of transactions not traceable to accounts (so-called over-the-counter transactions) was examined in view of their intrinsic opacity. Another line of analysis highlighted the operating points where a high percentage of customers make multiple deposits or withdrawals on the same day, behaviour that could conceal transaction splitting to make large movements of funds less evident. Further, an assessment was made of the importance of cash transactions carried out by natural persons or by sole proprietorships, potentially revealing movements of cash of a dubious nature, especially if the amounts are large. Lastly, the study considered the transactions carried out by persons operating on multiple accounts in the names of different holders or persons reported by other intermediaries. Initial applications of this methodology led to the identification of some anomalous situations in regard to which the Unit opened a dialogue with the heads of an intermediary's internal audit, in order to validate and enrich the methodology employed and realize ever more effective forms of active cooperation with reporting entities.

## 5.2. SARA reports

Aggregate AML Reports (SARA), submitted monthly by financial intermediaries, derive from the aggregation of data on their transactions according to criteria laid down by a UIF Measure ([only in Italian](#)). The data received from January 2021 onwards regard all transactions carried out by customers for amounts of €5,000 or more. The data are anonymous and cover the entire spectrum 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 and remittances). The data refer to both incoming and outgoing transactions, with the amount of any cash transactions stated separately.

The course of SARA data in 2022 reflected the altered macroeconomic conditions: compared with the previous year, the number of records transmitted and the number of underlying transactions rose modestly, by 7.7 and 4.0 per cent, respectively, while the value of the transactions reported surged by 27.5 per cent as a result of the post-pandemic recovery and the inflationary pressures that marked economic conditions during the year (Table 5.2).

SARA data

With respect to the last year before the pandemic (2018), the number of records and underlying transactions rose by around 70 per cent, while transaction value grew by 53.7 per cent, partly as a consequence of the UIF's latest SARA Measure ([only in Italian](#)), in force from January 2021, which lowered the reporting threshold to €5,000.<sup>20</sup>

<sup>20</sup> The comparison is with 2018, not 2019, because it was found that a group of reporting entities had transmitted some data incorrectly in 2019 (see UIF, *Annual Report for 2020*). For the UIF Measure, see UIF, *Annual Report for 2021*.

Table 5.2

<b>Aggregate anti-money laundering reports (SARA reports)</b>				
	<b>Number of reporting entities in the year</b>	<b>Number of records (1)</b>	<b>Total amount (billions of euros)</b>	<b>Number of underlying transactions</b>
Banks, Poste Italiane and CDP	469	149,727,437	44,788	441,438,317
Trust companies under Law 1966/1939	192	44,231	17	108,681
Asset management companies	245	2,158,951	278	10,055,916
Other financial intermediaries	206	2,739,835	404	6,832,311
Investment firms	129	265,689	198	2,318,737
Insurance companies	71	1,930,616	143	3,914,533
Payment institutions and EU-based PI points of contact	73	8,316,667	59	32,051,663
EMIs and points of contact of EU-based EMIs	18	9,451,082	135	67,867,299
Trust companies under Article 106 of the TUB	34	135,366	91	523,716
SICAFs	53	628	1	915
<b>Total</b>	<b>1,490</b>	<b>174,770,502</b>	<b>46,114</b>	<b>565,112,088</b>

(1) SARA data can be rectified by the reporting entities; the statistics given in the table are based on data as at 13 March 2023.

The degree of concentration of the transactions recorded in SARA data in the banking sector, responsible for 97 per cent of the transaction value reported even though it comprises just one third of all reporting intermediaries, remained unchanged during the year.

Good data quality is essential to ensure the reliability of analyses and studies of financial flows. To identify potential reporting errors, automatic checks based on statistical methods are performed on the aggregate data at the time of their acquisition by the UIF. This checking serves to detect not only possible erroneous data, but also possible anomalous flows warranting further examination by the reporting entity. There are two types of controls: systemic controls compare the data of each reporting entity with the reports of the entire system referring to the same months; and non-systemic controls compare the conduct of the individual intermediary with the reports it transmitted in the previous twelve months.

The data flagged as anomalous by the control algorithms are sent to the intermediaries for verification of their correctness and rectification of any recording errors.

#### Monitoring of data quality

In 2022 the Unit asked 808 intermediaries (including 434 banks) to run checks on more than 25,000 records that the system of controls on SARA data had identified as statistically anomalous. In 5.5 per cent of these cases, the reporting entities found errors in the data transmitted.

In 204 cases (0.8 per cent of the total flagged), the intermediaries re-examined the transactions to assess the possibility of sending a suspicious transaction report; in another 266 cases (about 1 per cent of the total flagged) matches were found to STRs already submitted to the UIF.

### Indicators of compliance with the SARA reporting obligations

Compliance with the rules and time limits for transmitting data is not uniform across SARA reporting entities. Furthermore, the number of reporting entities is large (in 2022 some 1,500 were registered with the reporting system). Monitoring them on an individual basis would be inefficient and costly.

Consequently, the Unit has devised a system of controls on SARA reporting entities' compliance level that provides an objective measure of the degree to which each entity fulfils its obligations. The ultimate purpose of the system, linked with the established automatic formal and statistical controls, is to ensure the quality of SARA data, which is crucial for UIF's intelligence activity at the operational level and, above all, for strategic analysis.

The system is based on a set of indicators regarding specific aspects of the management and transmission of SARA reports by intermediaries. The indicators are grouped in three categories, corresponding to the three main dimensions of compliance with the reporting requirements:

- organizational adequacy of the AML function: a check verifies whether the SARA reports officer (normally also the AML officer) holds an excessive number of positions with the reporting entity or with other intermediaries, and whether the position exhibits undue turnover;
- data reliability: the size of the reporting errors committed by each intermediary is measured by the deviation between the data supplied in any rectified reports and those transmitted previously; the frequency with which intermediaries transmit rectified data is also considered;
- regularity of data transmission: a check is run for instances of non-transmission of data, late transmission and the length of the delay.

On the basis of the analytical indicators, the Unit computes a composite indicator of compliance for each intermediary. This facilitates efficient and ongoing monitoring and can guide the UIF's control action in accordance with a risk-based approach.

After the considerable increase recorded in 2021, requests by reporting entities for assistance in transmitting SARA reports and gold declarations (see below) fell back to the 2020 level of about 2,200, still higher than in the preceding years.

The information on transactions carried out in cash is one of the most important components of SARA data from the AML standpoint. The SARA reports give not only the amount of cash withdrawn and deposited on bank accounts but also the amount settled in cash in other types of transactions (such as purchases and sales of securities and the issue of certificates of deposit).

Given the strong correlation between the use of cash and the size of the underground and illegal economy,<sup>21</sup> the cash transactions recorded in the SARA data receive special attention. In 2022 these had an overall value of €173.5 billion, 9.4 per cent more than in 2021; withdrawals totalled €8.4 billion and their growth rate of 17.0 per cent was almost double that of deposits (up by 9.1 per cent to €165.1 billion), while the number of underlying transactions rose overall by 6.7 per cent. The growth in cash transactions in 2022 did not

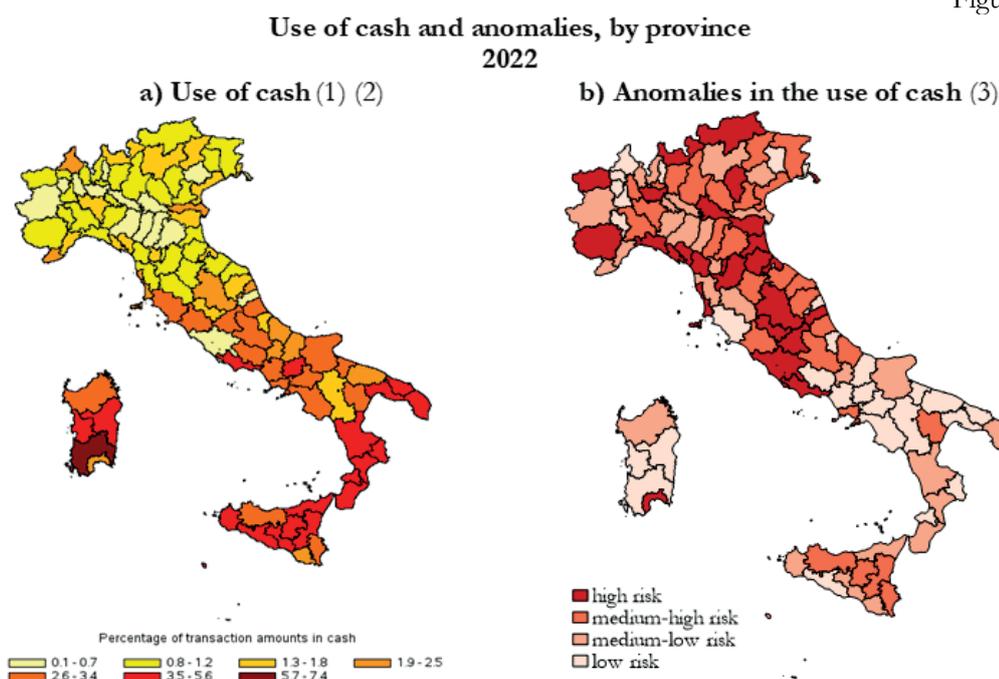
Use of cash

<sup>21</sup> See the study by M. Giammatteo, S. Iezzi and R. Zizza, 'Pecunia olet. Cash usage and the underground economy', *Journal of Economic Behavior & Organization*, 204, 2022, pp. 107-127.

recoup all of the pandemic-induced slump in 2020: compared with 2018, they were still down by 15.2 per cent in value and 23.0 per cent in number. This appears to confirm the signs, glimpsed in 2021, of a possible structural modification in spending habits as a result of the pandemic, with greater use of alternative payment instruments.<sup>22</sup>

Despite these developments, the geographical polarization between the Centre and North on the one hand and the South and Islands on the other does not appear to have undergone changes over time: the incidence of cash use in the total transactions reported to the UIF exhibits the traditional gap (Figure 5.7a).

Figure 5.7



(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 13 March 2023. – (3) Preliminary results. The target variable (use of cash) is updated to 2022, some explanatory variables to 2020 (the last year available as of March 2023). The shadow economy, at municipality level, is measured as a share of the under-declaration of value added estimated by Istat.

**Anomalies  
in the use of  
cash**

For a correct assessment of the picture that emerges from the diffusion of cash based on its utilization, one must consider the socio-economic and financial factors that determine the underlying propensity to use it (for instance, the diffusion of other payment instruments, spending habits, the local supply of financial services). Taking these fundamental determinants into account, we can identify the share of cash transactions that can be considered normal and isolate the potentially anomalous component, symptomatic of illegal activities. Using the econometric analysis developed some time ago at the Unit,<sup>23</sup> we obtain the underlying picture of the risk associated with the potential illicit use of cash, based on the incidence of the anomalous component (Figure 5.7b).

<sup>22</sup> The total value is less than that recorded for threshold-based communications (€242.9 billion; see Section 5.1, “Threshold-based communications”), owing chiefly to the differences in the reporting thresholds and the criteria for their application (€10,000 total, also as a result of multiple transactions individually in an amount exceeding €1,000, per person per month in the case of threshold-based communications; €5,000 per individual transaction in the case of SARA data).

<sup>23</sup> M. Giammatteo, ‘Cash use and money laundering: An application to Italian data at bank-municipality level’, UIF, *Quaderni dell’antiriciclaggio – Analisi e studi*, 13, 2019.

Going by this approach, in 2022, as in the preceding years, anomalous uses of cash were relatively more frequent in the provinces of the Centre (except for some provinces of Tuscany), in the North-West (especially the provinces of Cuneo, Genoa, La Spezia, Milan and Sondrio, as well as in Val d'Aosta) and in the North-East (particularly the provinces of Bolzano and Vicenza and in Romagna). In all these areas, among the richest in Italy, the level of cash use is lower, on average, than in the other provinces, but the better investment opportunities they offer seem to attract the interest of criminal organizations, among others. With the increments recorded during the year, the provinces of Mantua, Perugia and Rieti reached a significant level of risk compared with 2021. By contrast, in the provinces of Tuscany, the risk level diminished across the board.

Credit transfers are another payment instrument surveyed in the SARA flows that is of special interest for the fight against financial crime. The information content of the reports referring to credit transfers is substantial, also including data on the municipality (or foreign country) of residence of the counterparty and its intermediary. This wealth of information makes it possible to elaborate statistics and correlations based on the provenance and geographical destination of the funds.

Of specific interest are the cases in which a foreign intermediary involved in the transfer is located in a tax haven or non-cooperative jurisdiction: transfers of funds to these jurisdictions may be motivated by reasons that are not strictly economic but are bound up, instead, with the opacity of their tax and financial systems.

The effects of the economic recovery and the inflationary pressures that were felt in the course of the year stand out especially in the cross-border flows recorded in the SARA data: the total value of credit transfers rose by 37.6 per cent from €3,193 billion in 2021 to €4,392 billion in 2022, and by more than 60 per cent with respect to 2018. Outward credit transfers (up by 39.3 per cent, from €1,531 billion to €2,133 billion) made a slightly larger contribution to the overall growth than did inward credit transfers (up by 35.9 per cent, from €1,662 billion to €2,259 billion; Table 5.3).

The bulk of the flows is ascribable to trade with EU countries, whose share, boosted by 43.1 per cent growth, increased to 66.0 per cent. Credit transfers with non-EU countries increased by 27.9 per cent; the share attributable to the United Kingdom declined further, from 17.7 to 16.6 per cent. Among the other non-EU countries, there was an increase in the flows with the United States and China and a surge of 44.1 per cent in credit transfers in settlement with Russia, which nearly doubled with respect to 2018, driven above all by outflows relating to the energy sector.<sup>24</sup>

The flows with tax havens and non-cooperative jurisdictions<sup>25</sup> grew by 51.8 per cent, mainly as a consequence of the inclusion of Malta and Turkey in the official lists; net of these

**Flows with tax havens**

<sup>24</sup> According to United Nations Comtrade data, energy products represented more than 86 per cent of total Italian imports from Russia in 2022, with an increase in value of over 47 per cent compared with 2018. This trend was not affected by the economic sanctions that the European Union introduced in response to the war against Ukraine: the bans on seaborne imports of crude oil and of certain refined oil products from Russia have been in effect since 5 December 2022 and 5 February 2023, respectively.

<sup>25</sup> The list of non-cooperative jurisdictions and/or tax havens is drawn from the ministerial decrees implementing the Consolidated Law on Income Tax (TUIR), from the lists 'High-Risk Jurisdictions subject to a Call for Action ("black list")' and 'Jurisdictions under Increased Monitoring ("grey list")' published by the FATF in March 2022, from the 'EU list of non-cooperative jurisdictions for tax purposes' (February 2022 update) and from the list of countries identified by the European Commission with Delegated Regulation EU/2016/1675 and subsequent amendments. In 2022, Jordan, Malta, Mali, South Sudan and Turkey were added to the list and Botswana, Ghana and Iraq were dropped.

new entries, the increase would have been 30.3 per cent, less than the overall growth in cross-border flows.

Table 5.3

<b>Cross-border credit transfers by country of destination and origin (1)</b>			
<i>(billions of euros)</i>			
	<b>Outward</b>	<b>Inward</b>	<b>Total</b>
<b>Total</b>	<b>2,133</b>	<b>2,259</b>	<b>4,392</b>
<b>EU Countries</b>	<b>1,397</b>	<b>1,502</b>	<b>2,899</b>
France	422	452	874
Germany	396	411	806
Belgium	130	121	251
Netherlands	113	107	220
<b>Non-EU Countries</b>	<b>736</b>	<b>757</b>	<b>1,493</b>
United Kingdom	363	364	727
United States	146	167	313
China	34	15	49
Russia	17	12	29
Norway	6	5	11
<b><i>of which: tax havens or non-cooperative</i></b>	<b>120</b>	<b>118</b>	<b>238</b>
Switzerland	58	61	119
Turkey	15	14	30
Hong Kong	14	9	23
Singapore	8	5	13
Abu Dhabi	4	7	12

(1) See Figure 5.7, note 2.

The increase was especially steep in credit transfers in settlement with Abu Dhabi and Singapore (68.9 and 60.7 per cent, respectively). Compared with the preceding year, Albania and Senegal no longer figure among the top ten counterparty countries, having been replaced by Malta and Turkey (Figure 5.8).

The distribution by province of credit transfers with non-cooperative jurisdictions or tax havens is highly uneven across the Italian regions (Figure 5.9a).

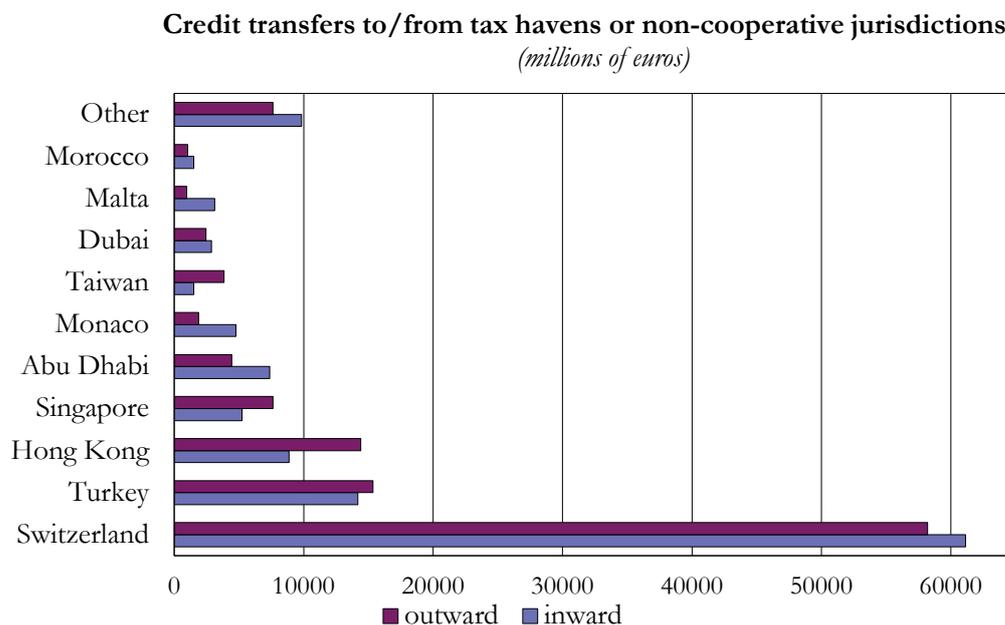
Compared with the previous years, in 2022 there was a higher incidence of cross-border outflows from the South and Islands, notably from Sardinia and from a good number of provinces of Calabria, Puglia and Sicily; the Marche region, too, showed substantial transfers, and the incidence of outflows was high again for the border provinces of Lombardy and Piedmont.

With regard to inflows, the share of credit transfers coming from non-cooperative jurisdictions or tax havens was relatively higher in some provinces of Basilicata, Liguria, Molise, Puglia and Tuscany, as well as in some border provinces.

The relative magnitude of the phenomenon changed in 2022. The incidence of outflows to non-cooperative jurisdictions or tax havens rose by an average per province of 1.8 per cent; the increase was sharpest in Sardinia and Umbria and, less markedly, in Abruzzo, Campania, Lazio, Lombardy and Sicily, the decline most pronounced in Basilicata and Molise. The incidence of inflows grew far more moderately, by an average of 0.7 per cent across all the regions, with larger increments in almost all the regions of the South and Islands, Lombardy, Marche, Piedmont and Tuscany; it contracted sharply in Abruzzo and

Val d'Aosta and, less so, in Sardinia.

Figure 5.8



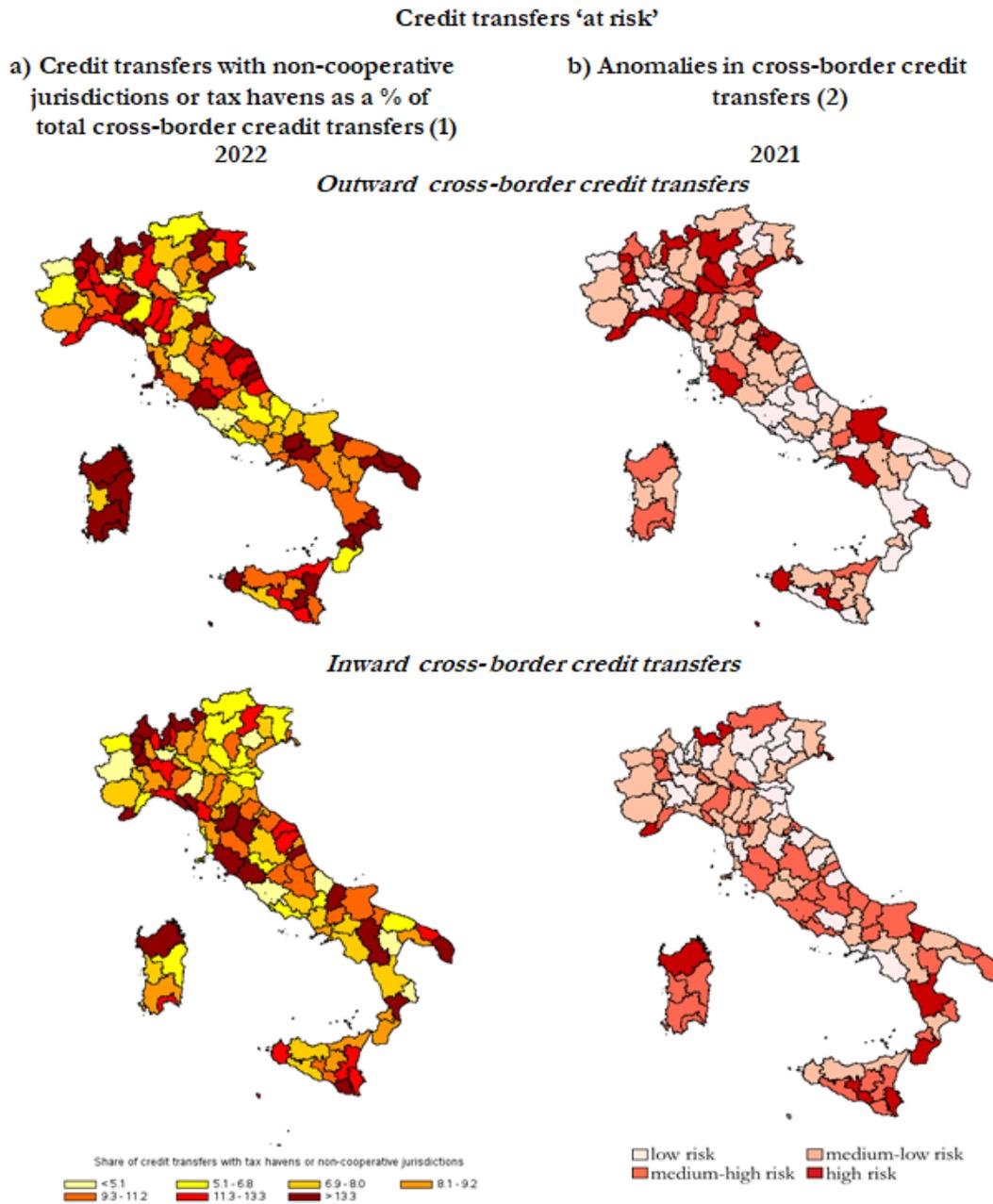
(1) See Figure 5.7, note 2.

However, the incidence of credit transfers ‘at risk’ is not an objective measure of the real importance at territorial level of potentially anomalous flows with the countries in question, given that, as with the use of cash, the financial transactions may have legitimate underlying economic reasons.

Some time ago the Unit developed an econometric analysis for cross-border credit transfers as well. By separating the share of cross-border flows attributable to the economic and financial fundamentals of the Italian provinces and counterparty countries, it enables the Unit to isolate the anomalous component, i.e. the portion not justified by those factors, and accordingly to construct the underlying risk picture associated with the incidence of these flows (Figure 5.9b).

The regions of northern Italy are those with the largest anomalies in outflows, with an especially high concentration in Liguria. The risk associated with inflows is highest in the border provinces (Imperia, Sondrio and Trieste) and in some provinces of the southern regions, above all Calabria, Sardinia and Sicily.

Figure 5.9



(1) See Figure 5.7, note 2. - (2) The maps on anomalies refer to 2021, the latest year for which all the data needed to estimate the model are available.

### 5.3. 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. The requirement applies to transactions in amounts of €12,500 or more for sales or the physical transfer of gold into or out of Italy.<sup>26</sup> In accordance with 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 previous month; and advance declarations, required prior to a physical transfer of gold out of the country.

After diminishing in 2021, gold transactions rose sharply in 2022 (Table 5.4).

Table 5.4

<i>Ex-post</i> monthly declarations of gold transactions			
Type of transaction	Number of declarations	Number of transactions	Declared value (millions of euros)
Sales	50,904	123,753	24,509
Gold loans (concession)	1,306	2,786	1,308
Gold loans (restitution)	314	428	78
Other non-financial transactions	137	143	43
Personal imports of gold	160	247	574
Provision of collateral	3	3	0
Investment gold delivery services	493	504	315
<b>Total</b>	<b>53,317</b>	<b>127,864</b>	<b>26,827</b>

The total value of the declarations rose significantly, as did both the number of declarations and that of the underlying transactions, increasing by 18.9, 30.4 and 23.8 per cent, respectively; meanwhile, the annual increment in the average price of the gold declared was only 13 per cent.

Sales and gold loans, in particular, recorded the largest gains in declared value (19.4 and 24.5 per cent, respectively). The declared value under the heading ‘other non-financial transactions’ grew by €33 million or 330 per cent, owing mainly to the increase in the filing of declarations *mortis causa*.

The last five years have seen a rising trend in prices, quantities declared and declared value (Figure 5.10); in particular, the average gold price declared rose by more than 60 per cent, the value of transactions by about 86 per cent and the quantities declared by about 16 per cent.

The number of reporting parties registered with the system grew further in 2022 with the entry of 20 new professional gold dealers, 80 natural persons and 13 legal persons.

Categories of declarants

<sup>26</sup> Law 7/2000 and subsequent amendments. With the entry into force of Regulation EU/2018/1672, declarations regarding the physical transfer into or out of the European Union of investment gold for amounts of €10,000 or more must be submitted to the Customs and Monopolies Agency.

Figure 5.10

## Quantities exchanged, value of operations and gold price

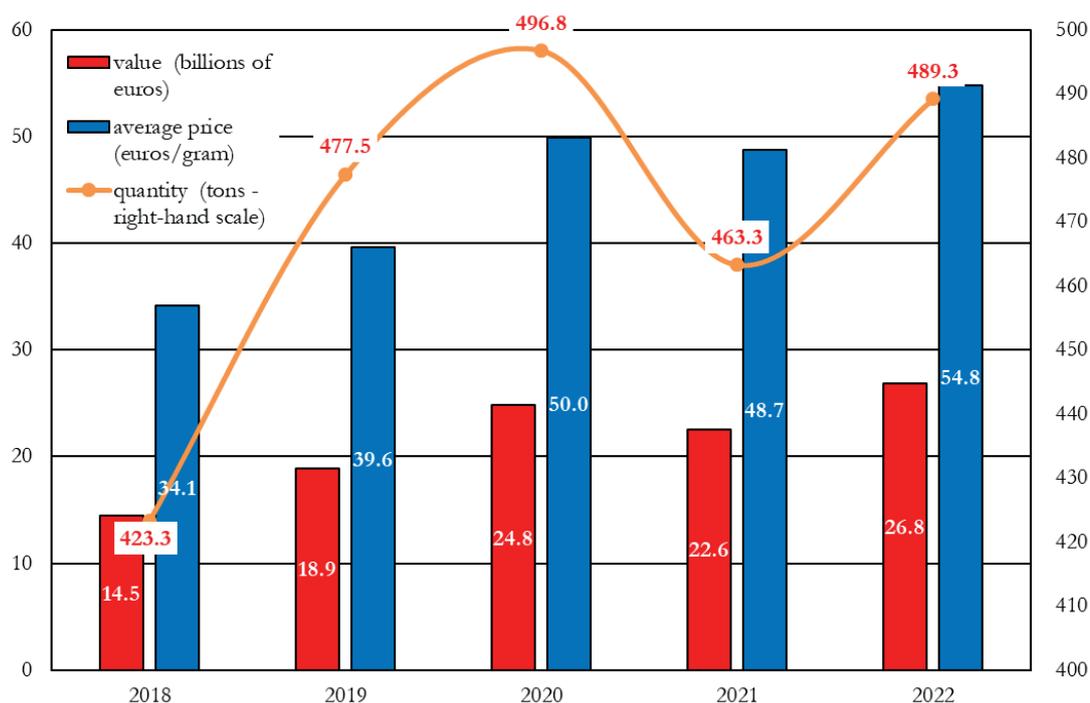


Table 5.5

## Reporting entities engaged in gold transactions

	Number of reporting entities registered	Number of reporting entities active in the year	Number of declarations
Banks	60	26	6,183
Professional gold dealers	502	376	47,646
Other, natural persons	292	64	186
Other, legal persons	129	27	387
<b>Total</b>	<b>983</b>	<b>493</b>	<b>54,402</b>

The number of active reporting entities, that is to say those that actually submitted declarations, rose by 39, or 8.6 per cent; this group comprised just over half of all registered reporting entities, a smaller proportion than in the preceding years. Professional gold dealers continued to account for the majority of the declarations (87.6 per cent), while the share attributable to banks contracted further to 11.4 per cent.

## Assistance to declarants

In order to provide obliged entities assistance on the most frequently asked questions regarding compliance with the declaration requirements established by Law 7/2000, the Unit has developed a set of indications regarding both regulatory and technical-operational aspects.

## FAQs about gold

In April 2022 the UIF published *frequently asked questions (only in Italian)* about gold declarations, which the Bank of Italy has delegated the Unit to receive. The FAQs distill many queries addressed to the Unit about legislative, technical and operational matters relating to gold declarations. They are intended to provide clarification on the questions that most often recur and thus to reduce the number of requests for assistance addressed to the Unit.

More in detail, the main legislative sources governing the matter are cited along with the related implementing provisions, with the specification that for transfers of investment gold into or out of the European Union the provisions of Regulation EU/2018/1672 also apply.

The FAQs on legal aspects (Section A) concern the persons subject to the declaration requirement, the transactions to be declared and the sanctions for violations. The FAQs on technical and operational aspects (Section B) treat issues bearing on the procedure for application and admission to the gold-declarations transmission system, the contents of gold declarations and the procedures for transmitting them to the UIF.

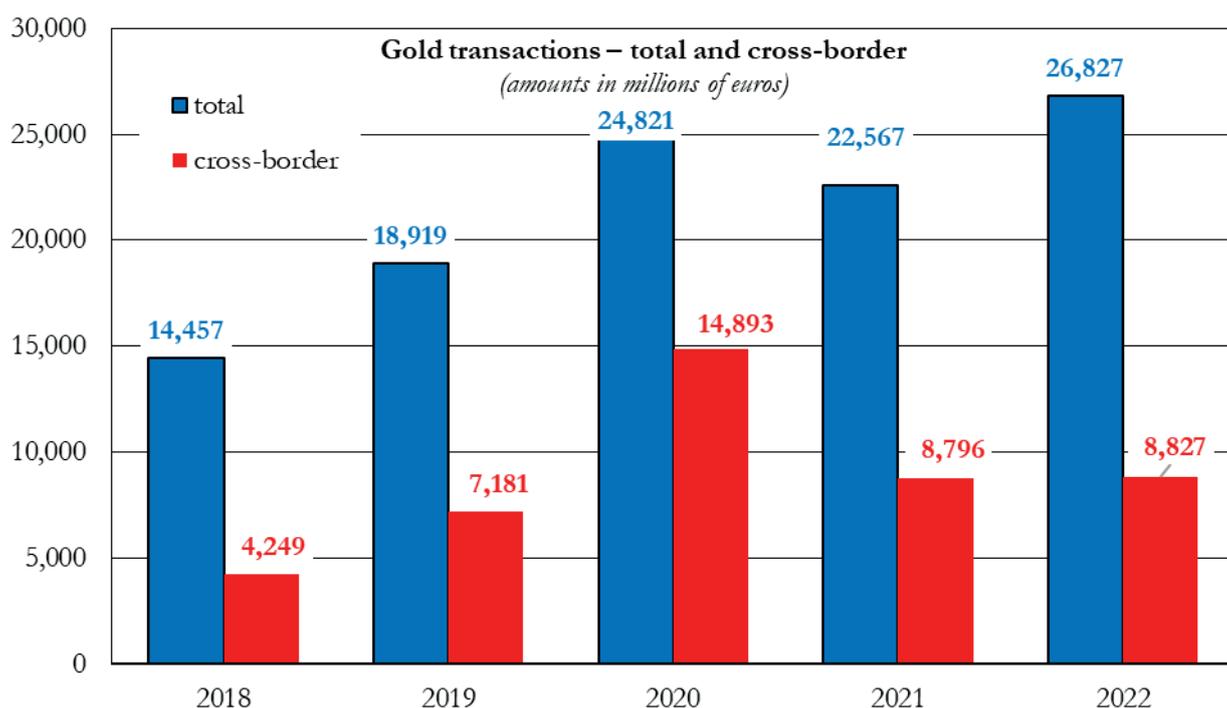
The share of transactions in investment gold continued to rise, from 53.5 per cent in 2021 to 56.3 per cent in 2022, and that of transactions in industrial gold to fall, from 41.1 to 38.1 per cent.<sup>27</sup> The geographical distribution of the Italian counterparties shows that the traditional goldsmithing districts maintained their majority market shares, particularly Arezzo (47.7 per cent) and Vicenza (10.7 per cent).

International transactions were broadly unchanged in absolute terms while diminishing by more than 6 percentage points, from 39 per cent in 2021 to 33 per cent, in 2022, as a proportion of total transactions (Figure 5.11).

Cross-border  
transactions

<sup>27</sup> The residual share consists of cases for which the purpose of the transaction was not specified; it rose slightly, from 5.4 per cent to 5.6 per cent in 2022.

Figure 5.11

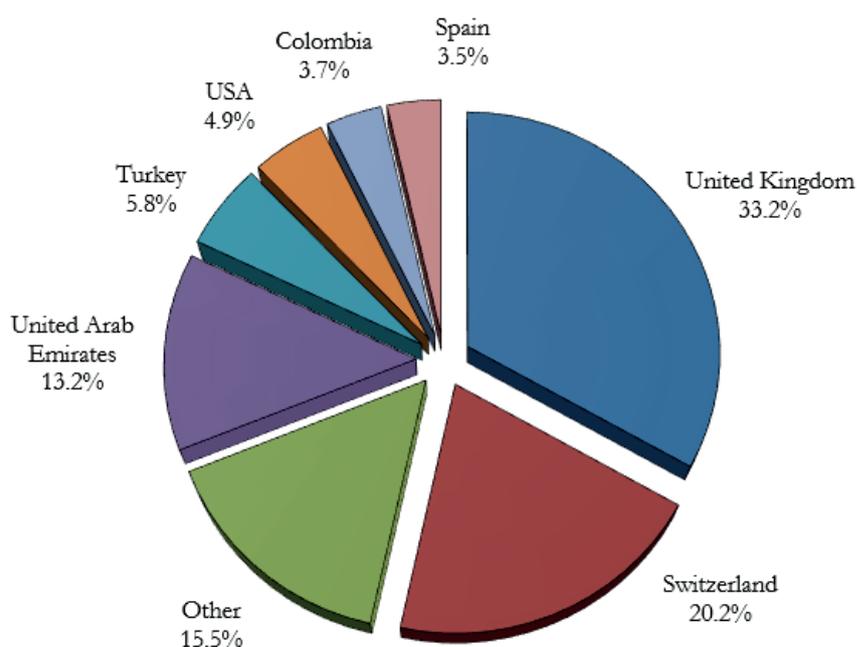


Statistics on advance gold declarations

The distribution of transactions by counterparty country remains highly concentrated: in 2022, 84.5 per cent of the value of cross-border transactions in gold referred to seven countries: the United Kingdom, Switzerland, the United Arab Emirates, Turkey, the United States, Colombia and Spain (Figure 5.12); in 2021, five countries had accounted for a similar share. The shares of the United Arab Emirates and the United States diminished, while those of Turkey and Spain expanded.

Figure 5.12

Gold transactions with foreign counterparties - distribution by country



Analysis of the ORO databank

Between 2021 and 2022 there was a sharp contraction in the value of advance gold declarations (Table 5.6), which fell by €1.16 billion or 54.8 per cent chiefly because of the

decline in the value of sales and of mere transfers, which diminished by €1.1 billion and €9.7 million, respectively.

Table 5.6

<b>Advance declarations (transfers of gold abroad) (1)</b>		
	<b>Number of declarations/ transactions</b>	<b>Declared value (millions of euros)</b>
Sales	1,054	945
No transaction (mere transfer)	27	7
Other non-financial transactions	3	1
Gold loans (restitution)	1	1
<b>Total</b>	<b>1,085</b>	<b>954</b>

(1) Advance declarations are incorporated in *ex-post* declarations if the transfer underlies a commercial or financial transaction.

Like SARA reports, and in accordance with the Unit’s proactive approach to managing the system for collecting gold declarations, the latter are monitored continuously to identify relevant anomalous behaviour, especially connected to significant changes in the amounts declared by Italian operators or in transaction flows with foreign countries. The Unit’s analyses of the significant cases are transmitted to the investigative bodies. An activity of this kind was performed to identify potential gold trades with Russia triangulated with third countries following the imposition of trade sanctions by the European Union as a consequence of the war in Ukraine (see the box ‘Anomalous triangulations with Russia: an analysis on SARA and ORO data’ in the following section).

## 5.4. Strategic analysis

The international standards put strategic analysis among the official duties of the FIUs alongside operational analysis. In accordance with those standards and with national legislation, the Unit is engaged in identifying and assessing phenomena and trends as well as the weaknesses of the system.

Among the purposes of strategic analysis is the evaluation of the risk of involvement in money laundering or terrorist financing of the economic and financial system as a whole or of specific geographical areas, payment instruments and economic sectors, and the identification of situations and contexts for possible targeted studies. The information also helps orient the UIF’s institutional action and planning.

The results of analysis are shared with the other authorities of the AML system according to their respective functions and published in the ‘Analisi e studi’ series of ‘Quaderni dell’antiriciclaggio’ ([only in Italian](#)) and in specialized journals.

The UIF’s main research activities in 2022 regarded the potential use of corporate vehicles for illegal ends, particularly by organized crime. A study was published that provides some empirical evidence of the financial profile of firms infiltrated by organized crime in Italy.<sup>28</sup>

**Use of corporate vehicles for illicit purposes**

<sup>28</sup> M. De Simoni, ‘The financial profile of firms infiltrated by organised crime in Italy’, UIF, *Quaderni dell’antiriciclaggio – Analisi e studi*, 17, 2022.

The study analyses the economic, balance sheet and financial developments of a sample of firms seized from organized crime in order to identify the characteristic features of their management and operations. The different strategies of infiltration were subjected to empirical verification. The results show significant differences not only between the infiltrated firms and those of the control sample – for instance, the former have higher revenues but lower profitability – but also across firms infiltrated for different objectives, both in capital composition and financial management.

Infiltration of firms by organized crime

The findings of the research have been used to develop an experimental algorithm to identify firms at risk of infiltration by organized crime.<sup>29</sup> In 2022 the sample of firms used for training the algorithm was expanded on the basis of additional evidence in the Unit's possession;<sup>30</sup> in addition, feedback from research institutes and the investigative bodies enabled the Unit to refine the methodology. Going forward, the indicator could be employed not only in the sphere of operational analysis but also for the monitoring of firms that use public funds, in order to permit controls to focus on the highest-risk situations. Another potential field of application is that of the control activity performed by the Unit.

Study on corporate opacity

The opacity of firms' ownership or governance structures may be indicative of the use of corporate vehicles for illegal ends. In 2022 the Unit constructed an indicator to measure the level of opacity of corporations and partnerships.

#### An indicator of opacity of Italian firms

The need to ensure greater transparency of corporate vehicles is central to AML action, served in part by the specification of beneficial ownership in the business registries of many countries. The few studies that have examined this topic confirm that opaque firms are more likely to be involved in illegal activities.

Given the importance of the issue, the Unit has developed an indicator that uses data from the InfoCamere archive and is based on three sub-indicators that measure opacity in different dimensions: ownership structures, governance structures and other corporate characteristics. Each sub-indicator is a composite of specific aspects of the corporate structure.

Opacity in ownership structures regards the presence of possible figureheads (very elderly members equity interests in other companies or very young members), high turnover of members, links with countries at risk (tax havens or non-cooperative jurisdictions), the presence as members of particular forms or types of institutions or companies (trust companies, trusts, foundations, informal partnerships), anomalies in the distribution of the equity interests among the holders of the capital. Similar factors are involved in the measure of opacity of the governance structure. They concern the possible presence of figureheads (elderly or very young directors), links between the management and foreign countries at risk, the representation among the directors of institutions or types of companies that are in themselves opaque, high turnover of directors. Lastly, among the other elements of opacity are frequent changes of head office, name, or legal status and the recurrence of addresses to which multiple firms refer.

<sup>29</sup> See UIF, *Annual Report for 2021*, Section 6.2.

<sup>30</sup> The sample of infiltrated firms initially drew on three sources: 1) the list supplied by the Special Operations Group (ROS) of the Carabinieri, based on the firms seized in the framework of the principal anti-mafia investigations in the period 2007-17; 2) the set of confiscated firms from the registry of the National Agency for the Administration and Destination of Assets Seized and Confiscated from Organized Crime (ANBSC); 3) an additional group of firms for which, from consultation of commercial data bases, it was found that at least one partner/director was investigated for organized crime offences. See UIF, *Annual Report for 2020*.

Starting from the sub-indicators, a composite indicator is computed to provide an overall measure of a firm's opacity. The indicator has been calculated for the more than two million Italian firms active from 2010 to 2021 to permit an evaluation of its evolution over time. A rise in the indicator was found in correspondence with the health emergency, due in particular to an increase in the opacity of ownership structures. The correlation with the risk of criminal infiltration shows, moreover, that the appearance of a member or a director linked to organized crime is associated with an increase in a firm's opacity, but that the infiltrated firms are, on average, also more opaque before infiltration. For the firms currently controlled by a politically exposed person (PEP), the indicator is lower than for firms in which the presence of a PEP has never been recorded, but it is higher in those controlled in the past by a PEP who no longer figures among the members or directors. This result might reflect, for example, an expanded presence of corporate vehicles after the departure of the PEP.

The indicator, now undergoing methodological refinement, can have various uses at operational level. The aggregation by geographical area or sector of economic activity can make it possible to calculate risk indicators at regional or sectoral level. The measure of opacity could also be useful for monitoring the use of public funds or the firms participating in public tenders. For the operational analysis of STRs, the indicator can supply additional information for the risk assessment of situations under investigation.

The infiltration of the legal economy by organized crime is the subject of several inquiries that the UIF conducted in past years in collaboration with the academic world and which continued in 2022. A first strand of investigation, developed with Bocconi University, concerns the relationship between financial vulnerability, expressed by firms' credit ratings, and criminal infiltration. A second topic of research, taken up in a collaboration between the UIF and the Einaudi Institute for Economics and Finance, regards the effects of criminal infiltration on firms' economic and financial performance. Finally, the UIF and the University of Padua are conducting a study on the behaviour of SARA flows – at province level, distinguished by type of transaction<sup>31</sup> – during the period of the pandemic, directed at identifying possible anomalies, with a focus on the territories and sectors at highest risk of infiltration.

In order to strengthen the tools for analysis and monitoring of the management of public funds, following a preliminary reconnaissance of the National Data Bank of Public Contracts managed by the National Anti-Corruption Authority and an examination of the relevant literature, the UIF defined a first set of indicators designed to provide a measure of possible anomalies in competitive procurement procedures. The reference dimensions considered are: the type of tender (e.g. the use of discretionary procedures), the award criteria (e.g. the most advantageous bid), the procedures for managing the contract (e.g. the existence of subcontractors) and the characteristics of the awardee firm (e.g. whether it has already done work for the same contracting entity). The indicators were validated using the outcomes of the experimental mapping of firms potentially connected to organized crime<sup>32</sup> in order to check their level of significance and relevance.

In 2022 the Unit effected an application of the model, developed in 2021, for detecting statistical anomalies in SARA financial flows between Italy and specific countries of interest. The application regarded the identification of potential flows with Russia triangulated with third countries in order to circumvent the international sanctions; the main anomalies detected to date are now the subject of specific inquiries, in part in collaboration with the intermediaries.

**Collaborative projects with academia on criminal infiltration**

**Transparency in public procurement**

**Statistical model for detecting anomalies in SARA data**

<sup>31</sup> Transactions in cash, credit transfers with countries at risk, etc.

<sup>32</sup> See the box 'An experimental mapping of the firms potentially connected to organized crime', UIF, *Annual Report for 2020*, p. 46.

The model, appropriately calibrated, has also been used for inspections: the findings are encouraging for the utilization of this approach as an analytical tool in this field, too.

### **Anomalous triangulations with Russia: an analysis on SARA and ORO data**

Following the invasion of Ukraine, Russia was subjected to commercial sanctions that have limited its foreign trade (see Section 8.8, ‘Activity relating to the war in Ukraine’). To circumvent the embargo and buffer its impact on the domestic economy, Russia could resort to trade triangulations by means of complicit intermediaries based in third countries, particularly with those with which it has longstanding economic and political ties. The UIF therefore undertook an analysis to identify possible triangulated financial flows with Russia that may have had Italy as their origin or final destination.

The analysis on SARA data was structured in successive phases. First, Istat foreign trade data were examined to select the countries with anomalous trade dynamics with Italy in 2022.

Second, the financial flows recorded in SARA for these countries were identified by applying a statistical model for anomaly detection.

Third, among the positions identified in the preceding phase, those of greatest interest were selected based on amounts, countries, and sectors of economic activity. The 21 positions so selected refer to flows totalling some €861 million (€609 million of outflows and €252 million of inflows). Some of these positions are now being examined in cooperation with the financial intermediaries involved.

An analogous activity of analysis was developed with reference to the ORO data. To soften the impact of the commercial and financial sanctions and obtain foreign exchange, Russia could have liquidated a part of its gold reserves through triangulation with other countries.<sup>33</sup> Accordingly, the UIF proceeded to analyse the gold trades in the first quarter of 2022 between Italian operators and foreign counterparties based in Russia or in other countries in order to identify anomalous patterns and changes; in particular, the Unit scrutinized the profiles which in the calendar quarter of reference showed sizable increments in the volumes of gold trade with Italy compared with the preceding quarters. The positions of greatest interest were forwarded to the investigative bodies for follow-up. Based in part on the findings obtained, the analysis is being extended to a longer period.

To monitor the cross-border financial flows recorded in the SARA data base, the Unit has created a procedure, implemented half-yearly, aimed at identifying the discontinuities at macroeconomic level in the financial flows between Italy and each counterparty country. The procedure brings out the relevant changes, i.e. variations that are both significant in size and protracted in time. The flows underlying the main discontinuities detected are subjected to specific in-depth examination.

Collaboration was begun with the University of Chicago to develop an econometric model for measuring the effects of banks’ AML safeguards on efficiency of credit disbursement. The project seeks to verify whether the costs associated with having such controls do not only produce benefits in terms of preventing and combating money laundering but also help to make the credit market more efficient.

The updating in 2021 of the econometric model based on bilateral foreign trade statistics,<sup>34</sup> directed at detecting flows attributable to trade-based money laundering, enabled the Unit to initiate a collaboration with the Customs and Monopolies Agency to

<sup>33</sup> The restrictive measures on Russia were extended to the gold trade in July 2022 in accordance with the amendment to Regulation EU/2022/1269.

<sup>34</sup> See UIF, *Annual Report for 2021*, Section 6.2.

achieve operational utilization of the results of the model, starting with the sharing of the anomalies detected.

The activity of the working group formed by the Bank of Italy, the UIF and Istat for the utilization of payment system transactions data to produce official estimates went forward.<sup>35</sup> The use of the data on electronic payment transactions and those drawn from the SARA records has improved the performance of short-term macroeconomic forecasts; in particular, it has facilitated timely tracking of the conditions of economic activity even in the setting of the pandemic.

The studies and research carried out by the UIF were presented at national and international conferences.

**Workshops  
and  
conferences**

The study on the financial profile of firms infiltrated by organized crime was presented at a conference organized by the Central Bank of the Bahamas on the use of empirical approaches in the fight against money laundering and financial crime. The indicator of infiltration based on machine learning techniques was presented at the conference ‘Central bankers go data driven: applications of AI and ML for policy and prudential supervision’ organized by the Netherlands Central Bank. The model for detecting statistical anomalies in SARA data was presented at the Conference of the Italian Statistical Society. The methods developed by the Unit for measuring illicit flows were presented in the webinar ‘New Statistical Horizons: Benefits and Challenges of Measuring Illicit Financial Flows’, organized by the Royal Statistical Society and the UN Office on Drugs and Crime. Lastly, SupTech developments at the Unit were presented at a conference organized by the Bank for International Settlements.

<sup>35</sup> See G. Ardizzi and A. Righi, ‘Uso statistico e previsivo delle transazioni elettroniche di pagamento: la collaborazione Banca d’Italia-Istat’, Banca d’Italia, Mercati, infrastrutture, sistemi di pagamento, 27, 2022.



## 6. CONTROLS

### 6.1. Inspections and document audits

The UIF's contribution to preventing and combating money laundering and the financing of terrorism includes controls on the obliged entities. On-site inspections and document audits 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.

The planning of controls 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 checks are directed at reconstructing specific financial movements, supplementing the information obtained in the analysis of STRs or from foreign FIUs, or at 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 receptiveness to active cooperation, enhance their ability to identify suspicious transactions and improve the quality of their reporting contribution.

In 2022 the UIF performed 12 general and 4 targeted inspections, plus one off-site audit. (Table 6.1). The Unit also wound up 4 inspections that it had begun in 2021.<sup>36</sup>

The controls bore on various types of obliged entity. For the first time there were targeted checks on pledge lending and pawnbroking. In addition, an inspection at a branch of an EU FinTech bank sought to verify compliance with suspicious transaction reporting requirements in a fast-growing sector marked by a high degree of digital innovation.

Table 6.1

Inspections and document audits							
	2018	2019	2020	2021		2022	
<b>Total</b>	<b>20</b>	<b>21</b>	<b>3</b>	<b>10</b>	<b>4<sup>(2)</sup></b>	<b>16</b>	<b>1<sup>(2)</sup></b>
Banks	8	15	2	6	1	5	1
Trust companies	3	1	-	1	-	1	-
PIs, EMIs and other financial intermediaries	2	2	1	1	3	4	-
Asset management companies and securities investment firms	4	-	-	-	-	-	-
Insurance companies	-	-	-	-	-	-	-
Other entities <sup>(1)</sup>	3	3	-	2	-	6	-

<sup>(1)</sup> Comprises professionals, non-financial operators and gaming service providers. - <sup>(2)</sup> Document audits.

<sup>36</sup> UIF, *Annual Report for 2021*, p. 64.

As part of the UIF's regular cooperation with the Bank of Italy's Directorate General for Financial Supervision and Regulation and its branches, in nine cases the Unit's inspection teams were joined by personnel from those structures; likewise, a UIF staff member took part in a broad spectrum inspection at an asset management company carried out by the Directorate General.

Cooperation with the sectoral supervisory authorities took the form of simultaneous checks, each body acting in its own area of competence.

Controls on an auditing firm were carried out simultaneously with a money laundering inspection conducted by CONSOB. The findings of the inspection, which related to shortcomings in customer profiling and in reporting confidentiality safeguards, were then shared for evaluations in the respective areas of competence. In concomitance with inspections conducted by the Bank of Italy's Directorate General for Currency Circulation and Retail Payments, the UIF carried out checks on two cash/valuables-in-transit companies. The controls found shortcomings in data presentation, in particular as regards the value and type of goods transported, with an adverse effect on proper monitoring of this sector with a view to active cooperation.

#### Inspection findings

Controls in the credit recovery sector highlighted a lack of awareness of money laundering risk on the part of corporate bodies, weaknesses in internal rules, the absence of a system for gauging customer risk, and more general shortcomings in due diligence, with adverse effects on the reporting process. The failure of management systems to identify the persons ordering credit transfers and the lack of controls during the check cashing process undermined, among other things, the entities' ability to identify anomalous cases of third-party payers.

Inspections continued at intermediaries involved in the securitization of non-performing loans,<sup>37</sup> confirming the existence of room for improvement in the measures for active cooperation. In one case the resources allocated to the AML function, centralized at group level, were inadequate, to the detriment of the depth of controls. In addition, information procedures were unsystematic, with shortcomings in the presentation of details on credit positions.

In 2022 the Unit conducted a targeted inspection of a company in the pledge lending sector, finding certain weaknesses in the arrangements for active cooperation, and in particular the failure, as part of due diligence, to acquire information on customers' economic activity or on the origin of the goods pledged. With regard to another aspect, the policy of classifying auction winners as occasional customers, even in the case of recurrent operations and persons with continuous relationships, prevented the overall assessment of the business where it is ascribable to a given person. As regards gold pledged, there were shortcomings in the controls designed to prevent errors in expert appraisal, as well as a lack of awareness of the reporting requirements laid down in Law 7/2000.

An inspection at a bank engaged in factoring brought out poor awareness of the laundering risk inherent, in particular, in the acquisition of health and tax credits vis-à-vis general government bodies. The failure to take account of the information available in the bank's multiple, inefficient databases, together with the lack of instruments for the automatic management of the factoring procedure, had an adverse impact on the capability for identifying and promptly assessing suspicious transactions.

<sup>37</sup> See the box 'Inspections in the securitization sector: results and critical issues', *Annual Report for 2021*, p. 64.

Targeted controls at several banks revealed a number of problems with the tools for active cooperation, such as to impede the detection of possible anomalies in customers' cash transactions and in transfers of impaired credits.

The checks were triggered by anomalies in the cash tracing procedure at money transport companies, which was found not to be subject to rules directed to AML action. Further, the detailed data on the highest-denomination notes deposited by customers were not assessed for purposes of active cooperation by the banks involved in the money transport service. In another area, there was a failure to conduct further inquiry, for reporting purposes, of acquisitions of NPLs by entities connected with the holder of the loans, or by the debtor itself.

The inspection of a FinTech firm detected the inefficacy of outsourced controls on the truthfulness of the data and information supplied by customers, resulting in erroneous AML profiles and potential harm to active cooperation. The procedures for analysis of potentially suspicious transactions lacked adequate confidentiality safeguards.

At the end of the year, on the basis of specific inquiries in the virtual asset sector,<sup>38</sup> an inspection was initiated at a virtual asset service provider in coordination with the Organization of Agents and Mediators and the Special Foreign Exchange Unit of the Finance Police. Inspections were also begun on entities active in fiduciary registration, online gaming and betting (the latter in relation to an analysis of the gaming market conducted by the Customs and Monopolies Agency), and real estate leasing, in order to gauge the impact of the financial crisis on compliance with reporting requirements.

In view of a general analysis of threshold-based communications (see the box 'Studies on threshold-based communications,' Section 5.1), an innovative collaborative project was undertaken with a leading bank for joint development of methods for supporting controls on operational units located in areas deemed to be at risk, with a view to fostering active cooperation and strengthening internal compliance.

#### **Virtual IBANs: AML issues**

Controls have revealed that customer payment services increasingly include business models known as 'IBAN as a service'. A significant feature in this field is so-called 'virtual IBANs', which allow rapid activation by a customer of multiple IBANs, so as to facilitate classification and accounting of large numbers of payments, possibly in various currencies (say, by associating a virtual IBAN with financial flows linked to a regular supplier). The flows handled through virtual IBANs are then reconciled on a principal current account held by the customer in order to concentrate liquidity on a single account and thus facilitate its management.

From the AML standpoint, virtual IBANs can render opaque and complicate the identification of the beneficial user of the principal current account, especially when the customer requesting this service is in turn a PI or EMI. In this case, attentive monitoring of the flows via virtual IBANs is required, in order to prevent improper use of the current account by entities not entitled to transact on it (for example, the customers of the PI or EMI) and that may not be known to the bank at which the principal current account is based. The possibility of associating a virtual IBAN with a current account with a different country code or bank code (in Italy, the ABI code) may also be an obstacle to the prevention of money laundering, insofar as this results in geographical and institutional dissociation,

<sup>38</sup> See the box 'Inspections of virtual asset service providers,' *Annual Report for 2020*, p. 66.

undermining correct identification of the obliged entity and the geographical retracing of the financial flows.

The difficulty in identifying the beneficial owner may compromise the capacity of the intermediary generating the virtual IBANs to assess whether the transactions are suspicious or not. Moreover, this geographical and institutional dissociation enormously complicates the FIUs' analysis of STRs with virtual IBANs.

Following inspections, the UIF informed the supervisory and control authorities of the aspects within their respective competence, including the Bank of Italy, its newly formed AML Supervision and Regulation Unit,<sup>39</sup> the CONSOB, the NSPV, the Ministry for Economic Development, and the Antitrust Authority. Information was also exchanged with judicial authorities.

## 6.2. Sanction procedures

Anti-money-laundering legislation envisages a complex system of administrative sanctions to punish violations of the obligations. The UIF, in inspections and off-site analysis, ascertains and notifies violations of the suspicious transaction reporting and communication requirements in its areas of competence; depending on the violation discovered, it transmits to the Ministry of Economy and Finance 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 5.3, 'Gold declarations').

### Information exchanges and coordination with the authorities

The complex structure of sanctioning powers has necessitated increasingly extensive coordination and liaison with the sectoral supervisory and other control authorities, with a view to enhancing the harmonization of sanction approaches and the quality of active cooperation.

With the Directorate General for Financial Supervision and Regulation, there has been a consolidation of the practice of regular mutual participation in the respective collegial bodies responsible for assessing irregularities, along with exchange of information on initiatives undertaken. Since the formation of the AML Supervision and Regulation Unit, these forms of cooperation have been instituted with it as well.

<sup>39</sup> Unità di Supervisione e normativa antiriciclaggio (SNA). As of 27 June 2022 the SNA took over the tasks of supervision of the AML activities of banks and financial intermediaries, previously performed by the Directorate General for Financial Supervision and Regulation.

The technical coordination panel on controls and sanctions instituted by the UIF in 2021 continued its work last year, with the participation of the other authorities involved in the ascertainment of irregularities.<sup>40</sup> The panel examined various issues in the course of the year, such as the use, for active cooperation, of the information deriving from judicial requests or measures relating to customers of obliged entities.

All the authorities agreed that charges of violation of reporting requirements must not be based on subjective irregularities relating exclusively to the reception of information requests by investigative bodies in the absence of objective, operational irregularities. As regards the requests or measures of investigative bodies, it was agreed that after instituting a higher risk profile and consequently applying reinforced due diligence, there should be a reassessment of the entity's business in order to detect possible connections of various kinds with other entities, presumably not known to the investigators, together with more stringent monitoring to discover any major subsequent operational or behavioural changes in the conduct of the account.

### A comparative analysis of failure to submit STRs

Considering the discretionary powers the European rules leave to the Member States in the exercise of sanction powers, in the course of 2022 the UIF carried out a comparative analysis of sanctions for failure to submit suspicious transaction reports. The aim was to compare the criterion governing the ascertainment of violations, the levying of charges, and the imposition of sanctions in Italy and in the other main EU countries (France, Germany, Spain) and the United Kingdom.

The focus was on the legal definition of failure to report and the subjective imputation of the responsibility for omission. In the UK the omission of a report is a penal offence, while the other EU countries envisage administrative sanctions for 'serious' violations of the STR requirement (France and Spain), in keeping with Directive EU/2015/849, which specifies a broad range of sanctions and administrative measures that Member States must envisage 'at least for breaches [of the reporting requirements] that are serious, repeated or systematic.' In Germany, only a simple violation of the requirement, without specifics, is needed, insofar as the seriousness of the breach affects only the amount of the pecuniary sanction. Generally, the degree of lateness in filing the report is relevant to the sanction procedure; in some countries (Germany) incorrectness or incompleteness is also relevant.

As to the definition of the violation consisting in failure to report, the analysis found that for purposes of the existence of the requirement for a report, hence of its omission, no typical constituent elements are envisaged. The legal systems analysed differ depending on whether the suspicion of money laundering on which the report is founded is anchored to the identification of the predicate crime or not. In France, for instance, the obligation arises simply when the conduct of the customer may be related to the commission of a crime of some seriousness, this itself depending on whether the offence is punished by more than one year's detention. In practice, the identification or definition of the predicate crime is not necessary; all that is needed is non-acquisition of information such as to demonstrate the legitimate provenance of the funds potentially involved in the commission of a crime. In Spain, all that is needed is that the suspicious transaction be potentially connected with money laundering or the financing of terrorism, based, among other things, on a clear inconsistency of the transaction with the customer's profile or transaction history. German law allows much less discretion in reaching a judgment of suspicion; it assigns special

<sup>40</sup> See the box 'The technical coordination panel on controls and sanctions,' *Annual Report for 2021*, Section 5.3.

importance to the conformity of the circumstances to the indications provided to reporting institutions by the FIU.

As to legal liability for omission of a report, this is assigned first of all to the obliged party, which may be a legal person (e.g., banking and financial institutions) or a natural person (e.g., a professional). Where the liable party is a legal person, in certain circumstances the natural person who failed to perform the entity's AML/CFT obligations may also be subject to sanction. This may be a director, an employee or any individual acting on behalf of the obliged entity, where direct, personal responsibility is ascertained (in Spain, however, employees below top management are excluded).

The findings of this comparative analysis were shared with the other competent authorities in the technical coordination panel on controls and sanctions, with a view to harmonization of approaches and the development of points to bring up during the negotiations under way on the Commission's proposals to strengthen AML regulations and supervision at EU level.

In the course of 2022, the UIF initiated nine administrative sanction proceedings for failure to report suspicious transactions, as ascertained in inspections (Table 6.2). One proceeding was opened against a credit recovery company for violation of Article 49(1) of Legislative Decree 231/2007. Two proceedings were initiated at the conclusion of off-site controls for violation of the requirement to freeze the funds and assets of designated persons in the framework of the European Union's financial sanctions in relation to the war between Russia and Ukraine. The violations depended mainly on difficulty in identifying the beneficial owner in the case of complex chains of corporate control and on lateness in updating internal lists of designated persons, a task often outsourced to other service providers. The violations notified to the persons concerned were transmitted to the MEF for the possible imposition of sanctions.

Table 6.2

<b>Administrative irregularities</b>					
	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>
Failure to report suspicious transactions	8	18	12	4	9
Failure to submit aggregate data	1	1	1	-	-
Violation of Article 49(1), Leg. Decree 231/2007	-	-	1	-	1
Failure to declare gold transactions	26	28	12	13	11
Failure to freeze funds and assets	-	-	-	-	2

**Sanction proceedings on gold transfers**

In 2022 the Unit sent the MEF documentation bearing on the investigations conducted as part of 11 sanction proceedings regarding gold transfers.

In most cases the charge of violation was notified to companies listed both in the register of professional gold operators and in that of gold buyers in relation to domestic sale or purchase of gold for investment, i.e., either involving industrial gold or investment gold for melting to produce gold relevant to the gold declarations. In four cases the charges involved the physical transfer of investment gold from abroad by individuals. The MEF agreed with the Unit's reading and imposed the consequent pecuniary administrative sanctions.

## 7. COOPERATION WITH OTHER 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.

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 the effort to prevent and combat crime.

### 7.1. Cooperation with the judicial authorities

In 2022, after two years of sharp increase, requests for cooperation from the judicial authorities and investigative bodies fell back to pre-pandemic levels, while the number of STRs submitted remained high. The UIF received 313 requests from the judiciary (a decrease of 38.6 per cent compared with 2021) and sent back 1,059 responses (down 27.6 per cent), including follow-up transmissions (Table 7.1).

Table 7.1

Cooperation with judicial authorities					
	2018	2019	2020	2021	2022
Requests for information from judicial authorities	265	395	558	510	313
Responses to judicial authorities <sup>(1)</sup>	488	779	1,188	1,463	1,059
Number of STRs forwarded	1,697	2,368	2,927	3,420	2,854

<sup>(1)</sup> The number of replies exceeds the number of requests, as it includes all the communications, following the first response sent to the judicial authority, in which, within an appropriate period of time, further relevant information received from the UIF is conveyed and the relevant documentation is forwarded.

For the most part, the requests addressed to the Unit are for acquisition of STRs and the related financial analyses, threshold-based communications, and information from foreign FIUs via the channels of international cooperation. The investigative bodies continued to display significant interest in more sophisticated forms of cooperation, asking the Unit to

assist in their investigations with analyses of financial flows traced to persons of interest in Italy and abroad. In particular, the requests asked the Unit to reconstruct flows in connection with serious crimes, often involving not only money laundering but organized crime, the financing of terrorist cells, or else tax evasion, fraudulent transfers of assets, fictitious ownership of assets, and international drug trafficking.

Cooperation under  
Article 12(8) of Leg.  
Decree 231/2007

Following the introduction of new provisions, under the ‘Support-*ter*’ decree<sup>41</sup> on information exchange in relation to terrorism,<sup>42</sup> the Unit received the initial requests for cooperation from the central police departments for the reconstruction of financial flows in connection with the financing of terrorist cells.

EPPPO

Information exchange with the European Public Prosecutor’s Office (EPPPO) was stepped up, in application of the memorandum of understanding signed in June 2022.<sup>43</sup> A good number of requests were forwarded by the public prosecutors’ offices of Naples, Turin and Venice. The first few months of activity under the memorandum revealed considerable interest in access to the Unit’s information in order to deal with the threat of economic crimes detrimental to the Union’s financial interests. The data produced by the Unit offer an invaluable source of supplemental intelligence and support in analysis of criminal activity within the competence of EPPPO.

Dialogue with  
foreign FIUs

The Unit’s intense dialogue with foreign FIUs continued at the request of the judicial authorities and delegated investigative bodies (see Section 8.1, ‘Exchange of information with foreign FIUs’). Cooperation mainly involved presumed money laundering, tax crimes, fraud, international corruption, unauthorized conduct of financial activity, and drug trafficking. Information exchanges in relation to computer crime were very frequent, especially IT-financial frauds, in whose regard the Unit also received requests to freeze funds transferred abroad.

The requests for foreign information on behalf of the judicial authorities were directed principally to the FIUs of Germany, the United Kingdom, Spain, Lithuania, Poland, Switzerland, Romania, Bulgaria, Hungary and the Netherlands. There were also significant exchanges of information with the FIUs of Portugal, Malta, Belgium, Ireland, Luxembourg, the United Arab Emirates and Slovakia.

Following the amendments to Article 38 of Legislative Decree 231/2007 on the confidentiality of AML information (see Section 9.2.1, ‘Legislative measures’),<sup>44</sup> talks were begun with representatives of the magistracy and the investigative bodies on the proper measures needed to reconcile the protection of confidentiality with the right to defence. Talks are now under way with the Ministry of Justice to assess the possible side-effects of application of the new rules.

### Memorandum of understanding with the DNA

To make their work to prevent and combat criminal activities still more effective, on 30 December 2022 the UIF and the National Anti-Mafia and Anti-Terrorism Directorate

<sup>41</sup> Decree Law 4/2022, Article 28-quinquies (1), converted with amendments into Law 25/2022.

<sup>42</sup> Legislative Decree 231/2007, Article 12(8), as amended by Law 25/2022, Article 28-quinquies, now provides that official secrecy cannot be invoked, even outside criminal proceedings, against the central departments of the Police, the Carabinieri and the Finance Police, in cases of absolutely urgent need for the Unit’s information or financial analyses for purposes of prevention, ascertainment, investigation or prosecution of conduct that may be linked to the crimes against the State envisaged by Articles 270 to 270-septies of the Penal Code.

<sup>43</sup> UIF, *Annual Report for 2021*, p. 84.

<sup>44</sup> Decree Law 228/2021 (converted with amendments into Law 15/2022).

(DNA) signed a new memorandum of understanding, superseding those of May 2018 and March 2021.

The new agreement further refines the mechanisms for sharing relevant information, with a view to enhancing the scope, efficiency and mutual usefulness of the exchanges while complying with the confidentiality safeguards laid down by legislation. More streamlined exchange procedures are provided for, as well as new synergies in institutional cooperation, given the potential utilization of STRs and information from foreign FIUs in carrying out the DNA’s functions of stimulus and coordination and in the framework of penal proceedings.

The effects of the memorandum in practical application will be determined by a special technical agreement. The other forms of cooperation stand confirmed: specifically, the DNA can ask the UIF to carry out analyses and studies on single irregularities, on specific sectors of the economy held to be at risk, on classes of payment instruments, and on specific local economic situations. The memorandum also envisages joint training initiatives, coordination meetings, regular meetings on specific issues, and joint analysis of important cases.

The number of reports pursuant to Article 331 of the Code of Criminal Procedure was again quite high, with 408 forwarded in the framework of technical reports submitted to the investigative bodies.<sup>45</sup> No reports were submitted directly to the judiciary (Table 7.2).

Table 7.2

<b>Reports to judicial authorities</b>					
	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>
Reports pursuant to Article 331 of the Code of Criminal Procedure	87	106	257	508	408
<i>of which:</i> submitted to the judicial authorities	-	2	1	-	-
made in connection with technical reports sent to investigative bodies	87	104	256	508	408
Informative reports for investigative purposes	16	11	11	3	6

The General Command of the Finance Police again made extensive use of the SAFE portal, within the framework of investigations on behalf of the judicial authorities. Prosecutor’s offices, however, continue to have little recourse to it. IT improvements to facilitate entry and utilization are under study.

SAFE

## 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 Financial Security Committee (FSC), instituted at the Ministry and charged

<sup>45</sup> Pursuant to Legislative Decree 231/2007, Article 40(1.d).

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 financial intermediaries, commercial operators and professionals regarding the application of financial sanctions pursuant to European regulations, within the framework of the Commission's numerous instructions for application.

In addition, the UIF monitors the application of measures to freeze 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 funds and assets frozen and facilitates the dissemination of the lists of designated persons. In 2022 the FSC assigned additional responsibilities to the Unit relating to the communication requirements laid down in connection with the sanctions imposed on the Russian Federation.

During the year the UIF again provided continuous support to the FSC through its representatives in the network of experts in weighing 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). The gradual introduction of new financial sanctions against Russia and the increase in the number of designated persons brought a considerable increment in applications and queries submitted to the Committee, requiring the expert network to undertake special inquiries to ensure compliance by the private sector with its obligations in terms of fund and asset freezes and provision of financial services.

Except for the sanctions imposed on the Russian Federation, in 2022 the UIF's checks pursuant to Legislative Decree 109/2007, Article 10, found no accounts or assets to which a freeze was applicable beyond those already detected in years past. The communications received from obliged entities (nine in number, all from banks) consisted solely in updates on accounts already frozen, in whose regard the Unit verified compliance with the conditions laid down for the release of the funds or the crediting of liquidity, the latter also subject to the conditions for release.

The amount of funds and assets frozen increased considerably, owing entirely to the EU sanctions against the Russian Federation (Table 7.3).

**New financial  
sanctions  
against Russia  
and Belarus**

Table 7.3

Measures to freeze funds at 31/12/2022					
	Accounts and transactions frozen	Persons to whom freezes applied	Amounts frozen		
			EUR	USD	CHF
ISIL and Al-Qaeda	21	17	14,742	115	-
Belarus	1	1	1,322	-	-
Iran	17	4	1,086,121	158,453	37,593
Libya	4	3	2,140,204	132,357	-
Syria	29	6	18,154,417	240,825	146,595
Ukraine/Russia	182	80	340,805,238	-	-
DPR of Korea	3	4	8,001	-	-
<b>Total</b>	<b>257</b>	<b>115</b>	<b>362,210,044</b>	<b>531,749</b>	<b>184,189</b>

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.

As part of the sanctions adopted by the European Union following the invasion of Ukraine, the FSC designated the UIF to acquire and gather data on the deposits held by citizens of Russia and Belarus, together with information on the presence of assets and liquidity subject to freezing (see Section 8.8, ‘Actions relating to the conflict in Ukraine’).

### 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 all 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, derogation to official secrecy in the context of such cooperation is provided for only between the MEF, the sectoral supervisory authorities, the UIF, the DIA and the Finance Police.

In 2022 the UIF submitted 25 communications to the supervisory directorates of the Bank of Italy concerning relatively simple possible irregularities.<sup>46</sup>

The Unit forwarded a number of communications to the Bank’s supervisory directorates (see Section 6.1, ‘Inspections and document audits’) concerning, among other matters: possible irregularities in the transfer of offsetting tax credits of an asset management company; possible violations relating to microcredit and conflicts of interest; problems found in some loans secured by pledge of one fifth of salary made by a financial agent. The UIF received from the supervisory departments communications in connection with inspections concerning possible shortcomings in active cooperation on the part of obliged

Exchanges with the Bank of Italy’s supervisory directorates...

<sup>46</sup> On the simplified procedure for information exchange, see UIF, *Annual Report for 2021*, p. 89.

entities (see Section 6.2, ‘Sanction procedures’).

... with  
CONSOB

The UIF transmitted a good number of communications to CONSOB, mostly involving possible fraud against private investors perpetrated via foreign online trading platforms – often engaged in trading of complex financial products and crypto-assets – and unauthorized conduct of financial activity.

... with  
IVASS

The UIF transmitted to IVASS communications on possible irregularities on the part of persons listed in the single register of insurance and reinsurance intermediaries for unauthorized conduct of insurance business or improper use of insurance-related terminology, or for violation of the requirement for separation of funds laid down in Article 117 of the Private Insurance Code.

... with MISE  
and the  
Antitrust  
Authority

The UIF informed the Ministry for Economic Development (MISE, as of 4 November 2022 renamed the ‘Ministry for Enterprises and Made in Italy’) of the findings of inspections at trust companies. It also continued its study on the need to update the AML regulatory framework. The findings of inspections at a bank were shared with the Antitrust Authority, with specific reference to the practice of non-competition agreements with other entities active in the business of acquiring claims in respect of bankruptcy proceedings, with potential market distortions.

Investor Visa  
Committee for  
Italy

As a member of 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 substantial investments or charitable donations in Italy, the UIF contributed to the evaluation of the applications presented during the year.

The Committee received 94 applications in 2022. They concerned investments in firms and innovative start-ups formed and operating in Italy, as well as Italian government securities. The investors came mainly from Russia,<sup>47</sup> the United Kingdom, the United States, the United Arab Emirates, Canada, Singapore, Australia, and Israel. In December, the UIF took part, in its areas of competence and in cooperation with the Finance Police, in filling out the European Commission’s questionnaire on ‘Investor residence schemes.’

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.

Specifically, the UIF transmitted to the Ministry of Justice six opinions pursuant to Article 25-octies(3) of the Legislative Decree, with observations and requests for amendments to adapt the codes to the AML regulations.

Memorandum of  
understanding with  
SACE

On 23 December 2022 the UIF and SACE S.p.A. signed a memorandum of understanding for measures to facilitate SACE’s compliance with the STR requirements pursuant to Legislative Decree 231/2007, Article 10, based, among other things, on a specific list of types of behaviour deemed to be at risk of money laundering. As regards SACE’s activities for the provision of economic support, the memorandum provides that SACE shall transmit to the UIF any and all information serving to detect and examine specific risk factors that may underlie the suspicion of money laundering or terrorist financing. With special reference to transactions involving guarantees backed by public funds, SACE shall

<sup>47</sup> Following the invasion of Ukraine, the Committee faced the issue of handling applications from citizens of Russia and Belarus. Given its technical nature and considering that any decision to suspend the applications of these investors was beyond its powers, the Committee elected to continue processing the applications submitted case by case. For further information on the procedure for issuance of the visa following the Committee’s evaluation, see the guidelines posted on the website of the Ministry for Enterprises and Made in Italy.

communicate to the UIF the list of persons that have applied for economic benefits and shall further inform the Unit, via an ad hoc communication, of any cases of refusal or revocation of the benefits. The agreement calls for the adoption of technical and organizational measures such as to protect the security of the information flow, guaranteeing integrity and confidentiality.

The inter-institutional Anti-corruption Coordinating Committee established at the Ministry of Foreign Affairs, of which the UIF is a permanent member, continued its activity of sharing initiatives and experiences, ensuring consistent Italian action in the international forums for preventing and combating corruption, in particular the G20's Anti-Corruption Working Group.

Anti-corruption  
Coordinating  
Committee

The Indonesian chairmanship of the G20 in 2022 maintained continuity with the actions promoted by Italy during its tenure in 2021, selecting, among the priorities for discussion, the role of the legal professions in combating the laundering of the proceeds of corruption. The UIF made presentations at the sessions devoted to this issue, describing Italy's experience and the requirements on professionals for prevention and cooperation. In 2023 the Indian chairmanship asked Italy to co-chair the Anti-corruption group, in recognition of Italy's leading role in international measures to prevent corruption.

In October 2022 the OECD Working Group on Bribery approved Italy's phase 4 Monitoring Report, assessing Italy's compliance with the OECD Convention on the bribery of foreign public officials. The UIF was part of the Italian delegation, coordinated by the Ministry of Justice, that discussed the Report in plenary session.

OECD Bribery  
Working Group  
evaluation of Italy

The Report acknowledges the progress made recently in strengthening anti-corruption legislation, while nevertheless highlighting problems of some importance, set forth in specific recommendations addressed to Italy, some of which would require modification of the regulatory framework (e.g., more severe sanctions on corporations, lengthening the statute of limitations, strengthening whistleblower protection) as well as greater awareness raising and more training.

As regards the AML apparatus, citing concrete cases the Report recognizes the impetus that STRs and the UIF's financial analysis impart to investigations and proceedings on international corruption. However, the evaluators recommend including explicit reference to foreign bribery in future updates of the national risk assessment and in the UIF's communications, so as to facilitate reporting, plan training activities targeted to that crime, and compile complete statistics on STRs that trigger or support investigations, penal proceedings and convictions for corruption.

In December 2022 the National Anti-Corruption Authority (ANAC) approved the National Anti-Corruption Plan (PNA) for 2022-24. For the first time, the Plan includes strong, explicit references to the AML obligations of general government bodies, to be fulfilled under an integrated approach consistent with the anti-bribery safeguards. The Plan emphasizes that these preventive measures are intended to protect 'public value' (taken in the broadest sense, as improvement in the quality of life and economic, social and environmental welfare of the national community, service users, stakeholders, the addressees of a public policy or service). The measures themselves produce value, with major positive impacts on the nation's social and economic organization.

ANAC

In its presentation at ANAC's public consultation on the Plan, the UIF stressed the need to highlight the STR requirements on general government bodies and the transparency of beneficial ownership of assets and enterprises. In December 2022 the Plan was officially presented at the eighth national Anti-corruption and Transparency Officer Day, entitled 'Valore pubblico, PNRR and PNA, 2022-2024,' in the presence of the Minister for General

Government, the President of ANAC and the President of the National Administration School. The UIF took part in a round table on ‘Public value, instruments and actors. What matters is building a network.’

Work is ongoing to renew the memorandum of understanding between UIF and ANAC for broader and more effective cooperation.

General  
government  
entities

The Unit took part last year in the work of the ‘Network of anti-fraud officers’ within the framework of the NPRR. It helped draft a set of guidelines for controls and accounting of NPRR projects within the competence of central government departments and implementing bodies (*Linee Guida per lo svolgimento delle attività di controllo e rendicontazione degli interventi PNRR di competenza delle Amministrazioni centrali e dei Soggetti attuatori*) annexed to the circular of 11 August 2022 from the NPRR central department (see also Section 9.2.2, ‘Secondary legislation and other measures’). The Unit is cooperating in the drafting of additional indications for the reporting of suspicious transactions and the identification of elements facilitating active cooperation.

The UIF participates actively in projects to prevent corruption and foster a culture of integrity as part of the National Action Plan for open government, coordinated by the public administration department. Together with the National Administration School, the Unit coordinates a working group of several public departments to foster dialogue and the sharing of experiences.

At the same time, the UIF is engaged in dialogue with individual general government bodies, conducting seminars and training sessions to heighten their awareness of their AML obligations. The Unit is also responsible, together with the National Administration School, for the technical side of a course of the School’s on money laundering for general government bodies. The initiative, which has been confirmed for 2023 as well, constitutes an important new opportunity to heighten awareness and diffuse an AML culture throughout the public sector.

## 8. INTERNATIONAL COOPERATION

### 8.1. Exchange of information with foreign FIUs

International cooperation serves to support financial analysis, with requests for information from foreign FIUs where objective or subjective connections with other countries are encountered. Requests for cooperation are intended to probe the connections with suspicious activities, to retrace the origins or utilization of funds transferred from or to other jurisdictions, identify economic assets, verify the ownership structure and beneficial ownership of companies and entities, and learn of checks or investigations under way in other countries. Information exchange with foreign counterparts also enables the UIF to acquire information useful to its cooperation with investigative bodies and judicial authorities.

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 multidisciplinary, for purposes of domestic analysis and for exchange, FIUs must dispose of financial, investigative and administrative information. FIUs must also provide the information requested, exercising the same powers of which they avail themselves for domestic analysis. Information exchanges between FIUs are effected 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 2022 the UIF exchanged information with 120 counterparts worldwide. It submitted 790 requests for information to foreign FIUs, down 5.3 per cent from 834 in 2021. Requests in support of judicial or law enforcement investigations diminished by 8.2 per cent, while those for purposes of internal analysis declined by only 3.0 per cent (Table 8.1).

Table 8.1

Requests sent to foreign FIUs					
	2018	2019	2020	2021	2022
Information required by judicial authorities	367	438	575	364	334
Information required for internal analysis	715	525	475	470	456
<b>Total</b>	<b>1,082</b>	<b>963</b>	<b>1,050</b>	<b>834</b>	<b>790</b>

In 2022, through the Egmont Secure Web and the European FIU.NET network, the UIF received 1,657 requests or spontaneous communications from other FIUs, about 2.4

Requests from  
foreign FIUs

per cent fewer than in 2021 (Table 8.2). The UIF provided 2,358 responses to requests or spontaneous communications.

Table 8.2

<b>Requests/spontaneous communications received and responses provided</b>					
	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>
Egmont network	594	621	695	872	776
<i>Requests/spontaneous communications</i>	<i>577</i>	<i>594</i>	<i>694</i>	<i>872</i>	<i>776</i>
<i>Exchanges on ISIL</i>	<i>17</i>	<i>27</i>	<i>1</i>	<i>0</i>	<i>0</i>
FIU.NET Channel					
<i>Requests/spontaneous communications</i>	<i>602</i>	<i>729</i>	<i>851</i>	<i>825</i>	<i>881</i>
<b>Total</b>	<b>1,196</b>	<b>1,350</b>	<b>1,546</b>	<b>1,697</b>	<b>1,657</b>
<b>Responses provided (1)</b>	<b>1,681</b>	<b>1,862</b>	<b>2,246</b>	<b>2,528</b>	<b>2,358</b>
<b>Communications sent to investigative bodies</b>	<b>3,070</b>	<b>2,533</b>	<b>3,296</b>	<b>3,608</b>	<b>3,800</b>

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

Cooperation with foreign FIUs, especially those in Europe, can rely on the sharing of a broad range of databases and other functions, some of them highly sophisticated.

The UIF makes systematic use of the Ma3tch function provided by FIU.NET for the anonymous matching of entire databases, which is now fully integrated into operational processes and utilized regularly in internal analysis. Mat3ch makes it possible to pick up the recurrence of the same name in links with other countries that would otherwise go undetected and consequently to request cooperation from the countries so identified.

#### Cross-border reports

The number of cross-border reports has continued to surge. In 2022 the UIF received 80,934 reports from 20 European FIUs, an increase of over 200 per cent on the year.

In addition to periodic sharing of the names of persons mentioned in these reports with the investigative bodies, in view of the large and exponentially increasing number of cross-border reports, the UIF identifies those communications whose analysis is high-priority and cases of special importance for financial inquiry and of possible interest to investigative bodies.

### Developments in cross-border reports

Cross-border reports are divided into two sets: cross-border dissemination (XBD), or information flows triggered by the criteria for selection and importance developed by a special working group within the FIUs' Platform; and cross-border reports (XBR), i.e. transactions reported by obliged entities with registered office in a Member State and operating also in other EU countries under the freedom to provide services.

The most serious problems with the incoming reports consist in failure to describe the phenomenon and the actual grounds for suspicion, poor data quality as regards the identity of the subjects of the report and connected persons, and lack of consent to disseminate the data to national investigative bodies. In some cases the data flow stems from

automatic selection, by criteria that are not always consistent with those agreed on at European level and are often insufficiently selective. Further, many reports referring to the same case are 'fragmented' owing to separate, transaction-by-transmission of the data. The persistent differences in format and content, as well as the use by some FIUs of the original language, impede automated processing and the use of text mining to identify the most important cases. The differing approaches taken also entail the reception of flows at different levels of concentration for different FIUs.

The Platform<sup>48</sup> has continued its work to overcome these problems and enhance the efficacy of reporting. The results of a special project initiated in 2022 and now nearing conclusion will serve as the basis for the adoption of application measures by the European Anti-Money Laundering Authority (AMLA). Stricter rules were drafted to harmonize data tracing and improve data quality; and the criteria for selecting the cases to be shared are now being refined to make sure that those selected are truly significant.

Despite the difficulties, in the cases of most fruitful cooperation the content of the communications enabled the UIF to identify relevant types of behavior. Some communications involved persons who had purchased virtual assets followed by practically immediate conversion or withdrawals, often for the entire amount of the purchase. The Unit also detected flows from or to persons with suspected ties to organized crime, drug trafficking, transactions linked to VAT fraud and IT scams. Other patterns observed involved the sale of counterfeit goods through online platforms, operations giving rise to suspicion of intellectual property violations, or presumed online frauds.

During the year the UIF transmitted to the relevant FIUs 6,896 cross-border STRs, about the same as in 2021, extracted thanks to filters allowing the automatic detection of specific types of suspicious transactions. The filters identify reports of medium-to-high risk and amounts above predetermined thresholds. The reports transmitted include a summary, in English, to allow reconstruction of the transactions reported and the connection criteria applied.

In 111 cases, 13 per cent more than in 2021, international cooperation was aimed to enable the competent authorities to recover the assets traceable to possible criminal activity.

In 53 cases, the foreign FIU asked the UIF to freeze illicit proceeds transferred to Italy subsequent to transactions traceable, for the most part, to fraud. The UIF intervened promptly, with the cooperation of the intermediaries, to prevent the dispersion of the funds or to discover how they were used, enabling the foreign authorities to evaluate and initiate the procedures for the recovery or seizure of the funds. In 58 cases, foreign FIUs informed the UIF of the freezing in their countries of accounts or other assets traced to persons with ties to Italy, most often under investigation. In these cases the UIF promptly informed the Italian investigative bodies, liaising with the relevant counterparty in order to prevent the release of the funds. In this way it was possible to identify, freeze, and foster the seizure of assets of persons under investigation that had not been detected in the course of domestic checks.

As in years past, the UIF forwarded information from foreign sources to the competent investigative bodies, after acquiring the consent of the relevant FIU (3,800 communications, compared with 3,608 in 2021). To better understand the operations reported by its foreign

<sup>48</sup> The Platform, established in 2006 and formally recognized by the Fourth AML Directive (Article 51), is the forum where the EU-based FIUs and the Commission discuss the application of European rules, the development of analytical and collaborative tools, and the conduct of joint operations (see Section 8.3, 'The EU FIUs Platform').

counterparts, the Unit also shares with those bodies the information obtained in the course of further examination by the obliged entities. The investigative bodies' transmission to the UIF of the investigative information needed to fulfill its international cooperation obligations is subject to significant limitations and conditions as prescribed by law.<sup>49</sup>

On 23 May of last year the UIF and the Algerian FIU (*Cellule de Traitement du Renseignement Financier*, CTRF) completed an exchange of letters of intent to develop bilateral cooperation and information exchange for the prevention of money laundering and terrorist financing. On 26 May, on the occasion of the state visit to Italy by the President of the Republic of Algeria, the UIF and the CTRF issued a joint statement recalling the importance of reciprocal information to support financial analysis and reaffirmed their commitment to develop their mutual relationship through the sharing of practices and methods.

## 8.2. The state of cooperation between FIUs and the main findings of information exchange

International cooperation still has serious problems to contend with, owing to significant, persistent differences 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, some countries' FIUs still lack sufficient access to major types of information. Some countries, for instance, have no central register of data on bank accounts or on the beneficial ownership of entities and companies. These divergences and the non-transposition of European rules limit the efficacy of the data exchanges. Moreover, exchanges of financial, tax and customs data with the FIUs of some third countries are restricted by secrecy rules or limits on information powers.

These shortcomings notwithstanding, cooperation with foreign FIUs remains an invaluable source of information for the performance of the UIF's institutional functions. Exchanges with counterparts abroad expand the Unit's stock of information and permit the detection of otherwise unknown connections to criminal activity, enabling the Unit to conduct more thorough domestic inquiries and respond to the information requests from investigative bodies and the judiciary.

### Significant phenomena

The Unit has begun reconnaissance on the most significant phenomena to emerge from information exchanges with foreign FIUs and deeper analytical inquiry into the most important cases. The suspicious transactions reported by the counterparts abroad and shared with the Italian Unit mainly relate to the use of foreign accounts for the transfer of funds, often not declared to the tax authorities, via triangulation of financial flows and cash withdrawals. There are a good many cases of companies with opaque ownership or trusts used to assign ownership of accounts or assets for purposes of dissimulation or interposition. An increasing number of cases involve the use of virtual currencies. Instances of fraud and corruption have also emerged, marked by the inward or outward transfer of the proceeds of crime; often, the persons involved are under investigation in Italy.

Information exchanges concerning IT scams continue. There are a variety of schemes, such as love and romance scams, phone scams, CEO and business email compromise fraud, and ransomware. Appropriation of funds by hacking IT systems also continues. Trade-based money laundering schemes have also been reported, mostly cross-

<sup>49</sup> 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.

border schemes, with the involvement of organized crime and the use of sophisticated modes of operation.

Cases of fiscal violations – such as invoicing fraud, intra-EU VAT fraud and tax evasion – and misappropriation of funds are especially common in the communications from foreign FIUs. These operations are often highly complex, frequently involving transactions also intercepted and reported by obliged entities in Italy.

Sixty-three of the communications received in 2022 resulted from the stiffening of EU sanctions imposed following the Russian invasion of Ukraine. The operating schemes consist mostly in: (a) funds transfers between companies, often with opaque structures and ownership; (b) suspicions concerning the origin or destination of the funds; (c) uncertainty about the ownership of properties by persons ‘designated’ by EU regulations; or (d) transfers of corporate equity interests or assets to persons considered to be ‘contiguous’ to listed persons, often immediately following the latter’s designation in EU regulations.

Between April 2020 and February 2023 the UIF received 254 communications from foreign counterparts on suspicious transactions referring to the COVID-19 emergency. While in some cases the communications were not directly related to the pandemic, the Unit’s investigations nevertheless detected significant connections with the health emergency. Many of the foreign FIUs’ requests and communications related to online payments that might relate to sales of child pornography and the sexual exploitation of minors (145 in 2022 against 112 in 2021, an increase of 29 per cent).

### **8.3. The EU FIUs Platform**

The FIUs Platform proceeded with its work on implementing the new European rules and developing good practices of coordination. Close attention continues to be paid to developments in the legislative proposals contained in the Commission’s AML Package (see Section 9.1.1, ‘European regulatory developments’). During the transition towards the constitution of the European Anti-Money Laundering Authority (AMLA), the Platform has an essential role to play, in particular with a view to greater involvement of the various FIUs in working groups and decision-making.

The UIF coordinated two working groups: on the configuration of uniform formats and contents of STRs and on the standardization and facilitation of cross-border exchanges, to ‘lay the groundwork’ for the development of the competences to be assigned to the AMLA’s mechanism of support and coordination. The Unit also takes part in the project to develop criteria and contents for the exchange of cross-border STRs.

Detailed templates were finalized for information requests, spontaneous communications, responses to information requests, and feedback, according to standardized models. Discussion continued on the definition of an acceptable degree of harmonization of the information content of STRs, with sufficient adaptability to differing national contexts and the diverse range of obliged persons. As to cross-border reports, the group specified additional fields of information to be included in the format in order to enhance the quality of the information and enable the receiving FIU to better set priorities and determine the possible criminal activity reported.

The Platform also discussed the remaining impediments to the FIUs’ cooperation with the European Central Bank as supranational supervisory authority, as envisaged by the Fifth Capital Requirements Directive (CRD V) and the EBA’s related guidelines. In 2022 further

study was undertaken on the Commission's proposed Artificial Intelligence Act,<sup>50</sup> to clarify the rules governing exclusion of FIUs from the scope of the provisions relating to law enforcement forces.

Within the framework of the Platform, the FIUs shared their experiences with application of the EU sanctions imposed in response to the Russian invasion of Ukraine in their areas of competence. Planning also proceeded for additional exercises of joint analysis, after the completion of a number of projects in recent years. Through the Platform the FIUs also took part in reconnaissance and analysis of cross-border risks, which the Commission used in the periodical Supranational Risk Assessment, an update of which was released in 2022 (see Section 9.1.2, 'Further European and international initiatives'). The FIUs also took part in the assessments directed to identifying third countries giving rise to significant risks of money laundering or terrorist financing for the EU, included in the European list.

#### 8.4. Developments in the FIU.NET

FIU.NET is the digital network for cooperation and information exchange among European Union FIUs for AML financial analysis.<sup>51</sup>

The application allows transmission of information to and from European counterpart FIUs and utilization of the matching system. Thanks to common criteria laid down by the FIUs Platform and extensive data sharing, matching detects otherwise unobservable connections with foreign countries.

The AML Package<sup>52</sup> envisages that the network will be managed by the nascent European Support and Cooperation Mechanism among FIUs under the AMLA, which is also to provide functions to enhance effective exchange among FIUs and serve the needs of joint analysis. With this in view, the Commission, as service provider, has taken a series of actions to improve the stability and increase the speed of FIU.NET and to strengthen safeguards for security and business continuity.

The Commission is engaged in active design and planning of a new FIU.NET through a defined process in the governance framework provided for by the service level agreement between the FIUs and the Commission. The procedure capitalizes on the involvement of the FIUs in setting strategic priorities, via the Platform, and in managing the network, via the Advisory Group composed of representatives of the European FIUs, including Italy's UIF, and operating on a mandate from the Platform. Further study is under way to determine appropriate ways to guarantee the integration of FIU.NET with the FIUs' internal databases, for more effective management of the information exchanged thanks to elimination of every residual phase of manual processing.

<sup>50</sup> The Commission's proposed Regulation, presented on 21 April 2021, envisages harmonized rules for the use of artificial intelligence within the territory of the European Union, complying with the principle of technological neutrality and safeguarding the rights of individuals and enterprises.

<sup>51</sup> 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). Since 16 September 2021 the Commission has been the infrastructure's service provider, supplanting Europol, which had taken over its management in 2016 (see UIF, *Annual Report for 2021*, p.99).

<sup>52</sup> Article 23 of the proposed sixth AML directive and Article 37 of the proposed AMLA regulation.

## 8.5. Relations with foreign counterparts and technical assistance

In 2022 the UIF took part in an initiative on behalf of the authorities of the Republic of Bosnia and Herzegovina within the EU Technical Assistance and Information Exchange programme (TAIEX) for third countries.

The initiative, addressed principally to representatives of the local Finance Ministry, centred on the configuration and application of the AML safeguards vis-à-vis crypto-assets envisaged by the Fifth AML Directive. In particular, the UIF's intervention concerned the emerging risks on these instruments as drawn from its own operational experience and studies carried out in international forums.

The Unit took part in meetings with Vietnamese authorities, including representatives of the FIU, as part of cooperation by the Bank of Italy with other central banks to strengthen banking regulation. The UIF reported on the features and main areas of its activity within the AML/CFT system. Joint initiatives were also held with the Vatican FIU, sharing the Unit's operational experiences in financial analysis and cooperation.

The Unit's work of support and technical assistance within the Egmont Group continued, in particular in the Training and Technical Assistance Working Group, the Membership, Support and Compliance Working Group, and the ECOFEL training centre.

These are initiatives of assistance to FIUs in their formation or consolidation phase, as well as development and implementation of training and specialization programmes to reinforce institutional activity. Some assistance plans are also addressed to overcoming problems in compliance with international standards and shortcomings in the efficacy of checking procedures.

Technical assistance to the *Zambian* FIU on trade-based money laundering proceeded. The Unit provided operational support in the implementation of the methodology used to study anomalous financial flows in connection with foreign trade.<sup>53</sup> The encouraging preliminary results achieved by the *Zambian* FIU suggest that the model developed for Italy may well be suitable for other countries as well.<sup>54</sup> The UIF is also part of a training project launched by the Egmont Group together with the World Customs Organization to develop synergies in analysis; in particular the Unit intervened on the issues of trade-based terrorist financing and money laundering, as well as certain other aspects of operational analysis. Lastly, the Unit is part of the programme of technical assistance to *Moldova*, coordinated by the IMF and intended to equip the local authorities with the competence to apply quantitative assessment methodology to the risks deriving from cross-border payments.

## 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.

<sup>53</sup> See M. Gara, M. Giammatteo and E. Tosti, 'Magic mirror in my hand ... How trade mirror statistics can help us detect illegal financial flows', *The World Economy*, 42 (11), pp. 3120-3147, 2019.

<sup>54</sup> The model is based on analysis of open source data from Comtrade, World Bank, and OECD.

In 2022 the Unit again participated constantly in the FATF's working groups and plenary session as part of the Italian delegation coordinated by the Ministry of Economy and Finance.

#### Mutual evaluation

The Unit contributes regularly to the various phases of mutual evaluation of the member countries, to check compliance with the FATF's Recommendations on certain aspects of legal transposition and the effectiveness of national AML systems. The fourth round of evaluations is running slightly behind schedule owing to the legacy of the pandemic. In 2022 the evaluations of France and the Netherlands were concluded, with the participation of UIF staff as, respectively, assessors and reviewers. During the year the FATF completed the strategic revision to ensure more timely and efficacious evaluations in the future and approved the methodology for the fifth round of mutual evaluations starting in 2024.

The evaluation of Italy will begin in 2024, and the report is scheduled for discussion in February 2026. Given the delay in the talks on the AML Package, the evaluation should not take account of the changes to the rules and supervisory mechanisms envisaged by the Package and so will be performed on a set of safeguards and measures that are being superseded.

In keeping with the strategic priorities set forth in the ministerial Declaration of 22 April 2022, the FATF has initiated a review of the Recommendations on asset confiscation and provisional measures and on international judicial assistance to enhance the effectiveness of the overall machinery of asset recovery.

#### The role of FIUs in asset recovery

Effective AML systems cannot do without a set of powers and instruments for the prompt identification, freeze and seizure of the assets held by criminal organizations. The effective recovery of these illicit proceeds serves as a deterrent to criminal activity and allows the return of the assets.

The widespread shortcomings uncovered in the course of mutual evaluations have led the FATF to undertake a series of initiatives to survey the operational obstacles in this area and strengthen cooperation among the competent authorities, with a view among other things to revision of the standards in order to design more incisive tools for asset recovery and combat cross-border crime more effectively. In this context FIUs have a key role to play, both as regards asset tracing and the securing of assets through their power to suspend suspicious transactions with a view to subsequent seizure and confiscation. Mechanisms for the suspension of suspicious transactions are recognized in various international agreements and regional provisions, such as the Warsaw Convention of 2005<sup>55</sup> and EU directives, but they suffer from the lack of uniform, global provisions. In fact, this power is not envisaged in the FATF Recommendations, not even with reference to FIUs. Explicit recognition by the FATF standards, now under consideration, would help foster a tendency towards greater uniformity of powers among authorities in different jurisdictions, with a clear gain in the speed of identification and seizure of criminal assets, including in cross-border situations. However, in keeping with the solutions envisaged by the European directives, the power of suspension should be assigned exclusively to FIUs, given their functions of reception, analysis and dissemination of STRs under the FATF's own standards; and its exercise should also be triggered at the request of investigative and judicial bodies and foreign FIUs.

<sup>55</sup> 'Council of Europe Convention on laundering, search, seizure and confiscation of the proceeds from crime and the financing of terrorism'.

The FIUs' recognized position within the AML system facilitates interaction with obliged entities, prompt collection of the information necessary for assessment and decision, even in the absence of a prior report, and rapid communication with investigative and judicial authorities, as well as the availability of rapid, secure and informal international channels for information exchange. In the context of international cooperation, exercise of the power of suspension by FIUs on input from foreign counterparts has proven to be a highly effective tool for the temporary segregation of illicit assets, pending initiatives of judicial assistance, as observed in the recent report of the Egmont Group.<sup>56</sup>

The need for stronger rules on asset recovery and confiscation, albeit in diverse contexts, has also emerged in a European framework, with the Commission's proposal for a directive to strengthen the powers of the competent authorities to identify, freeze and manage the assets subject to sanctions and to extend and enhance the efficacy of the rules for confiscation of illegal assets (see Section 9.1.1, 'European regulatory developments').

The revision of the standards on the transparency of beneficial ownership of corporate vehicles and trusts was completed. The aim is to strengthen safeguards and ensure prompt access to information on the part of FIUs and other authorities.

Transparency of  
beneficial  
ownership

The new standards introduce an approach based on differential modes of access by the authorities to information on beneficial ownership: countries may institute central registers (as provided for by the European AML directives) or adopt alternative means of information acquisition, as long as they ensure equivalent degrees of promptness, efficacy and completeness. The guidelines lay down detailed indications on the criteria for determining the beneficial ownership of corporate vehicles, the characteristics of the registers and alternative mechanisms, and on the requirements of adequacy, accuracy and promptness. The development of further guidelines for application of the standards on trusts and similar legal arrangements has begun.

The FATF continued analysis of the laundering risks inherent in virtual assets. The UIF is member of a special contact group to monitor emerging trends, among other things through dialogue with the private sector, and check for uniform implementation of the standards.

Virtual assets

The findings were brought together in a targeted [update](#) released in June 2022, highlighting the risks in connection with decentralized finance (DeFi) and non-fungible tokens (NFTs), as well as the burgeoning phenomenon of ransomware in connection with crypto-currencies. The update notes persistent unevenness in the implementation of the relevant Recommendations by member states, especially as regards the rules requiring systematic indication of the originator and the beneficiary of crypto-asset transfers (the 'travel rule'). Accordingly, special corrective measures are provided for (see the box 'International and Italian initiatives concerning virtual assets' in Chapter 9).

In 2022 the FATF released its updated [guidelines](#) for the real estate sector, with the aim of improving compliance. Special attention was paid to the revision of safeguards against the exploitation of non-profit organizations for the financing of terrorism. The purpose of the update is to mitigate the potentially undesirable consequences of unduly strict application of the standards to legitimate non-profit organizations.

The UIF made multiple contributions to the FATF's studies on typologies of money laundering and terrorist financing. The project for the identification of the most common methods of transferring and laundering the proceeds of migrant trafficking was completed ('[Money laundering and terrorist financing risks arising from migrant smuggling](#)'). The UIF

Migrant  
smuggling

<sup>56</sup> Egmont Group, 'Asset recovery – The role of FIUs', 2022.

reported case studies from its own operational experience, identified in implementation of the profiling of the financial behaviour of migrant smugglers that it had developed in 2016.

Another project in which the UIF was involved sought to deepen understanding of the risk of terrorist financing associated with various money or value transfer services. A report on MVTS,<sup>57</sup> Hawala and cross-border cash flows for terrorist financing was drafted in a workshop during the periodic sessions of the Joint Experts' Meeting organized by the FATF together with the United Nations Office on Drugs and Crime.

The UIF also took part in the study on types of illegal trade in goods of historical and artistic value ('Art, antiquities and cultural goods as a tool for money laundering and terrorist financing'), intended to develop risk indicators and possible best practices.

#### Ransomware schemes

The FATF project to typify cases relating to ransomware schemes and the laundering of the proceeds was concluded last year. The final report notes the increasing diffusion of ransomware attacks against governmental agencies and private corporations and highlights their frequent recourse to virtual currencies for the ransom payment, thanks to the inherent features of those instruments, which are harder to trace than the conventional means of payment. The UIF contributed to the project with a case study on instances of ransomware identified within a broader criminal framework with the involvement of members of organized crime.

The Unit is also following three projects: on crowdfunding for the financing of terrorism; on combating the financing of IT crimes; and on illegitimate granting of citizenship or residence permits in exchange for investment programmes.

### 8.7. Participation in other international organizations

#### The Egmont Group

The UIF is a member of the Egmont Group, the worldwide organization of FIUs that serves to strengthen their overall capacity for analysis and cooperation.

In 2022 the Group adopted a five-year strategic plan, specifying four thematic areas of action: i) enhancing the framework for effective information exchange between FIUs; ii) strengthening cooperation with international partner organizations; iii) developing and promoting knowledge on new or emerging methods and trends in money laundering and terrorist financing; and iv) enhancing support to Group members and candidate FIUs.

In the course of the year the UIF offered technical observations as part of the multiple procedures of support and compliance in relation to specific requests from member FIUs. In particular, these procedures consist in verifying the independence and confidentiality of the FIUs' activities and detecting possible shortcomings in analysis and information exchange. Following the checks, specific plans of action to correct the defects are drawn up. The UIF was also engaged in the Group's collateral activity of updating methods and the conditions for activating the procedures, with special reference to those initiated following negative assessments in the mutual evaluations of the FATF or regional bodies on matters relating to the FIUs' activities or competences.

The main purpose of the revision is to avoid the duplication of analogous procedures in the successive phases of mutual evaluations and focus the Egmont Group's interventions on appropriate actions to support FIUs in international cooperation and the use of financial

<sup>57</sup> For the definition of money or value transfer services, see the glossary annexed to the FATF Recommendations, p. 131.

intelligence. In particular, the UIF is following the work of the Review Table, assigned to supply support and guidelines and review the entire work of the Drafting Table, responsible for the material drafting of the documents.

As always, there was also attention to the Group's work on the sharing of experiences in analysis, on the identification of emerging phenomena and typologies, on the development of best practices and indicators, and on strengthening the FIUs' IT capabilities.

Ad hoc sub-groups are engaged in multiple studies. There is a project on trade-based money laundering and the misuse of corporate structures, as well as a new project on the risks in connection with the circumvention of international financial sanctions. A specific focus on terrorist financing marks the work on the use of crypto-assets, the distorted use of non-profit organizations, and subsidies to extreme rightwing organizations. There are also broader projects: on the use of open source intelligence (OSINT) in FIUs' analysis, now in its conclusive phase; and on cyber-enabled fraud. In order to share with the other FIUs the results of the study on cross-border laundering schemes, the UIF took part in the '2022 Best Egmont Case Award', presenting the analyses conducted on frauds by means of transfers of tax credits, the funds being frequently moved abroad. The UIF's presentation took second place in the Award competition.

The second phase of the project on technological development of the Egmont Secure Web, the platform for information exchange between the Group FIUs, is now under way. The work here focuses on the detailed definition of functions and the implementation and testing of the new IT system; in addition to the usual means of bilateral communication, the new system will make available more sophisticated forms of interaction (for instance, shared analytical activity and multilateral exchanges). Detailed specifications for security and inaccessibility on the part of the system manager are envisaged in order to guarantee the confidentiality of the information exchanged. The UIF is a member of the team assigned to develop the IT solutions, including confidentiality safeguards, and of that for the definition of policy issues.

As a member of the Italian delegation, the UIF participates in the activities of Moneyval, which is the Council of Europe's anti-money-laundering organization and part of the FATF's global network. The UIF's contribution relates in particular to specific evaluation procedures.

**Moneyval**

In 2022 the evaluation of the Principality of Monaco was concluded; this is of special interest to the UIF given its geographical proximity to Italy and the exposure of its financial market to the risk of laundering of proceeds from abroad, especially in the real estate and financial sectors. Widespread shortcomings in compliance with the standards and in the effectiveness of the AML system were found, with reference among other things to the development of financial intelligence and cooperation, and the Principality was accordingly placed under increased monitoring.

Moneyval also surveyed its member countries' effectiveness by comparison with those evaluated by the FATF and by other regional organizations. The members were found to have performed better than the countries belonging to other organizations. There remain disparities with the FATF countries in a number of areas (national risk assessment, use and development of financial intelligence, confiscation, implementation of sanctions), in whose regard no Moneyval member achieved a rating of full or substantial effectiveness.

A UIF expert provides support to the activity of the Conference of the Parties to the Council of Europe's 2005 Warsaw Convention on money laundering and terrorist financing.

**Conference of the Parties**

The Conference is charged with monitoring, transposition and implementation of the Convention by the signatory countries. To this end it uses the Mutual Evaluation reports of the FATF and Moneyval and also conducts verifications of its own on the relevant national

AML systems, producing special evaluation reports. In 2022 the Conference examined the transposition of the Convention provisions, which require member states to institute effective systems for the management and conservation of assets seized or confiscated. The Italian AML system received a positive evaluation: the regulatory apparatus is in line with the Convention and with the corresponding FATF standards; the information provided on the diversified management of movable and immovable assets and of corporations, and the use of databases in support of monitoring resulted in a positive judgment in terms of effectiveness as well.

Finally, the Unit participated in the initiative on ‘Comparative solutions and good practices for FIU strategic and operational analysis’, promoted by the Council of Europe to foster dialogue among FIUs on these matters. The UIF’s interventions concerned: strategic analysis of withdrawals using foreign payment cards; indicators of mafia infiltration of firms and techniques of machine learning; and analysis of crypto-asset STRs.

## 8.8 Activities relating to the war in Ukraine

**FATF** The military aggression against Ukraine beginning in February 2022 led a number of European and international organizations to take actions against Russia with a view to reducing its role and influence within the AML community. In March the FATF issued a public statement stressing how the actions of the Russian Federation clashed with the organization’s core principles of cooperation, dialogue and mutual respect, and announced that it was considering appropriate measures against Russia in the event of the persistence of hostilities.

The statement further urged that member countries strictly monitor the risks stemming from circumvention of the international financial sanctions against Russia and the further risks in connection with the conflict and that they facilitate detection and mitigation of these risks by the private sector. Specifically, the statement observed that malicious cyberattacks against financial institutions and systems could jeopardize the ability of the private sector and competent authorities to implement and monitor core AML/CFT controls.

In a joint statement in April 2022 the ministers of the FATF member countries reiterated their appeal to all jurisdictions for vigilance on the threats to the integrity and security of the international financial system that derive from the actions of the Russian Federation. From June on, Russia was barred from any leadership role in the FATF groups and from taking part in decisions on policy and standards or the governance of the Task Force. Russian experts were excluded from the Mutual Evaluation proceedings; further actions taken in October 2022 banned Russians from participation in certain project teams and the meetings of regional organizations.

With the military conflict continuing, in February 2023 the FATF suspended Russia’s membership, thus excluding it from all the rights to which members are entitled, without prejudice to the obligations of compliance with the standards or to Russia’s financial obligations to the FATF. Every plenary session of the Task Force will determine whether to revoke or modify these restrictions. In any case the Russian Federation remains part of the FATF’s global network as member of the Eurasian regional group (EAG) to combat money laundering, within which Russia retains its rights.

**Egmont Group** In December 2022 the summit of Egmont Group FIU heads ordered multiple restrictions on the Russian FIU (Rosfinmonitoring), subsequent to a series of complicated meetings between members of the Group.

The Russian FIU was barred from access to leading roles and representation of the Group, and the payment of contributions and subsidies was suspended. Its participation in the activity of the Group is permitted only in virtual form, where possible. For the moment, its voting rights and connection to the Egmont Secure Web for information exchange are maintained. The statement of the Egmont Group Chair noted that the military aggression against Ukraine compromises the foundations of mutual trust among members and negatively affects the success of joint AML/CFT efforts. In the firm belief that this situation has undermined the essential conditions at the basis of international cooperation, the European Union's FIUs, including the UIF, have voluntarily ceased cooperation with Rosfinmonitoring.

As of 17 March 2022 the Russian Federation was excluded from the Council of Europe, and consequently from Moneyval,<sup>58</sup> to which it had belonged since 1997. Accordingly Russia could no longer take part in Moneyval activities and evaluations.

Moneyval

Since February 2022 the European Union has significantly tightened the existing sanctions against Russia and Belarus with a rapid succession of 'packages' of restrictive measures. The number of persons to whom asset freezes apply has been progressively increased, and specific bans have been introduced both on exports of goods and services and on the provision of the related financial assistance. Such additional measures include the ban on accepting deposits larger than €100,000, except for certain specific, mandatory cases subject to prior authorization, and a ban on transfers or exports of euro-denominated banknotes. The UIF called obliged entities' attention to the new restrictive measures in special, constantly updated alerts,<sup>59</sup> consisting both in the additions to the list of persons subject to freezes and in announcements of new communication obligations for obliged entities. Moreover, on the basis of the data available, the Unit initiated monitoring of Italian intermediaries so as to determine the amount of funds available to the newly listed persons, also through domestic and foreign companies and vehicles, via targeted contacts with the intermediaries where there are financial accounts traceable to designated persons. The findings of these checks were promptly shared with the Financial Security Committee (FSC) to enable it to take the measures within its powers to identify the resources to be frozen.

European Union

As of 31 December 2022, 182 financial accounts and transactions in the name of 80 persons were frozen, over half of them formally held by companies and entities not explicitly on the EU lists but owned or controlled indirectly by designated persons. The total amount of funds frozen exceeds €340 million, of which €120 million in current account deposits and the rest in letters of credit and loans to commercial enterprises. The total value of the assets frozen, which consist chiefly in real estate, boats and motor vehicles, is estimated at €2.3 billion.

In addition to the communications envisaged by Legislative Decree 109/2007 on freezes of funds and economic resources by obliged entities, the competences of the UIF have been extended by new functions expressly delegated to the Unit by the FSC. By a measure of 16 March 2022 the FSC delegated the UIF to receive and collect data on deposits larger than €100,000 held by citizens of Russia and Belarus or natural persons resident in those countries and by legal persons, entities or organizations resident there ('Type A' communication) or by persons having acquired citizenship or residence in an EU Member State thanks to a programme of citizenship or residence for investors ('Type B'

<sup>58</sup> The expulsion was decided by the Committee of Ministers, pursuant to Article 8 of the Statute of the Council of Europe, at an extraordinary session.

<sup>59</sup> See UIF, *Annual Report for 2021*, p. 87.

communication).<sup>60</sup> And for Russian deposits only, Regulation EU/2022/2474 of 16 December 2022 adds the obligation to report deposits of over €100,000 held by legal persons, entities or organizations established outside the Union more than 50 per cent of whose ownership rights are held directly or indirectly by Russian citizens or natural persons resident in Russia ('Type A-bis' communication).

Lastly, Council Regulation EU/2022/1273 of 21 July 2022 introduced new requirements for verification and communication of the existence of goods and economic resources subject to freezes, in addition to those already provided for by national law. The new obligations require that all natural and legal persons, entities and organizations immediately inform the competent authority of the Member State in which they reside or are located of any information such as to facilitate compliance with the regulation (such as information about accounts and funds frozen or funds and economic resources belonging to or owned or held by designated persons). They further impose on the designated parties themselves an analogous requirement of communication, within six weeks of the date of their inclusion in the EU list. For these communications too, the FSC has delegated the UIF to receive and collect the information as well as to determine the content, format and mode of transmissions, which were specified in a Communication of 18 August 2022. The UIF makes the information on economic resources available to the Special Foreign Exchange Unit of the Finance Police (NSPV) with a view to the checks on the freezing of assets assigned to that body.

**Russia-related  
sanctions and  
illicit finance**

The UIF takes part in the ongoing work of the Russia-Related Illicit Sanctions and Finance group (RRIFS) for the development of synergies among FIUs in counteracting the circumvention of international financial sanctions.<sup>61</sup> There are still problems stemming from the differences between national legal systems, given that not all countries make sanction evasion a predicate crime for money laundering, with consequent lack of uniformity in the ability to use the AML powers and tools of analysis and cooperation in matters of economic sanctions.

In the periodic sessions, FIUs shared their operational experiences, problems and good practices for identifying and tracing assets to designated persons through analysis and cooperation. The purposes of the Group include facilitating the work of the intergovernmental Transatlantic Task Force created for the effective application of the financial sanctions.<sup>62</sup>

<sup>60</sup> The Unit's Communication of 24 March 2022 provided guidance on the timing and procedures for the submission of this information by credit institutions. In April 2022 the Unit posted on its website the first FAQs (UIF, *Annual Report for 2021*, p. 88).

<sup>61</sup> UIF, *Annual Report for 2021*, p. 88.

<sup>62</sup> UIF, *Annual Report for 2021*, p. 88.

## 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 within its competence. 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

In the course of 2022 negotiations continued, though not all at the same pace, on the four legislative proposals presented by the Commission on 21 July 2021, known as the AML Package.<sup>63</sup> The UIF is part of the Italian delegation, under the coordination of the Ministry of Economy and Finance, that takes part in the legislative talks within the EU Council and contributes, through the FIUs' Platform, to the development of common positions.

AML Package

The negotiating process for the proposal on funds transfers has been concluded,<sup>64</sup> while talks on the other three proposals are still under way. The Council stated its position on the regulation establishing the European AML Authority on 29 June 2022.<sup>65</sup> On 7 December it finalized its opinion on the proposed regulations on the prevention of the use of the financial system for money laundering and terrorist financing (AMLR)<sup>66</sup> and for a sixth AML directive (AMLD6).<sup>67</sup> On 19 April 2023 the Parliament, in plenary session, approved the proposed

<sup>63</sup> UIF, *Annual Report for 2021*, pp. 105 et seqq.

<sup>64</sup> European Commission, [Proposal for a regulation concerning information accompanying transfers of funds and certain crypto-assets \(recast\)](#), COM (2021), 422 final.

<sup>65</sup> European Commission, [Proposal for a regulation of the European Parliament and the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations \(EU\) 1093/2010, \(EU\) 1094/2010, \(EU\) 1095/2010](#), COM (2021) 421 final.

<sup>66</sup> European Commission, [Proposal for a Regulation to the European Parliament and the Council on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing](#) COM (2021) 420 final.

<sup>67</sup> European Commission, [Proposal for a Directive of the European Parliament and of the Council on the](#)

amendments to the three AML Package measures still under examination. In May, under the Swedish presidency, the ‘trilogues’ with the co-legislators began; these talks are likely to be highly complex in light of the numerous, substantial amendments passed by Parliament, especially as regards the functions of the AMLA, which among other things is assigned a central role in international financial sanctions.

The proposed regulation on funds transfers, which requires that they be accompanied by information on the originator and the beneficiary in order to ensure transparency and traceability (the Transfer of Funds Regulation (TFR) Recast), updates the safeguards instituted in 2015 and extends them to transfers of crypto-assets and their operators.<sup>68</sup>

The framework of the proposal ensures full conformity with FATF Recommendations 15 and 16. The definitions of ‘crypto-assets’ and ‘crypto-asset service provider’ (CASP) reiterate those of the EU Regulation on markets in crypto-assets (MiCA), on which the Council and Parliament reached provisional agreement on 30 June 2022.<sup>69</sup> Strengthening the guarantees of traceability of crypto-assets is especially urgent with a view to countering their possible use to evade EU financial sanctions. The co-legislators have aligned the calendar for implementation of the TFR with that envisaged for MiCA. The obligation of traceability applies to all transfers of crypto-assets involving at least one CASP on the side of the originator or of the beneficiary; considering the high risk exposure, the regulation also applies to transfers connected to ATMs for crypto-assets (crypto ATMs) if the payer’s or payee’s CASP has a registered office in the European Union. Specific measures are envisaged in the case of transfers with a self-hosted address.<sup>70</sup> In the case of crypto-asset transfers executed with the involvement of just one CASP, with a self-hosted address either on the originator or on the beneficiary side, the CASP must acquire the required information from its own customer and assess its reliability: if the transfer exceeds an amount corresponding to €1,000, the CASP must take measures to verify that the address is actually owned or controlled by the customer (Article. 14(5)).

Person-to-person transfers of crypto-assets without the intervention of service providers remain outside the scope of the regulation, as do those in which the originator and the beneficiary are CASPs in their own right.

The European Banking Authority is charged with issuing a series of implementing provisions and guaranteeing dialogue with stakeholders to develop technical solutions facilitating implementation of the requirements laid down in the regulation.

[mechanisms that Member States must set up to prevent the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive EU/2015/849, COM \(2021\) 423 final.](#)

<sup>68</sup> On 29 June 2022 the negotiators of the Council and the Parliament reached a provisional agreement on the text of the proposal, approved on 10 October also by the Parliamentary Committee on Civil Liberties, Justice and Home Affairs and the Committee on Economic and Monetary Affairs. Adoption of the provisional agreement requires the final approval of the Council. See General Secretariat of the Council, [Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets \(recast\), 2021/0241 \(COD\)](#).

<sup>69</sup> On 5 October 22 the Committee of Permanent Representatives (Coreper) of the Member States reached provisional agreement on the Regulation and transmitted it to the European Parliament, which passed it on first reading on 20 April 2023. The text will be published in the *Official Journal of the European Union* following formal assent by the Council as well.

<sup>70</sup> This is a form of transaction in crypto-assets not handled by any CASP or other operator providing services in Europe analogous to those of CASPs. See Article 3(18.a) of the proposed regulation, whereby ‘self-hosted address means a distributed ledger address not linked to either of the following: a) a crypto-asset service provider; b) an entity not established in the EU and providing similar services’.

### International and Italian initiatives on crypto-assets

The FATF's Virtual Asset Contact Group is continuing its work to monitor the implementation of its standards on virtual assets, identify areas of weakness and propose adjustments, also in the light of developments in the sector. The group has produced a specific roadmap to hasten governments' implementation of the standards. The discussion concerning national approaches to crypto-assets for AML/CTF purposes will continue, as will the dialogue with the private sector.

Announcements of the progress made in the various jurisdictions should be forthcoming in the near future, especially as regards the availability of information on transfers of crypto-assets, including data on the originator and beneficiary (the 'travel rule'). Further study is being conducted on emerging risks in relation to Decentralized Finance (DeFi), non-fungible tokens (NFTs), peer-to-peer transactions (P2P) and unhosted wallets. A further issue for consideration is the financial sanctions applicable to balances held in crypto-assets.

In Italy, on 16 May 2022 the Organization of Agents and Mediators' register of virtual currency traders went live, and by May 2023 it counted over 100 entities. Contacts are under way among the various authorities in this sector to examine questions of interpretation and application to these operators.

The most innovative aspect of the entire AML Package<sup>71</sup> is the European Anti-Money Laundering Authority, envisaged as a new, decentralized EU agency with novel features to serve as AML supervisor and as support and cooperation mechanism among FIUs. As regards the regulation establishing the AMLA, the position adopted by the Council<sup>72</sup> lacks agreement on the site of its headquarters (see the box 'Creation and headquarters of the AMLA: implementation issues and the impact on the UIF' below). The range of entities subject to the Authority's direct supervision is extended to include crypto-asset service providers with significant risk profiles; and supervisory tasks are extended up to 40 obliged entities and groups of banks or financial intermediaries, at least in the first selection procedure, so as to ensure full coverage of the internal market. Some limited changes to the Authority's governance are also enacted.

AML  
Regulation

Governance of the AMLA centres on two bodies: the General Board, with two distinct groups of members, one representing national supervisors and one FIUs; and the Executive Board with no representation of national authorities. The Chair, as top officer, represents the authority and is responsible for its activities, while the Executive Director, the organizational head, is assigned chiefly management tasks. An Administrative Board of Review offers recourse against adverse supervisory decisions.

In addition to assigning broader powers to the General Board, the Council also endorsed the proposal of the FIUs (which issued a common position in February 2022<sup>73</sup>) for a corrective to the Support and Coordination Mechanism with the creation of a Standing Committee (Article 47) in support of the General Board, freeing the latter to focus on strategic tasks and decision-making.

The Standing Committee, composed of nine members appointed by the General Board in keeping with the principles of balance and fair rotation among national FIUs, is not

<sup>71</sup> For the institutional characteristics, governance and functions of the AMLA, see UIF, *Annual Report for 2021*, pp. 107-109.

<sup>72</sup> General Secretariat of the Council, *Regulation establishing the AML Authority*, 2021/0240 (COD).

<sup>73</sup> UIF, *Annual Report for 2021*, p. 108.

endowed with powers of decision but is assigned permanent support functions, with tasks of initiative and proposal on all matters within the General Board's competence, working in close cooperation with the national delegates of the FIUs and with the AMLA staff. The creation of the Committee in no way limits the General Board's ability to create temporary internal committees in support of its functions.

As to the governance of the AMLA, the Parliament gave itself a stronger role in the selection and appointment of members of the Authority's ruling bodies. At the same time, it rejected the provision for a Standing Committee of FIUs in support of the General Board.<sup>74</sup>

With regard to joint analysis, the Council's position is not particularly ambitious. The role it envisages for the AMLA is not incisive, insofar as it is still anchored to the multinational as opposed to the supranational dimension, both in identifying possible relevant cross-border cases and in the operational development of exercises of analysis (Article 33). In these matters the Authority lacks significant powers, performing functions of mere operational support (such as IT, logistics and finance), conditioned by restrictions and limits on access to the FIUs' data, and ultimately has an essentially bureaucratic role, capable of generating very little value added in the current context.

In fact, in order to access FIUs' operational data, AMLA staff must have the explicit consent of all the FIUs involved in the joint analysis exercise; failing this, support to the exercise by means of access to data on the case can be provided only by the national FIU delegates to the AMLA (Article 35).

To combat criminals who – as noted in the Commission's recent Supranational Risk Assessment (see Section 9.1.2, 'Further European and international initiatives') – continually adapt their *modus operandi* to the changing context, seizing all the opportunities offered by European integration, the supranational dimension must be valorized, by strengthening the powers of the new Authority and assigning the FIUs greater responsibility for effective 'capture,' analysis and prompt dissemination to the competent authorities of cases of cross-border money laundering and terrorist financing. This position, however, runs counter to the majority view in favour of conserving national prerogatives in the launching and conduct of joint analyses, the limitation of the AMLA's role, and the segregation of FIUs' information.

The conditions envisaged for the dissemination of the results of joint analysis to investigative bodies – in the Council's draft, unanimous decision by all the participating FIUs – are likely to impede timely use of the information acquired for investigations, giving each FIU a *de facto* veto power.

By contrast, the European Parliament assigns the Authority a stronger role in joint analysis, both in selection and identification of cases and in the conduct of the analysis. Articles 33 and 34 charge the AMLA with tasks of direction and coordination and empower it to launch joint analyses at its own initiative. These changes capitalize on the supranational dimension of joint analysis and can enhance the capability to intercept and further investigate cross-border criminal activity. In addition, the Parliament gives the Support and Coordination Mechanism new tasks: mediation in the case of disagreements between FIUs (Article 5(5.da)); and monitoring and verification, also by means of peer reviews, of the regulatory and operational adequacy of the FIUs (Article 5(5.aa) and Article 5(5.db)). These functions can foster operational convergence and effectiveness among FIUs, but it is necessary to avoid duplications and inconsistencies between peer reviews and other, similar

<sup>74</sup> European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010.*

evaluation exercises conducted by international bodies, identifying the areas of potential coordination and synergy.

The Parliament's draft, moreover, assigns the AMLA a broad set of tasks intended to foster more effective, uniform application of EU financial sanctions and improve information sharing among authorities, a need that has emerged with the recent extension of the restrictive measures against Russia.

In particular, it extends to these issues the AMLA's power of direct supervision and promotion of convergence of the supervisory practices of national supervisors. The Authority is also given the task of facilitating compliance on the part of the obliged entities for those measures and is to serve as 'central contact point' for a broad, unspecified set of authorities competent for 'preparation, adoption, supervision and enforcement relating to targeted financial sanctions' for the sharing of information on the designated entities (Article 5(3) and 5(4a)).

However, the sets of obliged entities and competent authorities in this area do not correspond to those of the AML/CFT system, which constitutes one of the main problems with the amendments proposed.

### **Establishment and host city of the AMLA: implementation and the impact on the UIF**

The establishment of the AMLA will raise some AML supervisory functions to the supranational level. As a Support and Coordination Mechanism, however, the Authority should not perform the operational tasks proper to the FIUs, but it will have a significant impact on how national FIUs carry out these activities. In this context, a high priority for the Bank of Italy is mapping out and rapidly undertaking the necessary modifications of internal organization, instruments, procedures and resources to ensure active participation in the new supranational institutional framework, including with dedicated staff, and laying the groundwork for the requisite coordination with the AMLA in both areas of institutional action.

An inter-department roundtable on the institutional framework brought into being by the AML Package was held on 30 November 2022, with the participation of representatives of the Ministry of Economy and Finance, the Bank of Italy, and the UIF (see Section 10.3, 'Human resources'). The meeting decided to create a task force of staff from the supervisory department, the UIF and other relevant Bank of Italy functions to plan the actions needed to oversee the inception of the Authority and then, once it is fully operational, contribute to its various areas of activity, including the formation of Joint Analysis Teams, and meet the requirements, including information requirements, of the new Authority.

In the framework of a broader reform approved in 2022, changes have been made to adapt the UIF's organizational set-up to European developments, with the creation of a Division for 'Relations with international and European organizations,' dedicated to interaction and coordination with the nascent AMLA (see Chapter 10, 'Resources and Organization'). On 27 June 2022 the Bank of Italy activated an Anti-Money Laundering Supervision and Regulation Unit, under the Governing Board, with the function of guaranteeing effective cooperation with the new European AML Authority.

The protracted negotiations will result in a delay of about a year in the establishment of the AMLA, originally scheduled for January 2023, and also in the launch of its activity, initially set for 2024 for indirect supervision and the FIUs coordination mechanism and

2026 for direct supervision. Furthermore, while the governance arrangements have now been established, the nascent Authority's internal organization has yet to be determined, an issue now being examined by a task force at the Commission, nor has the host city for the AMLA been decided.

The host city for European agencies has been determined, to date, according to the general criteria laid down in the [Joint Statement and Common Approach on Decentralised Agencies](#) of the Parliament, Council and Commission of 19 July 2012. This procedure began with a call for tenders posted by the Commission, which evaluated the national candidacies and submitted them to the Council for decision. However, the European Court of Justice order of 14 July 2022<sup>75</sup> rejecting Italy's appeal against the choice of Amsterdam as seat of the European Medicines Agency, offers major elements elucidating the nature of the measure ('decision') determining the host city of European agencies, which are also relevant to the upcoming launch of the procedure for the AMLA. Specifically, the Court affirmed the legislative nature of these decisions, which accordingly cannot be adopted by the national governments but must result from a convergence of positions among the EU co-legislators. It is now up to the Commission, starting precisely with the launch of the procedure for the seat of the AMLA, to determine just how the Court order can be applied in practice. The three institutions are currently devising general requirements that must be satisfied by national candidacies for host city of European agencies.

A number of countries have announced their intention to propose candidate cities for the new Authority. On 17 January 2023, at a meeting with the EU Commissioner for financial services, financial stability and capital markets union, Italy's Minister of Economy announced Italy's candidacy to host the AMLA, in whose regard several Italian cities have expressed interest. The prospective location of the new Authority in Italy can count on a mature, sophisticated AML system characterizing both authorities and obliged entities and on the strong leadership in global and European contexts that the Italian authorities have always exercised in promoting more stringent harmonization based on more advanced safeguards. Italy, that is, represents a solid environment – in terms of the robustness of the AML apparatus and safeguards – for the location and development of the AMLA's activity. The criteria for the choice of host city, set out in considerable detail in the position of the European Parliament (Article 4) include not only high quality and reputation of the national AML system and the need for geographical balance and diversification of EU institutions but also various logistical and infrastructural factors, such as: accessibility of the seat; suitable educational structures, adequate access to the labour market, social security and medical care for children and spouses of the staff; the capability for close cooperation with the relevant European institutions and agencies; and strong safeguards for the digital and physical security of the agency's premises.

#### AMLD6

The proposed sixth AML directive, which will supersede Directive EU/2015/849, now in force, is intended to govern matters where margins of national flexibility need to be maintained.<sup>76</sup> These are provisions relating to the risk-based approach, registers of beneficial owners, bank accounts and real estate assets, the powers and duties of the supervisory authorities and the FIUs, the administrative sanction regime, and cooperation.

<sup>75</sup> European Court of Justice, [Order of the Court \(Grand Chamber\) 14 July 2022; 2022/C340/22](#).

<sup>76</sup> For a detailed examination of the AMLD6 proposal, see UIF, [Annual Report for 2021](#), pp. 107-108.

The Council's position paper on AMLD6<sup>77</sup> incorporates many of the proposals that the FIUs developed jointly in the Platform. In particular, as regards the power to suspend transactions (Article 20), the Council confirms that this may apply to one or more transactions, accounts or other relationships and specifies that it covers both current and future transactions.

The Council's draft calls for the flexible exercise of the suspension power, which is to be set by national legislation with a minimum and a maximum duration specified by the directive. The suspension would then be ordered for a term determined by the FIU case by case, within the duration specified by national law, and could be revoked by the FIU prior to expiry where the prerequisites are met. Considering the peculiar nature of the power of suspension, which is functional to the subsequent adoption of more stable measures, it cannot be open to appeal or other legal remedies; rather, the object of the appeal should be the seizure or confiscation order, which makes the temporary effect of the suspension permanent. The power of suspension could be exercised not only at the request of the FIUs of other Member States but also, on condition of reciprocity, at the request of counterparts in third countries, for the period and on the conditions specified by the national law of the FIU receiving the request.

The provisions concerning the feedback that FIUs must give to obliged entities are also more detailed. In particular, it is specified that the FIU cannot be required to provide feedback on every single STR but that 'such feedback shall cover at least the quality of the information provided, the timeliness of reporting, the description of the suspicion, and the documentation provided at submission stage' (Article 21(2)).

As to the information accessible to FIUs for their analytical functions, the Council's proposal contains excessive, unjustified restrictions and exceptions; what is needed, instead, is to enable FIUs to obtain relevant data in a direct and unfiltered manner, in keeping with the FATF standards, as regards all financial and administrative data, without prejudice to the restrictions on access to investigative information where this might impair ongoing investigations (Article 18).

The possibility for Member States to institute exceptions to the requirement for unfiltered access (Article 18(2.a)) on the part of the FIUs also for non-investigative data – e.g. financial and administrative data – where this would impair ongoing investigations or where there is a clear disproportion with respect to the legitimate interests of natural persons in relation to the purposes for which access is requested, gives the States ample margins for unduly restricting such access, impeding the efficacious performance of the FIUs' institutional functions.

The Parliament's draft on the proposed AMLD6<sup>78</sup> calls for numerous amendments designed to enhance the reliability and accessibility of the information contained in registers of beneficial owners and to extend their interconnections and application also to additional assets that are relevant to AML action and the implementation of financial sanctions, namely real estate (Article 16a), goods of high value such as yachts and aircraft (Article 16b) and goods held in bond (Article 16c). The National Risk Assessment, in this position, should now also cover implementation and evasion of financial sanctions (Article 8).

AML Regulation

<sup>77</sup> General Secretariat of the Council, *Proposal for a Directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*, 2021/0250(COD).

<sup>78</sup> European Parliament, *Report on the proposal for a directive of the European Parliament and of the Council on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU) 2015/849*.

The Parliamentary draft also introduces several measures to strengthen inter-FIU cooperation. It specifies that information interchange must not depend on the type of predicate offence and must be possible even where the predicate offence is not identified (Article 24(1)); it introduces monitoring to prevent the misuse of exceptional cases for refusal (Article 24(8)); in the case of dissemination of the information to third authorities, it would prohibit automatic utilization as evidence in judicial proceedings (recital 50c). The Parliament also calls for access to financial, administrative and investigative data on the part of FIUs ‘regardless of their organisational status’ (Article 18(1))

The proposed regulation to prevent the use of the financial system for money laundering or terrorist financing contains all the provisions applicable to the private sector with regard to preventive measures and the transparency of beneficial ownership.

The Council’s draft<sup>79</sup> introduces numerous amendments to further extend the typology of obliged entities, further harmonize the provisions on beneficial ownership, and align the definition of high-risk third jurisdictions to the FATF lists through their automatic transposition into the list issued by the European Commission.

Specifically, the entities subject to AML obligations would now include the entire set of crypto-asset service providers, who are required to perform due diligence on customers for occasional transactions of €1,000 or more, plus additional mitigation measures towards self-hosted wallets, as well as third-party financing intermediaries,<sup>80</sup> jewelers, watchmakers and goldsmiths.

As to the design of the obligation to report suspicious transactions (Article 50), it is stated explicitly that the suspicion should regard (apart from terrorist financing) any and all relevant circumstances upstream of the profit-generating crimes and downstream from the phase of money laundering proper; to mitigate the risk of an excessive number of possibly worthless reports, the reporting entity is expressly required to motivate and document the logical procedure followed and the decisions taken. The FIU’s power to acquire information is specified and complemented by the possibility of setting a deadline for the entity’s response.

The main problem with the formulation of this provision, however, is its allowance for possible derogations from the reporting requirement in cases of ‘low criminal intensity’ and absence of impact on the internal market, especially considering how difficult it is for obliged entities to identify such circumstances. Moreover, in concrete cases, even cases transactions of apparently little importance or involving small amounts may actually form part of extremely serious criminal operations, such as those involving child pornography.

The AMLA’s power to issue ‘draft implementing technical standards’ has been circumscribed to the minimum dataset of reports, canceling – with respect to the Commission’s proposal – the reference to format harmonization. In addition, it is specified that the new Authority’s issuance of guidelines in support of the obligations of active cooperation shall be without prejudice to the FIUs’ powers to supplement these instruments in the light of the risks and methods identified at national level.

In allowing outsourcing of the tasks connected with performance of the AML obligations laid down in the Regulation to reliable, qualified service providers, the draft reaffirms the ban

<sup>79</sup> General Secretariat of the Council, *Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*, 2021/0239(COD).

<sup>80</sup> A third-party financing intermediary is a firm not included among those obliged for other reasons, such as those providing crowdfunding services, whose business consists in matching or facilitating the matching of owners and financiers of a project via an information system based on internet open to the public or a limited number of financiers (Article 2(14c)).

on outsourcing tasks in connection with the detection and reporting of suspicious transactions or other strategic activities, such as risk assessment and the organization of policies and internal controls in support of compliance. Further, without prejudice to the ban on ‘tipping off’ unauthorized third parties that an STR has been or is being submitted, the draft enlarges the perimeter of permissible information exchange for the sharing of STRs among obliged entities (including those in different categories and with no need for reference to customers in common), with the objective of more effective detection of criminal operations with cross-border connections. Such exchanges are also considered as part of vaguely defined ‘partnerships for information sharing.’ These are mechanisms that can be included in national legislation for formalized cooperation between obliged entities and, where appropriate, public authorities for sharing data and data-processing, possibly also using artificial intelligence. Among the multiple, generic conditions for such sharing is the necessity for explicit authorization, case by case, by the FIU, but the pre-conditions and aims of the authorization are not defined.

The Parliament’s draft report on the proposed regulation<sup>81</sup> significantly increases the set of obliged entities to include, among others, certain categories that are not unequivocally defined, such as ‘wealth or asset managers’ and, drawing on the findings of the Commission’s Supranational Risk Assessment, leading football clubs, sports agents and associations, entities in the luxury goods business, and platforms marketing ‘non-fungible cryptoassets.’ In addition, the threshold for the application of customer due diligence is lowered from €10,000 to €5,000 for art dealers and auction houses (Article 3).

The draft would also introduce bans and specific measures for enhanced due diligence in relation to ‘golden passport’ and ‘golden visa’ investment schemes (Article 6a); and with regard to high-risk third countries it would broaden the criteria for identification (Article 24(3)) and assign powers of monitoring and assessment to the AMLA (Article 25). The threshold for cash payments is lowered from €10,000 to €7,000 euro (Article 59).

As to the reporting requirements, the Parliament’s draft does not rehearse the aforesaid derogations and exemptions envisaged by the Council, which are susceptible to problems of interpretation. Instead, it introduces a single European procedure for obliged entities’ transmission of STRs, via the FIU.NET ‘one-stop shop’ (Article 50(6a)). STRs are to be transmitted not only to the FIU of the Member State in whose territory the transmitting FIU is established but also to any other FIU concerned. This change would appear to be premature and of dubious feasibility, considering the structural characteristics of FIU.net, the heterogeneity of the national systems for handling reports, and the likely very high costs of implementation. This provision also poses legal and operational problems, especially in the coordination of activities.

On 25 May 2022 the Commission presented two legislative proposals to complete and harmonize the set of rules and safeguards governing financial sanctions and confiscations. The restrictive measures and financial sanctions adopted by the Union through regulations, pursuant to Article 21 TEU and Article 215 TFEU, are not backed by harmonized sanction measures. The Union’s lack of competence in penal matters produces shortcomings and discrepancies in national sanction laws as regards both type (civil, administrative, penal) and size. These problems came out extremely clearly in the face of the increased complexity and scope of the economic sanctions adopted by the EU against Russia and Belarus, with a consequent increase in the risk of sanction evasion through arbitrage. The Commission proposes uniform sanctions for the violation or evasion of the restrictions, with the

**Proposed directive  
on financial  
sanctions**

<sup>81</sup> European Parliament, *Report on the proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.*

application of a penal regime by a procedure requiring the preliminary broadening of the matters ‘eligible’ for European interventions of penal regulation pursuant to Article 83(1), TFEU.<sup>82</sup>

To be specific, the proposal calls for a ‘Council Decision,’ which is necessary to extend the criminal competence of the Union and lay the juridical basis for subsequent legislation – by means of a regulation – to criminalize sanction evasion. The Council adopted the decision on 28 November 2022,<sup>83</sup> followed immediately by the Commission’s adoption of the proposal for a directive.<sup>84</sup>

The proposal sets out the minimum elements defining this crime, the penalty perimeter, and the criteria for its rooting in jurisdiction. It calls for punishment of violations of multiple restrictive measures (freezes, embargos, prohibitions), of the evasion of those measures, and of the conditions laid down in authorizations issued by the competent authorities. It contemplates specific sanctions for legal persons as well. It further provides that in cases of evasion of restrictive measures the funds and assets subject to it are to be treated as proceeds of crime subject to confiscation pursuant to the future Directive. Article 17 of the proposed directive would amend Directive EU/2018/1673, Article 2(1), in order to define the violation of EU restrictive measures itself as a ‘criminal activity’ and eligible predicate offence for money laundering.

**Proposed  
directive on  
confiscation**

A second proposed directive<sup>85</sup> is intended to strengthen the capabilities of competent authorities to identify, freeze and manage the assets subjected to sanction and to extend and make more efficacious the regime of confiscation of illicit assets. This objective is pursued via the easing of the burden of proof for prosecutors and the introduction of ‘non-conviction-based confiscation’<sup>86</sup>, in keeping with FATF standards (Recommendations 4 and 38) and the Council of Europe’s Warsaw Convention of 2005.<sup>87</sup>

Article 2 of the proposed directive determines the scope of the serious crimes to which the new confiscation measures shall apply. These include the future crime of sanction evasion, which will also be a predicate offence for money laundering. The introduction of this latter crime, already envisaged in some European legal systems, could have significant effects on the activity of the UIF, which would then be in a position to exercise all its functions of analysis, cooperation and dissemination in this sphere as well.

<sup>82</sup> European Commission, *Proposal for a Council Decision on adding the violation of Union restrictive measures to the areas of crime laid down in Article 83(1) of the Treaty on the Functioning of the European Union* (COM (2022) 247 final, 25 May 2022). Article 83(1) of the Treaty provides that the Union may ‘establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension. On the basis of developments in crime, the Council may adopt a decision identifying other areas of crime that meet the criteria specified in this paragraph.’

<sup>83</sup> *Decision (EU) 2022/2332*, OJEU 308, 29 November, p. 18.

<sup>84</sup> European Commission, *Proposal for a directive of the European Parliament and the Council on the definition of criminal offences and penalties for the violation of Union restrictive measures*, COM (2022) 684 final.

<sup>85</sup> European Commission, *Proposal for a Directive of the European Parliament and the Council on asset recovery and confiscation*, COM (2022) 245 final.

<sup>86</sup> Specific circumstances allowing confiscation without conviction are listed in Article 15. These are cases in which the criminal proceedings cannot continue because of: (a) illness of the suspected or accused person; (b) absconding of the suspected or accused person; (c) death of the suspected or accused person; (d) immunity from prosecution of the suspected or accused person, as provided for under national law; (e) amnesty granted to the suspected or accused person, as provided for under national law; (f) the time limits prescribed by national law have expired, where such limits are not sufficiently long to allow for the effective investigation and prosecution of the relevant criminal offences.

<sup>87</sup> Italy ratified the Convention with Law 153/2016.

### 9.1.2. Further European and international initiatives

The evaluation of the Italian AML system that the Commission began in the second half of 2021 to assess the efficacy of implementation of the measures adopted by the Member States, focusing on the transposition of the rules and their effectiveness, was concluded last year.<sup>88</sup> The exercise will result in an aggregate survey, which should be published in 2023, on the overall level of transposition and implementation of the fourth directive, highlighting the main problems discovered.

Assessment by the Commission

On 27 October 2022 the Commission published an account of the updating of the supranational risk assessment (SNRA) for 2019, to which the European FIUs contributed with reports on the results of their operational activity through the FIUs Platform.<sup>89</sup>

SNRA

Specifically, the Commission updated its assessment of the risk of money laundering and terrorist financing for the internal market posed by 43 products and services, grouped into eight categories, taking account of the intervening changes to the European AML regulatory framework and relevant contextual factors, such as the pandemic and the stiffening of sanctions against Russia and Belarus.<sup>90</sup>

The report also considers the heightened money laundering risk consequent to the pandemic in various areas of activity – fraud, cybercrime, corruption – and the risks generated by the conflict in Ukraine. The discussions within the Freeze and Seize Task Force – instituted by the Commission to ensure effective application of the sanctions and information exchange among authorities – have made it clear that the difficulties of identifying oligarchs’ assets (‘screened’ by complex corporate structures with branches in multiple jurisdictions, including outside Europe, and by local nominee shareholders) are such that a top priority for the competent authorities is access to accurate, up-to-date information on beneficial ownership.

This exercise too is accompanied by recommendations calling on Member States to ‘comply or explain.’ The measures recommended include allocating adequate resources to the FIUs and supervisory authorities, conservation of accurate, up-to-date information on the beneficial ownership of corporate structures and trusts, where possible bringing forward the application of the measures envisaged by the AML Package, and closer cooperation between authorities and obliged entities, with forms of public-private partnership (PPP).

Cooperation between the relevant authorities and the private sector through public-private partnership arrangements brings value added to the fight against money laundering and terrorist financing, heightening risk awareness and enhancing the quality of STRs thanks to the exchange of strategic and operational information. Lacking a harmonized definition, the models in place in the various Member States are heterogeneous in form and structure; and depending on the nature and degree of confidentiality of the information exchanged, they are covered by differing mechanisms of data protection. In line with the Action Plan of 2020 and following a public consultation in 2021, on 27 October 2022 the Commission

PPP guidelines

<sup>88</sup> UIF, *Annual Report for 2021*, p. 111.

<sup>89</sup> Article 6(1) of the AML Directive requires the Commission to update the SNRA every two years (or more often if necessary). The first SNRA was published in 2017, the second in 2019; the third was delayed by the pandemic. See European Commission, *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, COM (2022) 554 final.

<sup>90</sup> Specifically: 1) Cash-related products and services; (2) Financial sector; (3) Non-financial products and services; 4) Gambling sector; 5) Non-profit organizations; 6) Professional sports; 7) Free zones; and 8) Investor citizenship and investor residence schemes.

released a set of guidelines<sup>91</sup> for sharing – given the great diversity of the PPP structures and typologies in place in the different Member States – the good practices of public-private cooperation, in order to better grasp the potential value added and sustain their development.

These guidelines include: a) clear governance structure and objectives; b) involvement of FIUs and data protection authorities; c) national guidelines or regulations specifying the objectives of cooperation and the rights and duties of the participants; d) a secure IT platform for sharing specific types of confidential information; e) key performance indicators to measure the effectiveness and results of the partnership;<sup>92</sup> and f) involvement of NGOs and academic and research institutions, where expertise on specific risks and activities is required

#### Digital Euro

The special High-level Task Force formed at the ECB in July 2021 continued its study of the issuance of digital euros. Two reports, released in September and December 2022, dealt with the problems of AML safeguards and controls to which the digital currency will have to be subject.<sup>93</sup>

### AML aspects of the digital euro

The digital euro would be one among other Central Bank Digital Currencies (CBDCs), instruments issued by central banks and quite distinct from the multiple varieties of crypto-asset. According to the ECB Task Force, the special configuration of the digital euro as legal tender complementary to cash requires striking the proper balance between maintaining the anonymity of cash (a desirable cash-like feature) and incorporating appropriate safeguards for AML/CFT purposes. In the model hypothesized by the Task Force, once issued by the ECB the digital currency would be made available to users exclusively through supervised intermediaries, in dedicated digital accounts or wallets. The model also calls for quantitative limits on holdings of digital euros. To prevent illicit use, full anonymity is precluded, and in any case customer due diligence will be required.

The Task Force considers various options as to the scope and depth of transaction monitoring. The baseline scenario posits full access for intermediaries to data on customers' digital euro transactions for AML/CFT purposes. Two other options, however, would entail a restricted spectrum of controls in order to replicate the confidentiality guarantees typical of cash payments. One, designated 'selective privacy,' would allow simplified due diligence for low-value or low-risk payments, while subjecting transactions above the threshold to the ordinary controls. The second, 'offline functionality,' would totally shelter from controls all transactions effected with no online connection (by validation criteria still to be defined) and with physical proximity of the parties, on the model of cash payments.

The Task Force has further considered the compatibility of simplified controls and obligations with European rules and the AML Package, interacting with the Commission, which should present a proposal for a regulation on the digital euro this year. By the end of 2023 the ECB Governing Council will decide on the launch of the phase of realization and implementation of the digital currency.

<sup>91</sup> European Commission, *On the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing*, SWD (2022) 347 final.

<sup>92</sup> For example: number of reports, investigations, trials or convictions consequent to PPPs, or improvement in the quality of STRs.

<sup>93</sup> ECB, *Progress on the investigation phase of a digital euro* and *Progress on the investigation phase of a digital euro – second report*, 2022.

## 9.2. The Italian legislative and regulatory framework

Italian primary AML legislation underwent only limited changes in the course of 2022. However, a number of significant secondary legislative measures were issued in implementation of the AML Decree.

### 9.2.1. Legislation

The AML Decree was amended to incorporate an additional derogation to official secrecy in information exchange with police forces.<sup>94</sup> Confidentiality safeguards for AML information were reinforced, in particular in the case of its use by the judicial authorities in penal proceedings.<sup>95</sup>

**Sostegni-ter and Milleproroghe decrees**

The budget law for 2023<sup>96</sup> newly modified the threshold for cash transfers between different parties; as of 1 January 2023 the limit is raised to €5,000.<sup>97</sup>

**The 2023 budget law**

For the first time, Italian law now includes tax rules governing crypto-assets. Specific provisions on the matter have been introduced into the Consolidated Income Tax Law, governing capital gains and income deriving from transactions in ‘crypto-assets.’<sup>98</sup>

The ‘tax simplification decree’<sup>99</sup> alters the rules for monitoring for tax purposes of transfers by means of banking, financial and other intermediaries.<sup>100</sup> The new rules are intended to re-establish coordination between the communication requirements laid down by the decree and the obligation of data conservation governed by the AML decree.

**‘Tax simplification decree’**

First, the law lowers to €5,000 the threshold above which banks and financial intermediaries shall report to the Revenue Agency and transmit the data on transfers, including those in virtual currencies, from or to foreign countries, on behalf or to the benefit of natural persons, non-commercial entities, simple partnerships and equivalent associations. Also, it eliminates the communication requirement in the case of split transactions, i.e. those that in economic terms constitute a single operation but are carried out via a series of

<sup>94</sup> Article 12(8) of Legislative Decree 231/2007 as amended by Decree Law 4/2022 (‘Sostegni-ter’ decree) provides that official secrecy cannot be invoked against the central services of the Police, the Carabinieri or the Finance Police in cases in which data or analyses of the UIF are of the most urgent necessity for the prevention, detection, investigation or prosecution of actions definable as crimes against the State as per Articles 270 to 270-septies of the Penal Code (UIF, *Annual Report for 2021*, p. 113).

<sup>95</sup> Specifically, confidentiality protection was extended in objective terms and now covers, in addition to the identity of the reporting parties narrowly defined, also the transmission of STRs and of information sent by the FIUs and the content of those messages; and the ‘identification data of reporting parties’ are now covered by reinforced and more specific protections. Finally, a new sanction of from two to six years imprisonment is introduced for persons convicted of wrongly revealing the identity of reporting parties or disclosing information on the transmission or the content of the report or information forwarded by the FIUs, where the information is such as to identify the reporting party (Article 38(3) and (3-bis) of Legislative Decree 231/2007, introduced by Article 3(1.b) of Decree Law 228/2021, converted with amendments by Law 15/2022; UIF *Annual Report for 2021*, pp. 114-115).

<sup>96</sup> Law 197/2022.

<sup>97</sup> Article 49 of Legislative Decree 231/2007 as amended by Law 197/2022, Article 1(384.b).

<sup>98</sup> Under the new rules, capital gains and other earnings realized via redemption or sale, exchange or holding of crypto-assets, however denominated, for a total amount of at least €2,000 during the tax year shall be considered ‘other income’ for tax purposes. However, the exchange of crypto-assets with the same features or functions has no tax implications (Consolidated Income Tax Law, Article 67(1.c-sexies), introduced by Law 197/2022, Article 1(126)).

<sup>99</sup> Decree Law 73/2022, converted with amendments into Law 122/2022.

<sup>100</sup> Decree Law 167/1990, converted with amendments into Law 227/1990.

transactions, each below the reporting threshold, effected at different times within a circumscribed period, set at seven days.<sup>101</sup>

The Decree also simplifies certain obligations laid down in the law to counter the financing of firms producing anti-personnel mines, cluster munitions and submunitions,<sup>102</sup> without prejudice to the UIF's controls on financial flows traceable to those firms.

The new rules require supervisory bodies to issue instructions for the exercise of enhanced controls on the actions of authorized intermediaries.<sup>103</sup> They eliminate the requirement for supervisory bodies to draw up a list of companies to which the ban on financing applies. Authorized intermediaries are required to institute appropriate procedural safeguards and check, at the least, the publicly available lists of companies that produce anti-personnel weapons and cluster munitions and submunitions. The rules on controls have also been revised, assigning them to all supervisory bodies, as have those on sanctions.

#### Civil justice reform

Within the broad process of reform of civil trial procedures, Legislative Decree 149/2022 revised the procedure for property dispossessions, imposing AML information requirements on the awardee.<sup>104</sup>

In particular, the Decree amends Article 585 of the Code of Civil Procedure, laying down that within the time limit fixed for payment the awardee shall communicate to the executing judge or delegated professional, in writing, and in awareness of the civil and penal liabilities for false or mendacious declarations, the information specified in Article 22 of Legislative Decree 231/2007 in the matter of due diligence.

#### Transfer of tax credits

A succession of legislative measures in 2022<sup>105</sup> repeatedly revised the rules on the transfer of tax credits under the 'Relaunch Decree'.<sup>106</sup> In this context the legislation expressly recognizes the importance of application of the AML obligations.<sup>107</sup>

The revisions in the course of the year involved the number of transfers allowed for tax credits, with provision for up to three additional transfers only in favour of banks and financial intermediaries, companies belonging to banking groups, or insurance companies authorized to do business in Italy pursuant to the Private Insurance Code specified in Legislative Decree 209/2005, without prejudice to the obligation not to proceed with the acquisition of the credit where the conditions are met for an STR to the UIF or where it is impossible to perform customer due diligence. Banks and companies belonging to a banking group may always transfer tax credits to persons other than consumers or holders of current

<sup>101</sup> Article 16 of Decree Law 73/2022 (converted into Law 122/2022), which amends Article 1(1) of Decree Law 167/1990.

<sup>102</sup> Law 220/2021. See UIF, *Annual Report for 2021*, p. 115.

<sup>103</sup> The law also extends, with specifications, the list of authorized intermediaries subject to prohibitions and limitations, which now includes electronic money institutions and payment institutions, micro-credit firms in the list referred to in Article 111 of the Consolidated Law on Banking, insurance and reinsurance undertakings (including secondary branches in Italy of foreign undertakings), Italian branches of foreign securities investment firms, asset managers, banks, electronic money institutions and payment institutions, Poste italiane S.p.A. (for 'bancoposta' operations) and Cassa depositi e prestiti S.p.A.

<sup>104</sup> Legislative Decree 149/2022, Article 3(41.a).

<sup>105</sup> Decree Law 4/2022 (the 'Sostegni-ter' decree), converted with amendments into Law 25/2022; Decree Law 17/2022 ('Bollette' decree), converted with amendments into Law 34/2022; Decree Law 50/2022 ('Aiuti decree'), converted with amendments into Law 91/2022; and Decree Law 176/2022 ('Aiuti-quater' decree), converted with amendments into Law 6/2023). See UIF, *Annual Report for 2021*, pp. 113, 114.

<sup>106</sup> Decree Law 34/2020, converted with amendments into Law 77/2020.

<sup>107</sup> Decree Law 34/2020, Article 122-bis(4).

accounts with the same bank, or with the parent bank, but the latter may not effect any further transfer.<sup>108</sup>

Lastly, Decree Law 11/2023 blocked, from 17 February 2023 onwards, the transfer of credits deriving from tax bonus programmes, save for building projects that have already been initiated.<sup>109</sup>

DL 11/2023

Another provision precludes the liability of the transferee in the case of total or partial non-fulfilment of the requirements for obtaining the tax credit where the transferee is in possession of specific documentation; this requires, among other things, an attestation of fulfilment of the obligations specified in Articles 35 and 42 of the AML decree, issued by the counterparty to the transfer.<sup>110</sup>

### 9.2.2. Regulatory and other measures

In the course of the year the Unit continued with the complete revision of the anomaly indicators, with the aim of bringing together in a single, consistent regulation the types of cases that can be helpful to the obliged entities in fulfilling their obligations of active cooperation.

#### The new anomaly indicators

The new anomaly indicators, following wide-ranging discussions with the Finance Police, the supervisory authorities, self-regulatory bodies and the other main AML/CFT stakeholders, have been designed to reconcile the updating of operational provisions with the need for a simplified and systematic typology of the multiple cases identified over the years.

The Measure formulated by the UIF is addressed to all obliged entities and meets the need for consistency in this matter, as well as for homogeneity and correctness in fulfilment of the STR reporting requirements, with a view to improving the quality of the reporting flow. In applying the new indicators, obliged entities will have to perform an appropriate evaluation of the transactions that come to light in the course of their professional activity, avoiding the indiscriminate equation of anomaly with suspicion and exploiting the correlations between the subjective and objective aspects of the operations.

The Unit designed 34 indicators, each with a set of sub-indicators as examples of the main indicator. Some indicators, with their sub-indicators, related to the conduct or salient characteristics of the party whose transactions are being considered (Section A), while others relate to the characteristics and configuration of transactions also with respect to specific sectors of activity (Section B) and still others, finally, refer to transactions that might be related to the financing of terrorism or the proliferation of weapons of mass destruction (Section C).

Obliged entities must apply the indicators selected in the light of the concrete activity performed; for each indicator identified, they select the relevant sub-indicators for that type of activity, as long as the circumstances described by the indicators and sub-indicators are relevant to the suspicion, where they are not justified by specific needs

<sup>108</sup> Decree Law 34/2020, Article 121(1.b).

<sup>109</sup> Article 2 of Decree Law 11/2023, converted into Law 38/2023, prohibits, in relation to the projects referred to in Decree Law 34/2020, Article 121(2), any further exercise of options alternative to the tax credit referred to in Article 121(1.a and 1.b) of that Decree.

<sup>110</sup> Where this counterparty is a listed company or a member of a banking group but not an obliged entity pursuant to the AML regulations, the attestation shall be issued by an auditor engaged to this purpose (Article 1 of Decree Law 11/2023, as amended in conversion into Law 38/2023).

explained by the party engaging in the operations or by other reasonable grounds. The list of indicators and sub-indicators is neither exhaustive nor binding, however; that is, other types of behaviour, while not described in the indicators, may give rise to concrete grounds for suspicion.

New indicators of involvement of politically exposed persons, Italian or foreign, and also of public entities or entities with public functions, have been introduced. Independent importance is ascribed to elements of anomaly in connection with the use of crypto-assets, with the assignment or acquisition of credits or the assignment of assets in the context of bankruptcy proceedings or credit guarantees, and also with regard to recourse to correspondent current accounts and the like. Specific sub-indicators, finally, refer to collective financing schemes (such as crowdfunding) or peer-to-peer lending. In sectors already highlighted by the previous set of indicators or anomaly patterns (e.g. money transfer agents, trusts, gaming), the new indicators capitalize on the UIF's experience of financial analysis and inspections, as well as the contributions and dialogue with authorities and associations in various sectors.

The Unit has published a table comparing the old and new indicators to help obliged parties identify the areas of effective change.

#### MD 55/2022

On 25 May 2022 the Ministry of Economy and Finance issued Ministerial Decree 55 for implementation of the register of beneficial owners of enterprises with legal personality, private legal persons, and trusts and similar entities, pursuant to Article 21 of Legislative Decree 231/2007. The register is not yet operational, however, owing to the failure to approve several additional implementing provisions;<sup>111</sup> owing to this delay, on 26 January 2023 the Commission sent Italy a formal notice of infringement under Article 258 of the TFEU, thus initiating the proceeding for inadequate transposition of the fourth AML directive, as amended by the fifth directive in 2018.<sup>112</sup>

#### The register of beneficial owners in the light of DM 55/2022 and the Court of Justice Judgment of 22 November 2022

The register of beneficial owners,<sup>113</sup> a special section of the register of enterprises, was instituted in implementation of the fifth AML directive in order to enhance transparency and prevent the use of corporate screens and instruments for purposes of money laundering.

Ministerial Decree 55/2022, which went into force as of 9 June 2022, lays down provisions concerning: communication to the register of enterprises of data and information relating to beneficial ownership, to be entered and conserved in the autonomous section and the special section; access to the data and information for authorities, obliged entities and other parties; and security in the handling of the data and information.

<sup>111</sup> On 20 April 2023 the Ministry for Enterprises and Made in Italy issued a directorial decree approving the technical specifications for the electronic format of the single communication of the enterprise. However, the decrees on secretariat fees and on the forms for the issue of certificates and copies, including digital copies, are yet to be issued, as is the final decree ascertaining that the communication system is operational.

<sup>112</sup> A notice of infringement along the same lines was also sent to Spain.

<sup>113</sup> To enhance data sharing and transparency, at European level a Beneficial Ownership Registers Interconnection System (BORIS) has been instituted. Boris went operational on 22 March 2021 following publication of the Commission's implementing regulation EU/2021/369.

Once the register goes operational it will be necessary to make sure that its consultation is not the sole check made by obliged entities as part of customer due diligence. Instead, there must be a critical, proactive approach to the information that is acquired about customers. Accordingly, an especially important provision of DM 55/2022 is the institution of the requirement for prompt communication to the competent chamber of commerce of any differences discovered between the information on beneficial ownership in the register and that found by the obliged entity in the course of due diligence.<sup>114</sup> These communications will permit monitoring of the discrepancies found by the obliged entities and will be accessible to the authorities that can access the register, with a guarantee of anonymity for the reporting parties.

The time required to realize the register of beneficial owners was also affected by the European Court of Justice. In its Judgment of 22 November 2022 on the joined cases C 37/20 and C 601/20, the Court struck down the AML directive provision for accessibility to ‘any member of the general public’ of information on beneficial ownership of companies and other legal entities established in EU Member States.<sup>115</sup> The Court held that access to beneficial ownership data for the general public constitutes a serious infringement of the fundamental right to respect for these parties’ private life and personal data protection,<sup>116</sup> allowing a potentially limitless number of persons to be informed of the material and financial situation of the beneficial owner. The possible consequences for these parties stemming from illicit use of their personal data are aggravated by the fact that once they become publicly available the data can not only be freely consulted but also conserved and disseminated.<sup>117</sup>

The register of beneficial owners could play a significant role in averting the risks in connection with implementation of the NRRP; to this end it would be especially useful to recognize the right of general government bodies to access the register.

On 22 April 2022 the Ministry of Economy and Finance adopted a new regulation (Ministerial Decree 59/2022) on the working of the Financial Security Committee, with provisions on its procedure for adopting resolutions and on the network of experts. In addition, the regulation denies access to some documents produced or held by the Committee relating to national security, defence, and the continuity and correctness of foreign relations.

**MD 59/2022**

With a decree dated 31 May, the Ministry also laid down rules governing the technical process of data input and consultation of the register of accredited entities and agents of payment service providers and electronic money institutions provided for by Legislative Decree 231/2007.<sup>118</sup>

**MD of 31 May 2022**

<sup>114</sup> DM 55/2022, Article 6(5).

<sup>115</sup> Article 30(5.1.c) of Directive EU/2015/849, as amended by Article 1, point 15(c) of Directive EU/2018/843.

<sup>116</sup> Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

<sup>117</sup> In order to comply with the Judgment, the Ministry of Enterprises and Made in Italy, in accord with the Ministry of Economy and Finance, acknowledged the necessity not to apply Article 7(1) of DM 55/2022, and also, pending legislation fully complying with the Judgment, to restrict access to the data on beneficial ownership of enterprises and private legal persons solely to persons who can demonstrate a legitimate, specific interest.

<sup>118</sup> Article 45 of the Legislative Decree.

The Ministry determined the data that shall be notified to the Association of Agents and Mediators (OAM) and the time limits for making such communications. The communication must be in electronic form, using the service available in the dedicated, private section of the OAM portal. A period of three months from the Decree's entry into force (7 September 2022) was set for the OAM to begin management of the register and its sections and subsections.<sup>119</sup>

MEF Circular  
56499/2022

Nearly five years after its previous circular (No. 54071, 6 July 2017), the MEF Treasury Department issued Circular 56499 (17 June 2022) containing updated operational instructions to the central offices and branches of the Ministry charged with applying the sanctions referred to in Title V of the AML decree.

With reference to the violation consisting in failure to file an STR, after distinguishing between simple and severe violations pursuant to Article 58 of Legislative Decree 231/2007, the Circular provides detailed indications for defining severe infractions as 'grave,' 'repeated,' 'systematic' and 'multiple' and consequently subjecting them to stiffer fines.<sup>120</sup> As to the amount of the fines for these cases, the Circular reiterates the further subdivision of sanction measures into three ranges, corresponding to three degrees of severity of the violation. Similar indications are also given for violation of the requirements of due diligence and conservation of data. Finally, the Circular provides further clarification on cumulative sanctions, on the principle of *favor rei*, and on the time limit for conclusion of the proceeding and application of a reduced fine.

MEF Circular  
30/2022

On 11 August 2022, the State General Accounting Department of the MEF issued Circular 30/2022 on control and accounting of NRRP measures, with specific guidelines for central government departments and implementing parties (*Linee Guida per le Amministrazioni centrali e i Soggetti attuatori*). The Circular highlights the importance of AML obligations to avert the risks inherent in the implementation of the measures.

The Circular includes the adoption of measures and controls for the correct identification of beneficial owners among the key activities in this process, both for 'implementing parties' and for 'central government departments responsible for NRRP measures.' Section 3.4 of the guidelines presents the AML/CFT regulatory framework and the institutional architecture of the AML system, calling attention to the role of the UIF and in particular to the Communication ([only in Italian](#)) of 11 April 2022 with initial indications for the prevention of the risks connected with the NRRP.

CONSOB notice

On 20 December 2022 CONSOB issued a notice to legal auditing firms and legal auditors under its supervision, reminding them of the high risk of money laundering in connection with activities involving crypto-assets and the consequent need for special

<sup>119</sup> The electronic services of registration for the entry of central contact points of EU payment service providers and electronic money institutions went operational on 6 December 2022, in the dedicated section of the Register for accredited entities and agents. These services can also be used for accreditation, by PSPs and EMIs established in Italy, for their twice-yearly communications of accredited entities and agents operating in Italy (OAM press release of 6 December 2022 - [only in Italian](#)).

<sup>120</sup> The authority reporting the infraction, in defining it as violation of the obligation to report suspicious transactions, is required in its charge to identify which of the two types of infraction envisaged by the law corresponds to the actual case at hand, without prejudice to its power to make a motivated redefinition of the case (*in melius* or *in peius*), on the basis of the facts in its possession, including those acquired in the course of the inquiry or provided by the party under inquiry as part of the participation in the procedure as provided by the regulations in force. Unlike its predecessor, the new Circular also specifies that any redefinition *in peius* must be adequately motivated with reference to the parameters that define severe violations under Article 58(2) of Legislative Decree 231/2007.

prudence in performing the obligations of risk assessment with respect to assignments conferred on them from customers operating in that sector.<sup>121</sup>

The National Council of the Order of Labour Consultants, in a resolution of 27 May 2022, approved a set of technical rules with indications for the assessment by labour consultants of money laundering risk in connection with their professional activity,<sup>122</sup> considering the types of customer and professional services requested, as well as the size and organizational features of the professional practice. There are also rules on customer due diligence and on the conservation of data and information.

**Labour  
Consultants  
technical rules**

Lastly, on 16 November the National Council of Notaries (CNN) and the National Council of Accountants and Bookkeepers (CNDEC) signed an agreement for AML cooperation. Under the agreement, the CNN will make available to the CNDEC its information technology for transmitting to the UIF any STRs submitted by their members.

**Agreement  
between CNN  
and CNDEC**

<sup>121</sup> Given customer and assignment risk factors resulting in the attribution of high money laundering risk, enhanced due diligence is mandatory, with provision, both at the acceptance of the assignment and during the provision of the professional service, for more thorough, more extensive and more frequent analyses and controls, including accounting controls, in order to detect any elements of anomaly or suspicion to report to the UIF.

<sup>122</sup> Legislative Decree 231/2007, Article 11(2).



## 10. RESOURCES AND ORGANIZATION

### 10.1. Organization

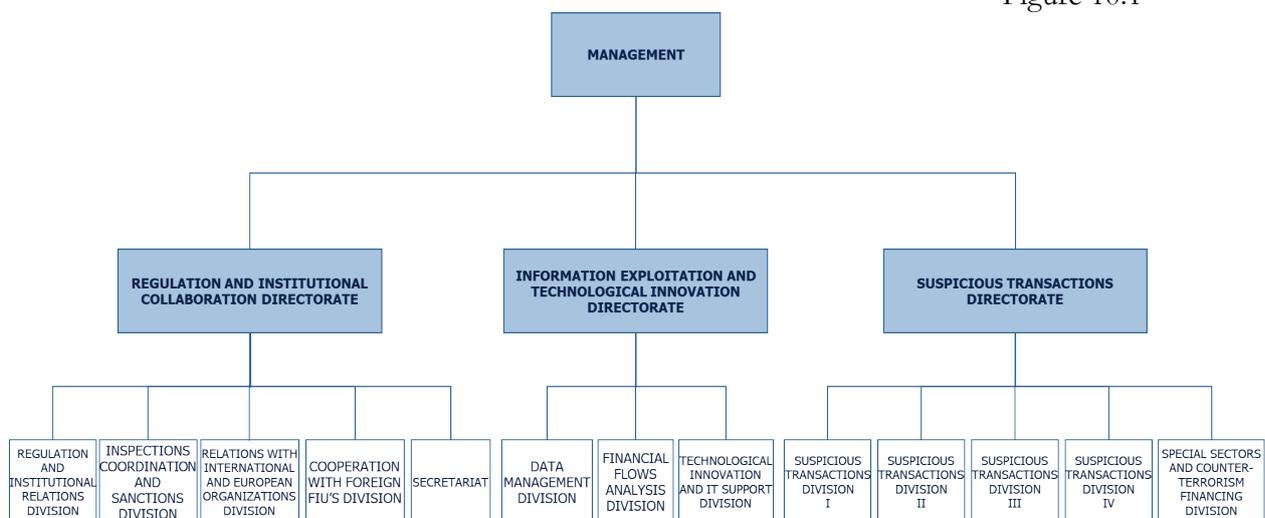
The UIF is headed by the Director, who is assisted by the Deputy Director and a number of staff managers. It is structured as three Directorates: the Suspicious Transactions Directorate, for the financial analysis of suspicious transaction reports; the Regulation and Institutional Collaboration Directorate, which is responsible for legislation, inspections, cooperation with the judiciary and other domestic and foreign authorities, and also comprises the Unit's Secretariat; and the Information Exploitation and Technological Innovation Directorate, responsible for IT activities, database management and statistical and econometric analysis.

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

A Committee of Experts, 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, is an invaluable forum for discussion, providing constant support for the Unit's activities and insights into the most important issues.

The UIF's steadily intensifying institutional engagement and the innumerable changes that have occurred, not least the implementation of the European AML Package, necessitated the reinforcement of its organizational structure. In February 2023 a third Directorate was created and the number of Divisions increased from 10 to 13. The new organizational arrangement is specified in Article 5 of the Bank of Italy's regulation on the organization and functioning of the Financial Intelligence Unit, issued on 2 November 2022 pursuant to Article 6 of Legislative Decree 231/2007 (Figure 10.1).<sup>123</sup>

Reorganization



<sup>123</sup> Published in *Gazzetta Ufficiale*, 264, 11/11/2022. The new Regulation replaces that of 30 January 2019.

The new Information Exploitation and Technological Innovation Directorate encompasses the functions of data analysis and management, previously performed by the two pre-existing Directorates. The objective is to heighten specialization and further rationalize the Unit's IT, statistical and econometric activity. The new Directorate consists of three divisions, two of them pre-existing (the Information Management Division, taken from the Suspicious Transactions Directorate, and the Financial Flows Analysis Division, from the Regulation and Institutional Cooperation Directorate), and one newly formed, the Technological Innovation and IT Support Division. The latter takes over and amplifies some of the tasks of the Data Management Division, so as to constitute a single centre of IT competences and skills for the development of all the Unit's projects. The Regulation and Institutional Cooperation Directorate (formerly the Analysis and Institutional Relations Directorate) focuses on cooperation with the authorities and the drafting of regulations. The tasks of the old International Cooperation Division are reallocated between two new divisions: the Relations with International and European Organizations Division, which among other things coordinates activities relating to the Unit's participation in the nascent European AML Authority; and the Cooperation with Foreign FIUs Division, charged with information exchanges with counterpart FIUs abroad, including analysis and dissemination of cross-border STRs. In order to strengthen analytical activity in the face of the constantly increasing flow of STRs, the Suspicious Transactions Directorate has been enlarged by the addition of Suspicious Transactions Division IV.

The new organization will enable the Unit to more effectively discharge the tasks stemming from the growth in the various types of reporting flow (suspicious transactions, threshold-based communications, cross-border reports), the increasing complexity of the phenomena observed, the extension of duties deriving from the changes to domestic and international regulations, and the formation of the new European AML Authority.

The Governing Board of the Bank of Italy, acting on the proposal of the Governor, appointed Enzo Serata as Director of the UIF with effect from 1 January 2023. He succeeds Claudio Clemente, who left the position at the end of 2022 after two five-year terms.

## 10.2. Strategic Plan and performance indicators

Strategic  
Plan, 2020-2022

The Strategic Plan for 2020-22 was completed, with full attainment of all the objectives.

In the course of the three years the Unit carried out an intensive programme of activity affecting all its IT infrastructures and applications. The work succeeded in improving the performance of the applications and reinforcing the safeguards for data confidentiality, integrity and accessibility.

The Unit also created a system for the automatic classification of suspicious transaction reports, which will be integrated into the renewed interface of RADAR (see Section 10.4, 'IT resources'). Work continued on full exploitation of the database drawn from threshold-based communications, which serves to support financial analysis and studies designed to identify new money laundering and terrorist financing risk contexts (see the box 'Studies on threshold-based communications' in Section 5.1).

In the course of the year the Unit reviewed its method for assessing the riskiness of the STRs submitted, and from the start of 2023 it began periodically informing reporting entities of the outcomes of these analyses (see Section 1.3, 'The quality of active cooperation'). Consideration is being given to ways to amplify and further improve this feedback.

The UIF participates, in international forums, in the definition of shared standards that will allow automated acquisition of data flows deriving from cooperation with foreign FIUs, with a view to more efficient use of resources and better automation of serial processes.

The Unit has now published its strategic plan for 2023-25. It sets new objectives taking account of the setting in which the Unit acts, which is highly dynamic both as regards regulatory evolution and as regards the framework of risks and operating conditions.

**Strategic Plan  
2023-25**

For prompt and effective handling of all the reports submitted, whose number can only be expected to grow further, the UIF will revise the procedures and methodologies of automatic classification, of selection, and of analysis; the aim is to foster integration with strategic analysis for the detection of operations at risk of money laundering. Renewal of the RADAR infrastructure will be completed, and it will be integrated with foreign data, counting on modularity and flexibility to allow it to adapt faster to changing analytical needs and processes.

**Operational  
analysis**

A key objective for these three years is improving the quality of STRs, to be attained through regular dialogue with the reporting entities and the enrichment of the UIF's feedback both as regards individual reports and as regards active cooperation overall, as well as through proportionate control activity.

**Enhancing the  
quality of STRs**

The new plan calls for stepping up cooperation with the judiciary and with investigative bodies, including support to ensure that their respective IT systems evolve synergically so that the exchange of data flows becomes still richer and modulated according to their respective exigencies. The UIF also intends to raise the level of cooperation with a broad range of authorities competent in complementary sectors, and to renew its commitment to strengthening the safeguards for the confidentiality of the data at its disposal, in collaboration with the other authorities.

**Collaboration with  
other  
authorities**

An additional high-priority objective is upgrading the Unit's communications on activity, results, risks and proposals, by means of information initiatives and publications that serve to heighten its accountability and disseminate greater awareness of the UIF's role and the achievements of its AML prevention apparatus.

**Data and  
information  
for  
accountability**

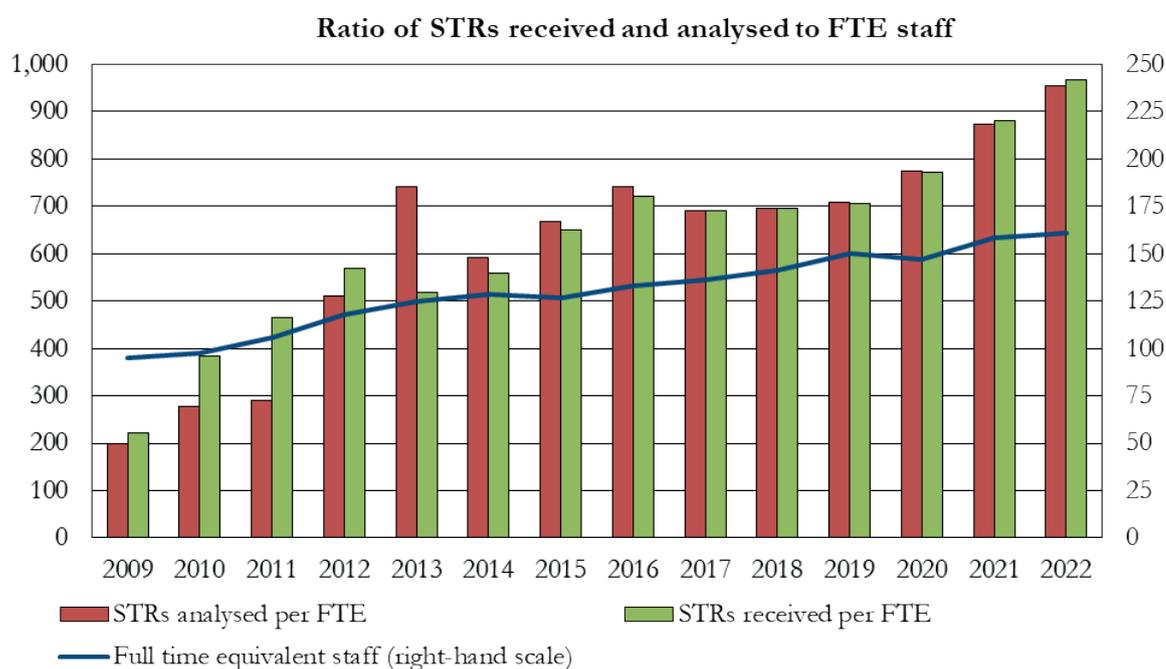
The systematic reform of the European institutional and regulatory framework, and notably the creation of the AML Authority, necessitates stepped-up international engagement on the part of the UIF, which the Unit will handle thanks to the internal reorganization already carried out, with the creation of a new division responsible for relations with the AMLA (see Section 10.1, 'Organization'). The UIF will continue to play an incisive role in designing the new European institutional system, through active participation in the negotiations and the work of the FIUs' Platform, the precursor to the nascent Support and Coordination Mechanism for FIUs, as well as in the implementation of the new European rules in Italy.

**International  
activity**

Still on the international front, the UIF has set the objective of improving and capitalizing on the instruments of cooperation with foreign FIUs, notably thanks to a new, dedicated base unit and the development of new methods and tools for analysis, including massive analysis, of cross-border reports.

In 2022 the Unit's performance indicator rose to 954 STRs analysed per full time equivalent staff member (FTE), an increase of 9.2 per cent by comparison with 2021 (Figure 10.2).

Figure 10.2



The total number of days worked by UIF staff declined by 1.1 per cent on the year, following growth of 6.2 per cent in 2021. Given the appreciable increase in the number of STRs received, the backlog of those still being processed remained extremely small (6,264 at the end of the year, or 48.4 per cent of the monthly flow, as against 37.5 per cent in 2021).

### 10.3. Human resources

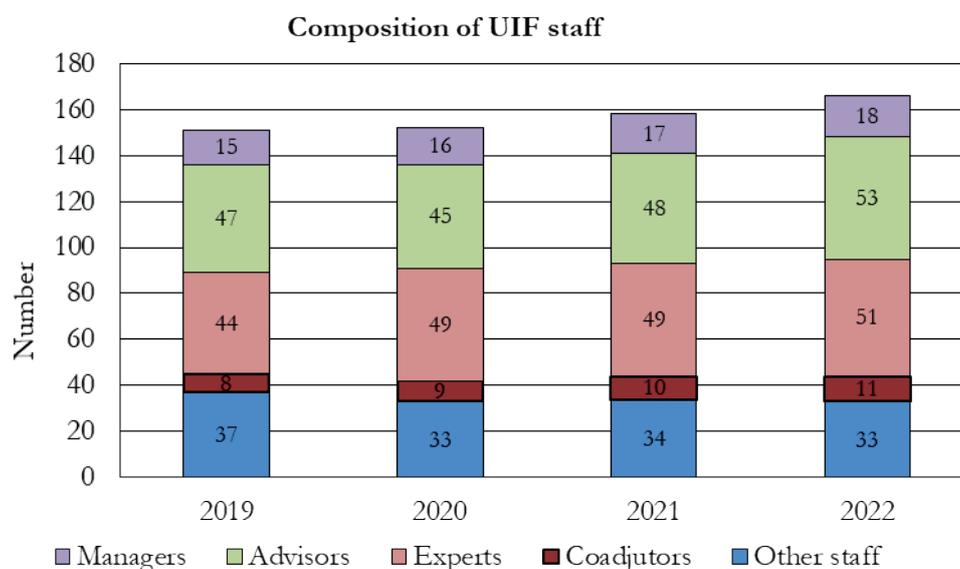
At the end of 2022 UIF staff numbered 166, excluding the Director and Deputy Director, an increase of eight over the previous year as a result of five departures and thirteen additions – nine new hires and four transfers from other Bank of Italy departments. (Figure 10.3). The average age of the personnel was essentially unchanged at 45.

At the end of the year, 96 staff members were assigned to the Suspicious Transactions Directorate (91 in 2021) and 68 to the Analysis and Institutional Relations Directorate (65 in 2021).

The shortfall from the staffing level of 172 called for in the Strategic Plan for 2020-22 was entirely made good in the first few months of 2023, in part with a view to the expected expansion under the new plan for 2023-25, which should bring total staff to 190.

The Unit resorts on a routine basis to the hybrid work mode in accordance with the model instituted by the Bank of Italy, in which remote working co-exists and is integrated with working in person. In the course of 2022 the entire staff made ample use of remote working, which accounted for 51 per cent of the total, on average, as against 69 per cent in 2021.

Figure 10.3



The UIF pays close attention to the training of new staff and refresher courses for existing staff, with the development of their technical-professional knowledge and skills. In 2022 the Unit organized five internal training initiatives for the entire UIF staff and two meetings open also to outside participants.

#### Training

In November 2022 the UIF held a seminar on the AML rules that apply to auction houses, art galleries and antiques dealers, in order to share experiences in this area with the authorities and provide an opportunity for encounter with the private sector focusing on the obligations laid down by those rules: contacts with these operators had brought out grave deficiencies of communication as regards money laundering.<sup>124</sup> The seminar examined the difficulties for practical application of the obligations of customer due diligence, data storage and reporting of suspicious transactions. The findings of the analysis of suspicious transactions in the art trade were set forth.

Also in November, the Unit, together with the Bank of Italy's Anti-Money Laundering Supervision and Regulation Unit and other departments, held a round table entitled *Verso un nuovo sistema antiriciclaggio europeo. L'AMLA quale Supervisore e quale Meccanismo delle FIU* ("Towards a new European AML system. The AMLA as supervisor and FIUs mechanism"). The gathering focused on the expected impact of the institution and working of the AMLA and on initiatives for effective participation and contribution to the new system.

The UIF also participated in a number of initiatives held by the Bank of Italy (79 events for 98 UIF staff members) and by other entities, some of them international, aimed at strengthening skills and competence on questions of institutional interest and imparting knowledge on emerging issues.

#### 10.4. IT resources

The advancement and extension of the Unit's IT tools continues in close coordination with the Bank of Italy's Directorate General for Information Technology. This activity exploits the new opportunities opened up by technological advances, especially in the fields of big data and artificial intelligence. Starting in the last quarter of 2022, increasingly ample

<sup>124</sup> UIF, *Annual Report for 2021*, p. 65.

versions of the new RADAR interface have been made available to a group of users (with a range of roles in the analytical process) in order to validate its features and obtain feedback to help improve users' experience.

This initial phase confirmed the potential of the new graphic interface and the possibility of optimizing the various phases of the process of financial analysis. The constant interaction between users and system developers, thanks among other things to the utilization of innovative development techniques, has made it possible to create a system that conforms constantly to users' needs and to resolve any malfunctions immediately. The interface version that can support all the phases of the report analysis process will be released to all users within the next few months.

#### **New system for identity resolution**

The Unit has begun work on a new system for the resolution of identities, with the aim of forming a central register of the persons and accounts contained in the data flows received.

The project calls for the total renewal of the name matching engine, for the prime purpose of efficient handling of the ever-growing volume of the flows from different sources and more effective processing of name variants, reducing the number of dubious cases that require examination by the analysts. The system can count on special functions to improve the accuracy of matching also in the case of transliteration of names written originally in different alphabets (for example, Arabic and Chinese). It also envisages the creation of new interface functions to simplify consultation of the name links between reports and also with the other databases at the analysts' disposal, facilitating the identification of contexts at risk of money laundering or terrorist financing.

#### **Automatic classification**

During the year the Unit created a system for calculation and consultation of a vast set of indicators which, based on the data in STRs and other data sources, offer a composite indication for the possible classification and mode of handling of the reports. In addition, with reference to the STRs for special sectors (payment cards, gaming, remittances, virtual assets) an ad hoc selection system has been developed to provide a guided assessment of the STR's degree of risk (see Chapter 2, 'Operational analysis').

The interface for accessing this new set of indicators was designed and developed with the aim of creating a single virtual space capable of providing the UIF's analysis function with a comprehensive visualization of all the data processed. Internal testing has shown the new selection and classification system to be particularly well suited to certain phases of STR processing, in that it is complementary to and compatible with the procedures now in use and those under development. In the course of 2023 the new set of indicators is to be integrated into the renewed RADAR interface. For the realization of the first set of indicators, and in order to shorten development time for the new indicators under study, experimentation is under way with innovative development methodologies calling for increasingly close cooperation of UIF staff with the Directorate General for Information Technology.

#### **Graph analysis**

In 2022 the functional prerequisites for the introduction of graph analysis tools were defined. The public tender for acquisition of a graph database was completed and the fulfilment of the conditions for the contract award and the consequent product supply are under way. The Unit's analysts and technicians are now designing a graph data model that can be applied within the new system, capable of representing the complex reality of relationships emerging from all the data sources exploited for financial analysis. This year a series of tests are scheduled that will enable definition of new, more highly articulated modes of analysis applicable to reports or groups of reports embedded in broad, complex financial contexts.

As of 1 September 2022, following internal studies and the completion of a public procurement procedure in cooperation with the competent units of the Bank of Italy, the UIF's new 'System for forensic analysis of virtual assets' was made available. The project required managing a series of new elements relating to the mode of provision of the new services. In fact, the system is made available by an outside provider in public cloud, via 'software as a service' mode. This supply model offers great flexibility, reducing the costs to the client of system development and management, which are charged exclusively to the service provider, but at the same time it requires a series of special measures for the handling of information, especially as regards confidentiality. From this standpoint, the project has adhered to the policy specifications for public cloud solutions adopted by the Bank of Italy. The framework agreement with the provider not only specifies the tool for visual analysis mentioned above (see Section 2.4, 'Methodology') but envisages a tool for massive screening of transactions in virtual assets, which could be used in the future if the current growth in STRs submitted by virtual asset service providers continues, and in particular with the introduction of the register of virtual asset operators at the Organization of Agents and Mediators (see the box 'International and Italian initiatives on crypto-assets' in Chapter 9).

System for forensic analysis of virtual assets

Last year saw a series of interventions on the system for data exchanges with other organizations (SAFE), which improved the logic used in matching data, reinforced monitoring of the status of requests and expanded the set of functions of the portal available to the judiciary. Additional changes scheduled by the end of 2023 include adaptation of interfaces to the standards of the RADAR environment, easier modes of access to the portal, and a dedicated channel for the exchange of confidential information.

SAFE procedure

With the takeover of management of FIU.NET by the European Commission in September 2021 (see Section 8.4, 'Developments in the FIU.NET'), the operation and maintenance of the platform were reviewed in order to attain higher levels of service and stricter security standards. This entailed stepped-up interaction between the Commission's technical structures and the local officers responsible for planning and execution of interventions. More specifically, the software components of the platform are now updated monthly. In September 2022 a data cleaning operation eliminated the non-essential data accumulated over the years and made it possible to upgrade the platform's performance.

FIU.NET Platform

Streamlined, more secure modes of connection with the Egmont Secure Web were introduced in 2022 (see Section 8.7, 'Participation in other international organizations'), which can now be accessed from IT work stations either in person or remotely. Within the Egmont Group, in collaboration with the Bank of Italy's Directorate General for Information Technology, the UIF takes part in work on the new platform based on services provided via public cloud, helping to orient project choices and seeking to assess their impact on the UIF itself, not least with a view to interoperability with internal systems.

Egmont Secure Web

In April 2022 Infostat made available a new database of reports on deposits traceable to Russian and Belarusian nationals (DEPRU), introduced by Regulations EU/2022/328 and EU/2022/398, in whose regard the CSF, in its sessions of 3 and 16 March 2022, delegated the UIF to receive and store the data. Further interventions to the IT procedure enabled acquisition also of the additional data specified in Regulation EU/2022/2474 of 16 December 2022 (see Section 8.8, 'Activity relating to the war in Ukraine').

DEPRU

## 10.5. External communication

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, market operators and the

professions. A year ago, on the occasion of the presentation of the *Annual Report for 2021*, the initiative ‘UIF meets the reporting entities’ was resumed, in this case dedicated specifically to active cooperation in the area of gaming and payment cards (see Section 1.3, ‘The quality of active cooperation’).

To bring the issues of prevention of money laundering and terrorist financing to the attention of an ever broader public, the UIF continues its online publication of *Quaderni dell’antiriciclaggio* on AML topics, divided into two series: ‘Statistics’ and ‘Analysis and studies’. In addition, a periodic ‘Newsletter’ offers succinct updates on the UIF’s activities and the main developments in AML issues.

In the course of 2022, the UIF continued its work to heighten awareness of the reporting requirements in the general public and among the various classes of obliged entities, taking part in more than 50 events (conferences, seminars and meetings) with national and supranational authorities on issues involved in countering money laundering and terrorist financing.

## GLOSSARY

### Accredited entities and agents

Pursuant to Article 1(2)(nn) of Legislative Decree 231/2007, these 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 Consolidated Law on Banking, 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 in Italy.

### Administrations and bodies concerned

Pursuant to Article 1(2)(a) of Legislative Decree 231/2007, these are the bodies responsible for supervising obliged entities not supervised by sector-specific authorities, i.e. the administrations, including tax offices, those with powers of inspection or authorized to grant concessions, authorizations, licenses or other enabling documents, however denominated, with respect to obliged parties, and the bodies responsible for verifying the possession by such parties of the requisites of professionalism and integrity as prescribed by the relevant sectoral rules. For the sole purposes set out in the aforesaid decree, the category of administrations concerned includes: the Ministry of Economy and Finance, in its capacity as the authority responsible for supervising auditors and auditing firms with no mandate to audit public-interest bodies or bodies under an intermediate regime; and the Ministry of Economic Development, in its capacity as the authority responsible for the supervision of trust companies not listed in the register referred to in Article 106 of the TUB.

### Anti-Mafia Investigation Department (Direzione Investigativa Antimafia - DIA)

A specialized interforce investigative bureau with jurisdiction throughout Italy. Instituted within the Ministry of the Interior's Department of Public Security by Law 410/1991, it has the exclusive task of ensuring the coordinated conduct of preventive investigations into organized crime, in all of its forms and connections, and of carrying out judicial police investigations into crimes of mafia-like association or crimes related thereto.

### Beneficial owner

Pursuant to Article 1(2)(pp) of Legislative Decree 231/2007, the natural person or natural persons, other than the customer, in whose interest, ultimately, 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 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 in Italy 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 anti-money laundering safeguards, as identified by the FATF in public statements issued three times a year. Based on these assessments ([High-Risk Jurisdictions subject to a Call for Action – February 2023](#) and [Jurisdictions under Increased Monitoring – February 2023](#)) as of March 2023 the following countries were not aligned with the legislative and regulatory provisions against money laundering and terrorist financing: Albania, Barbados, Burkina Faso, Cayman Islands, Democratic Republic of the Congo, Democratic Republic of Korea, Gibraltar, Haiti, Iran, Jamaica, Jordan, Mali, Mozambique, Myanmar, Nigeria, Panama, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Turkey, Uganda, United Arab Emirates and Yemen.

### Cross-border report

This term refers to suspicious transaction reports received from an EU FIU that concern another Member State and which, pursuant to Article 53(1) of the Fourth Directive, must be forwarded promptly to the relevant counterparties. These reports are identified based on a methodology developed within the EU FIUs Platform.

### **Designated entities**

Pursuant to Article 1(1)(l) of Legislative Decree 109/2007 designated entities means natural persons, legal persons, groups and entities designated as being targeted by asset freezes 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 natural or legal persons that provide professional services to third parties, including online services, for the safeguarding of private cryptographic keys 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 extend its benefits. The number of participating FIUs has grown steadily over time. 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 Units (FIUs)**

Central national units 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, terrorist financing and the related predicate offences, and disseminating their findings. A country's legislation may designate its FIU as an administrative authority, a specialized structure within a police force or as part of the judiciary. Some countries have adopted a mix of these models.

### **Financial Security Committee (FSC)**

Pursuant to Article 3 of Legislative Decree 109/2007, this committee was established at the Ministry of Economy and Finance (MEF). It is chaired by the Director General of the Treasury and composed of 15 members and their respective deputies, appointed by decree of the Minister of the Finance and Economy, on the basis of the nominations made, respectively, 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 UIF. The Committee also includes an official in service at the MEF, an officer of the Guardia di Finanza (Finance Police), an executive-level official or police officer of equivalent rank under Article 16 of Law 121/1981, in service at the Anti-Mafia Investigation Department, an officer of the Carabinieri, a manager of the Customs and Monopolies Agency and a magistrate serving in the National Anti-Mafia Directorate. For asset freezes, the Committee is supplemented by a representative of the State Property Agency. The entities represented on the FSC communicate to the Committee, also by way of derogation from any provisions on official secrecy, the information in their possession relevant to matters within the Committee's competence. In addition, the judicial authorities transmit any information deemed useful for combating the financing of terrorism and the proliferation of weapons of mass destruction. With the entry into force of Legislative Decree 231/2007, the Committee's competences, initially limited to coordinating action against the financing of terrorism, were extended to the fight against money laundering (see Article 5 paragraphs 5, 6 and 7 of Legislative Decree 231/2007).

### **Financing of terrorism**

Pursuant to 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 to commit such crimes.

### **Financing of weapons of mass destruction proliferation programmes**

Pursuant to Article 1(1)(e) of Legislative Decree 109/2007, the financing of weapons of mass destruction proliferation programmes refers to the supply 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**

An infrastructure for communication among the Financial Intelligence Units of the European Union that enables structured, multilateral sharing of information, ensuring standardized implementation, promptness and security of 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, location, 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 entities responsible for tax collection at national or local level, regardless of their legal form.

### **High-risk third countries**

Pursuant to Article 1(2)(bb) of Legislative Decree 231/2007, these are non-EU countries whose legal systems exhibit strategic deficiencies in their national AML/CFT systems, as identified by the European Commission with Delegated Regulation EU/2016/1675 and subsequent amendments, in the exercise of the powers referred to in 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: Afghanistan, Barbados, Burkina Faso, Cambodia, Cayman Islands, Democratic Republic of the Congo, Democratic Republic of Korea, Gibraltar, Haiti, Iran, Jamaica, Jordan, Mali, Morocco, Mozambique, Myanmar, Panama, Philippines, Senegal, South Sudan, Syria, Tanzania, Trinidad and Tobago, Uganda, United Arab Emirates, Vanuatu and Yemen, (see [Delegated Regulation EU/2023/410 of 19 December 2022](#)).

### **Laundering and investment of money, assets or utilities of illegal provenance**

Article 648-bis of the Penal Code makes punishable for the crime of money laundering anyone who, apart from cases of complicity in the predicate offence, ‘substitutes or transfers money, assets or other utilities 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, apart from the cases of complicity in the predicate offence and the cases specified in Article 648 and 648-bis, ‘invests money, assets or other utilities deriving from crime in economic or financial assets.’ With reference to both crimes, Legislative Decree 195/2021 extends the liability for punishment to cases regarding ‘money or things deriving from a violation punishable with detention for a period of between a maximum of one year and a minimum of six months.’ 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 abetting 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, holding or use of property, carried out in the knowledge 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 under the preceding subparagraphs, association with others to perpetrate such actions, attempts to perpetrate them, the act of abetting, instigating or advising someone to commit them or the fact of facilitating their performance.

### **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 available instrument making it possible to transfer, move or acquire, including by electronic means, funds, valuables or financial assets.

### **Moneyval (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 is the body responsible for the Council's anti-money laundering policies, also taking into account the measures adopted by the FATF, and makes specific recommendations to the member countries on the matter. It evaluates the anti-money laundering measures adopted by Council of Europe member countries other than FATF members. It holds FATF Associate Member status as a regional group. Under a thoroughly revised charter, Moneyval has served since January 2011 as an autonomous Council of Europe monitoring body on AML/CFT, reporting directly to the Committee of Ministers, to which it submits its annual report.

### **National Anti-Corruption Authority (Autorità Nazionale Anticorruzione - ANAC)**

Pursuant to 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 investee companies and subsidiaries, including through the implementation of transparency in all aspects of management, as well as supervision with regard to public contracts, appointments and whatsoever sector of public administration that could potentially be subject to corruption. In the execution of its mandate, it must avoid making procedures overly burdensome, with negative effects on individuals and businesses, and guide the behaviour and activities of public employees with interventions in advisory and regulatory frameworks, 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 Decree Law 367/1991, converted with amendments into Law 8/1992, is tasked with national coordination of investigations of organized crime. Its competence was extended to cover terrorism proceedings, including international ones, by Decree Law 7/2015, converted with amendments into Law 43/2015. Pursuant to Article 103 of Legislative Decree 159/2011, the Directorate is headed by a magistrate with the functions of national Public Prosecutor and two magistrates with functions of assistant prosecutors, together with, as their deputies, magistrates chosen from among those who have performed, even if not continuously, the functions of public prosecutor for at least ten years and have specific aptitude, organizational skills and experience in handling proceedings involving organized crime 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, Anguilla, Bahamas, British Virgin Islands, Costa Rica, Fiji, Guam, Marshall Islands, Palau, Panama, Russia, Samoa, Trinidad and Tobago, Turks and Caicos Islands, United States Virgin Islands and Vanuatu (Conclusions of the Council of 24 February 2023).

### **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 states, 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 referred to in Article 128-undecies of the TUB (Consolidated Law on Banking). The OAM also keeps: i) the register of foreign exchange dealers, which has a special section for virtual currency service providers (Article 17-bis, paragraph 8-bis, of Legislative Decree 141/2010, introduced by Legislative Decree 90/2017 and amended by Article 5(1)(a) of Legislative Decree 125/2019); ii) the register of affiliates and agents referred to in Article 45 of Legislative Decree 231/2007; and iii) the register of cash-for-gold dealers referred to in 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 hold or have ceased to hold important public offices for less than one year, as well as their family members or persons known to be their close associates, as listed below: 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, Regional Executive Board Member, Mayor of a provincial capital or metropolitan city, Mayor of a municipality with a population of not less than 15,000 inhabitants, and similar positions in foreign states; 1.2 member of the national parliament, senator, member of the European Parliament, regional councillor and similar positions in foreign states; 1.3 member of the central governing body of a political party; 1.4 Constitutional Court judge, magistrate of the Court of Cassation or the Court of Auditors, State Councillor and other members of the Administrative Justice Council for the Region of Sicily, and similar positions in foreign states; 1.5 member of the governing bodies of central banks and independent authorities; 1.6 ambassador, chargé d'affaires or equivalent positions in foreign states, senior officer of the armed forces or similar positions in foreign states; 1.7 member of the administrative, management or control bodies of enterprises controlled, including indirectly, by the Italian State or by a foreign state or majority or wholly-owned by regional governments, by provincial capitals and metropolitan cities and by municipalities with a total population of not less than 15,000 inhabitants; 1.8 general manager of a Local Health Authority or public hospital, university hospital and other National Health Service entities; 1.9 director, deputy director, member of the management board or person performing equivalent functions in international organizations; 2) family members of politically exposed persons include: parents, spouse or person linked in civil union or de facto cohabitation or comparable relationship to the politically exposed person, their children and their spouses as well as persons linked to their children in civil union or de facto cohabitation or comparable relationships; 3) persons who are known to be close associates of politically exposed persons include: 3.1 natural persons linked to politically exposed persons by joint effective 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 de facto in the interest and for the benefit of a politically exposed person.

### **Sectoral supervisory authorities**

Pursuant to Article 1(2)(c) of Legislative Decree 231/2007, these are: the Bank of Italy, CONSOB and IVASS as authorities responsible for the supervision and control of banking and financial intermediaries, auditors and audit firms with mandates to audit public-interest entities and entities subject to intermediate regimes; and the Bank of Italy in respect of non-financial operators that carry on the activity of safekeeping and transport of cash and securities or valuables by means of sworn security guards, have the licence referred to in Article 134 of the TULPS (Consolidated Law on Public Security), limited to handling of euro banknotes, and are included in the list referred to in Article 8 of Decree Law 350/2001, converted with amendments into Law 409/2001.

### **Self-laundering**

Pursuant to Article 648-ter.1 of the Italian Penal Code, 'whoever, having committed or abetted an offence with criminal intent, uses, replaces or transfers money, assets or other utilities deriving from the commission of such offence to economic, financial, entrepreneurial or speculative activities in such a way as to materially hinder detection of their criminal origin' shall be punished for the offence of self-laundering. This provision was introduced by Article 3(3) of Law 186/2014, most recently amended by Article 1(1)(f) of Legislative Decree 195/2021.

### **Self-regulatory bodies**

Pursuant to Article 1(2)(aa) of Legislative Decree 231/2007, these are representative bodies designated by professional associations, including their territorial branches and the disciplinary board, on which the legislation in force confers powers of regulation, supervision, control of compliance with the rules governing the exercise of the profession and the imposition, through the bodies instituted for that purpose, of the sanctions envisaged

for their infringement.

### **Special Foreign Exchange Unit (Nucleo Speciale di Polizia Valutaria - NSPV)**

Formed as a unit of the Finance Police (Guardia di Finanza), it operates in the fight against money laundering, both as an investigative police body and as an administrative body responsible, together with the Bank of Italy and the Anti-Mafia Investigation Department, for controls on the financial intermediation sector.

### **Standardized archives**

Archives through which the data and information envisaged by the provisions issued by the competent sectoral supervisory authorities pursuant to Article 34(3) of Legislative Decree 231/2007 are made available, in accordance with the technical standards and the analytical reasons referred to therein. They include the Single Electronic Archives (Italian acronym: AUI) 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**

Countries and territories listed in the so-called black list contained in the Decree of the Minister of Finance of 4 May 1999 (most recently amended by the Ministerial Decree of 12 February 2014): Andorra, Anguilla, Antigua and Barbuda, Aruba, Bahamas, Bahrain, Barbados, Belize, Bermuda, Bonaire, British Virgin Islands, Brunei, Cayman Islands, 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, Maldives, Malaysia, the Marshall Islands, Mauritius, Montserrat, Nauru, Niue, Oman, Panama, Philippines, Principality of Monaco, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, Seychelles, Singapore, Sint Eustatius and Saba, Sint Maarten -- Dutch Part, Switzerland, Taiwan, Tonga, Turks and Caicos, Tuvalu, United Arab Emirates (Abu Dhabi, Ajman, Dubai, Fujairah, 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 transferring value through the use of commercial transactions in an attempt to legitimize the illicit origin of the proceeds.

### **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)
AMLA	Anti-Money Laundering Authority
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
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)
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
EPPO	European Public Prosecutor's Office
EMI	Electronic Money Institution
EPPO	European Public Prosecutor's Office
ESA	European Supervisory Authority
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force
FSC	Financial Security Committee
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

MENAFATF	Middle East and North Africa Financial Action Task Force
NRA	National Risk Assessment
NRRP	National Recovery and Resilience Plan (Piano Nazionale di Ripresa e Resilienza - PNRR)
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
PEP	Politically Exposed Person
PI	Payment Institution
RADAR	Collection and Analysis of AML Data (Raccolta e Analisi Dati AntiRiciclaggio)
ROS	Special Operations Group of the Carabinieri
SACE	Italian Export Credit Agency (Servizi assicurativi del commercio estero)
SARA	Aggregate AML Reports (Segnalazioni AntiRiciclaggio Aggregate)
SGR	Asset management company
SICAF	Fixed capital investment company
SICAV	Variable capital investment company
SIM	Securities investment firm
SNA	AML Supervision and Regulation Unit (Unità di Supervisione e normativa antiriciclaggio)
STR	Suspicious Transaction Report
TFEU	Treaty on the Functioning of the European Union
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
UNODC	United Nations Office on Drugs and Crime
VASP	Virtual Asset Service Provider
VAT	Value Added Tax
VD	Voluntary Disclosure
WMD	Weapons of Mass Destruction