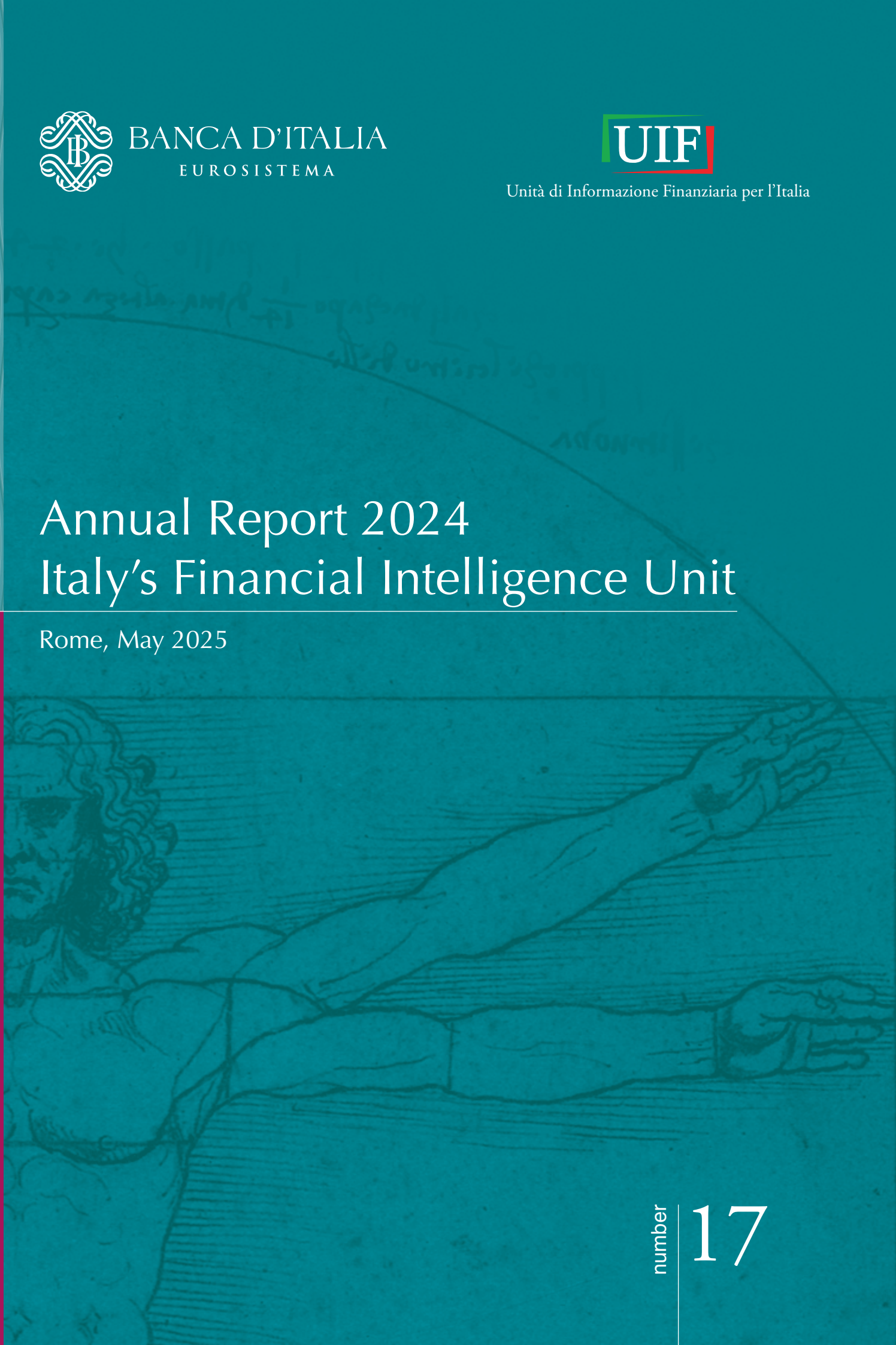
BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2024
Italy's Financial Intelligence Unit

Rome, May 2025



year 2024

number 17

BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

Annual Report 2024
Italy's Financial Intelligence Unit

Rome, May 2025

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.

Unità di Informazione Finanziaria per l'Italia

Director
Enzo Serata

Address
Largo Bastia, 35 – 00181 Roma – Italia

Telephone
+39 0647921

Website
https://uif.bancaditalia.it

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

Designed by the Printing and Publishing Division of the Bank of Italy, June 2025

CONTENTS

List of boxes

FOREWORD

In 2024, the decline in suspicious transaction reports (STRs) observed in the previous year was confirmed. The decreasing number of reports from banks and Poste Italiane, the main reporting entities, was partly offset by an increase in reports submitted by professionals, as well as by a significant rise in STRs from some payment institutions (PIs) and electronic money institutions (EMIs) recorded in the final quarter. Notable increases in reports submitted by virtual asset operators and by entities engaged in gold trading or in the manufacture and sale of precious items were observed among non-financial obliged entities. Reports from gaming service providers remained substantial, although in decline, while those from companies involved in the custody and transport of valuables almost halved. The reporting flow from public administrations also continued to grow, albeit still marginally and limited to a small number of entities. Reports relating to terrorist financing showed an increase.

The reduction in reporting volumes also reflected the numerous initiatives undertaken by the UIF to improve the quality of active collaboration; this correlation is clear in the marked decrease in STRs analysed in 2024 and deemed as having a low risk of money laundering, which dropped from 25 per cent the previous year to 20 per cent. Alongside the improvement of the system for monitoring the quality of active collaboration, 2024 also saw further fine-tuning of the new feedback forms, which were the subject of consultation with the main reporting entities. These new forms will be based on a wide set of indicators focusing on innovative qualitative aspects and will become the primary tool for engaging with reporting parties on the outcomes of quality monitoring in a constructive way. The decline in the number of STRs was more than offset by an increase in the complexity of the cases reported and in the volume of data and information included in the reports. This trend impacts the techniques used for analysis, with (a growing prevalence of) methods that allow full exploitation of the UIF's information assets, and the approaches to aggregate and network analysis becoming more widespread.

The money laundering schemes identified through STR analysis are increasingly complex and often characterized by intensive cross-border operations, including those carried out through innovative financial channels and instruments, and sometimes involving intermediaries and operators established and active in jurisdictions that permit regulatory arbitrage. These schemes are designed to hinder the detection of criminal activities, the persons involved, and the destination of illicit proceeds, and are particularly frequent in cases relating to tax offences and in traditional risk areas such as the misuse of public funds, corruption, and organized crime, which continue to feature prominently in the STR flows. The widespread use of technology influences the type of cases reported by STRs, with a growing prevalence of cyber fraud and the ongoing evolution of the methods for using crypto-assets for money laundering purposes.

Threshold-based communications on cash transactions showed a slight decrease in the number of operations compared with 2023, while the average amounts remained stable. SARA data confirm that unusual uses of cash were more concentrated in the provinces of Central and Northern Italy in 2024 as well. Both incoming and outgoing bank transfers involving tax havens or non-cooperative countries fell sharply, mainly due to a change in the composition of the countries classified as being at risk compared with the previous year. The value of advance declarations for the transfer of gold carried abroad recorded a significant increase, as did the value of ex-post declarations, largely linked to trends in gold prices.

As part of strategic analysis, the study of criminal infiltration into the legal economy continued, while a study that provides a conceptual framework to explain and classify the

underlying motivations behind organized crime infiltration into the economic fabric was finalized in the public administration and an algorithm for estimating the risk of mafia infiltration into local authorities was developed. A machine learning algorithm is currently being tested to identify STRs potentially relating to child pornography cases. Significant improvements were made to IT and analytical tools in order to reduce manual tasks, ensure data confidentiality and make applications more aligned with methodological, regulatory and technological developments. Information exchanges with Investigative Bodies and the National Anti-Mafia Directorate (DNA) were made even more secure.

The UIF's inspection activity among non-financial operators identified issues in the gaming sector, particularly online gaming. Controls on gold sector reporting entities also revealed shortcomings in anti-money laundering safeguards and in awareness of legal obligations; the Unit carried out targeted awareness-raising initiatives for operators in the sector.

Requests for information from judicial authorities and investigative bodies decreased slightly, although they involved a marginally higher number of STRs than in 2023. In July 2024, the Finance Police and UIF signed a new Memorandum aimed at strengthening cooperation, particularly through coordination of inspection activities, in order to focus their efforts on sectors and phenomena posing higher risks.

Information exchanges with foreign Financial Intelligence Units (FIUs) remained substantial and increased compared with 2023. The quality of both requests and spontaneous disclosures received from other FIUs improved, thereby enriching the UIF's information assets and confirming the growing analytical capacity of foreign FIUs. Residual difficulties remain in the UIF's access to investigative data, due to legislative constraints. At the European level, international cooperation also benefited from cross-border exchanges; the UIF received over 65,000 STRs in 2024 and sent more than 10,000. The Unit continues to carry out the functions and tasks delegated by the Financial Security Committee (FSC) concerning international sanctions, particularly those targeting the Russian Federation. Work to update the National Risk Assessment, to which the UIF contributed within the framework of the FSC, was completed in 2024. The Assessment confirms that the risk of money laundering in Italy remains very high and identifies corruption, extortion, tax evasion and tax offences, bankruptcy and corporate crimes as being among the most significant threats to the national system.

The FATF's Mutual Evaluation of the Italian AML system began in the second half of 2024. The activity, in which the UIF is also involved, verifies both the formal compliance of the regulatory framework with international standards and the effectiveness of the measures adopted and activities performed. The launch of the European Anti-Money Laundering Authority (AMLA) and the new EU regulatory framework are giving rise to a new institutional structure that could strengthen integration between Member States in AML/CFT activities.

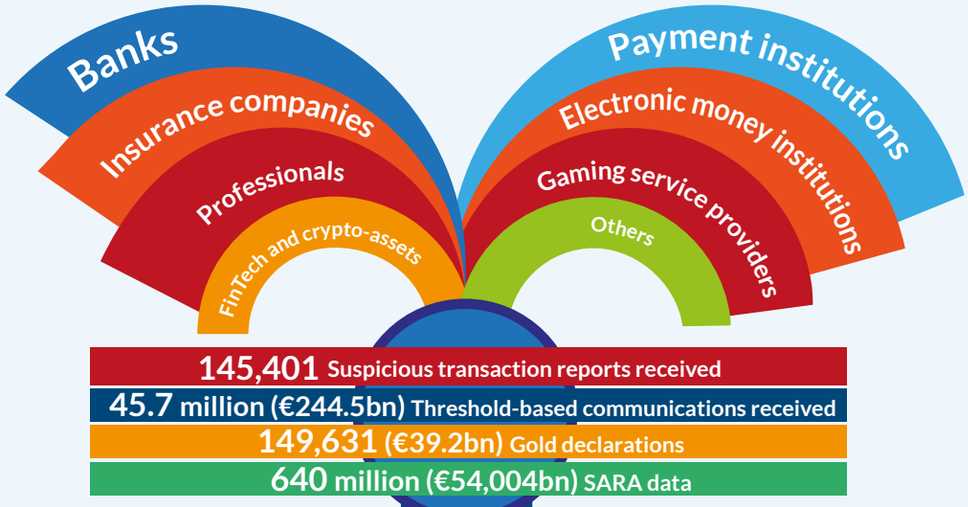
In the face of the risks arising from the global geopolitical situation and the evolution of economic and financial crime, the Unit reaffirms its commitment to playing a constructive and proactive role within the national and international anti-money laundering system, in order to continue ensuring effective prevention and enforcement in cooperation with other authorities and reporting entities, and with the valuable contribution of its staff.

The Director

Enzo Serata

ACTIVITY AT A GLANCE

Financial analysis



145,401 Suspicious transaction reports received

45.7 million (€244.5bn) Threshold-based communications received

149,631 (€39.2bn) Gold declarations

640 million (€54,004bn) SARA data

Intelligence, dissemination and controls

UIF

143,850 Suspicious transaction reports analysed

46,053 STRs on payment cards, crypto-assets, gaming and money transfer transactions assessed using aggregate analysis

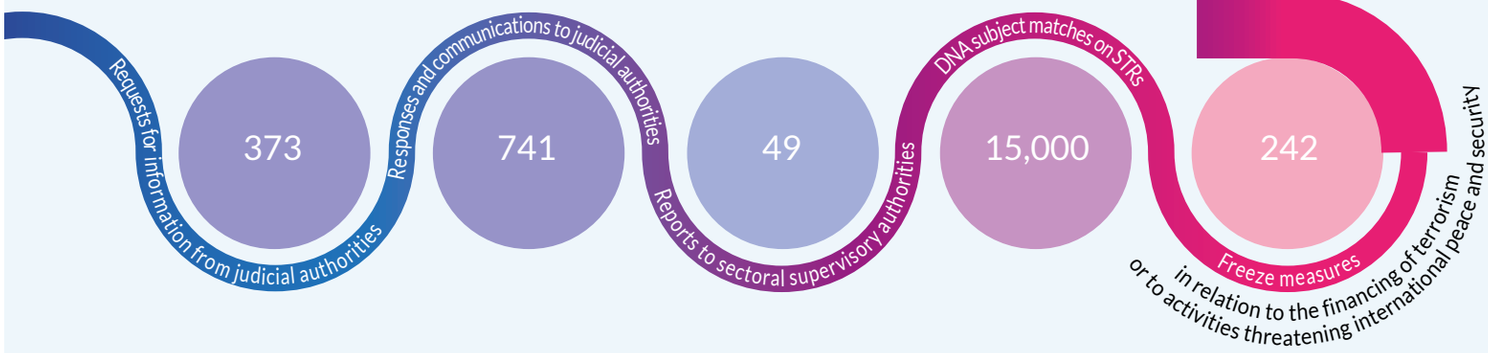
188 Suspicious transactions examined with a view to suspension

28 Suspension orders

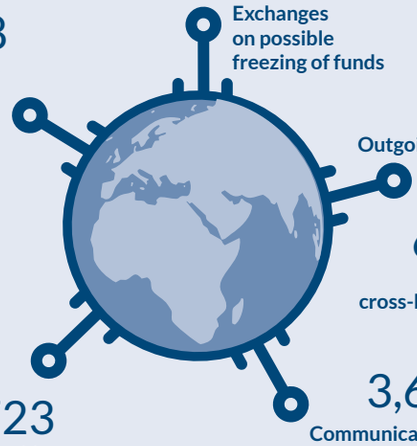
24 Inspections and off-site controls

20 Sanction procedures

Cooperation with national investigative bodies and authorities



FOREIGN FIUs



122
Exchanges on possible freezing of funds

1,508
Requests and spontaneous communications received

10,267
Outgoing cross-border report and disseminations

65,692
Incoming cross-border reports

3,619
Communications of foreign FIUs sent to investigative bodies

723
Requests sent to other FIUs

DISSEMINATION

of knowledge about money laundering

14
Speakers at international conferences and workshops

46
Speakers at conferences and workshops held by Italian institutions

31
Training interventions at regional bodies and other general government offices

19
UIF publications and contributions to scholarly journals

Secondary legislation and UIF communications

2024

June

IVASS Communication
Amendments and additions to Regulation 2019/44

November

Bank of Italy Measure
On the organization, procedures and internal controls aimed at preventing the use of intermediaries for the purposes of money laundering and terrorist financing

December

UIF and Bank of Italy Communication
On anti-money laundering requirements regarding virtual IBANs

2025

January

UIF Communication
News on gold declarations

February

UIF Communication
Clarifications on gold declarations

IT Infrastructure

Analysis IT environment
New indicators (financial ranking, link rating, neutral subjects)
Support for the definition of STRs operational framework

Analysis tools
Graph DB
Identity resolution system

Innovation
Testing of machine learning algorithms in databases with high levels of data protection

Automation and support
Automation of suspension proceedings
Data exchange between the UIF and the Ministry of the Interior on Russians transfers

Security
Management of STRs on Politically Exposed Persons (PEP)
Implementation of the Memorandum of Understanding UIF-DNA-DIA- Finance Police

1. SUSPICIOUS TRANSACTION REPORTS

1.1. Reporting flows

The number of suspicious transaction reports received by the UIF decreased by 3.3 per cent in 2024, confirming the reduction recorded in 2023 (see Table 1.1). This contraction in the overall flow was associated with a lower percentage of STRs with a low risk of money laundering (see Section: 'The quality of active cooperation').

Table 1.1

Reports received					
	2020	**2021**	**2022**	**2023**	**2024**
Number of reports	113,187	139,524	155,426	150,418	145,401
Percentage change on previous year	*7.0*	*23.3*	*11.4*	*-3.2*	*-3.3*

Reporting entities

The category comprising banks and Poste Italiane recorded a 9.4 per cent decrease compared with 2023, while continuing to represent the sector from which the highest number of STRs originates. Conversely, a significant increase in the number of reports submitted by professionals (+27.9 per cent), primarily notaries, was observed. Although financial intermediaries other than banks also showed an overall decline in the number of reports during the year, the last quarter of 2024 recorded a marked increase in STRs submitted by electronic money institutions (EMIs), payment institutions (PIs) and their respective EU points of contact, with a notable rise compared with previous months. The sector of non-financial operators displayed a substantial increase in the number of STRs submitted – almost double compared with 2023 – mainly attributable to virtual asset operators (+168.0 per cent), also due to the considerable contribution of new reporting entities active in the sector, and to gold traders or manufacturers and retailers of precious items (+76.6 per cent). The decrease in reports from entities providing custody and transport of valuables services continued (-46.2 per cent), and the STRs from gaming service providers declined (-20,6 per cent). Public administrations submitted 1,264 reports, confirming the upward trend, which nonetheless remains marginal and limited to a small number of entities (Table 1.2).

In the first four months of 2025, the number of STRs received stood at 53,446, marking a 16.3 per cent increase compared with the same period in 2024. The number of STRs analysed rose by 17.1 per cent.

Suspicious transaction reports

The number of STRs relating to terrorist financing amounted to 340, up by 43 compared with 2023 (see 'Combating the Financing of Terrorism' in Chapter 3). Reports associated with the financing of programmes for the proliferation of weapons of mass destruction remain limited in number (25 in 2024).[1]

Lombardy once again recorded the highest number of STRs in absolute terms, accounting for 19.1 per cent of the national total, followed by Lazio and Campania (Table 1.3).[2] The most significant declines were observed in the regions of Basilicata (-26.5 per cent) and Calabria (-17.7 per cent). Online transactions also fell by 16.2 per cent compared with

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

[2] The territorial location of reports refers, by convention, to that of the first transaction reported in the STR.

2023. As in the previous year, most STRs related to online transactions were submitted by gaming service providers (4,509 STRs) and EMIs (4,297 STRs). Reports concerning transactions carried out abroad increased by 31.1 per cent, with a particular concentration in Lithuania (239 STRs), Germany (210 STRs), and the United Kingdom (186 STRs). In 2024, the top two provinces in terms of the number of STRs relative to population were again Milan and Prato, with between 494 and 382 reports per 100,000 inhabitants, followed by Naples and Reggio Emilia (Figure 1.1).

Table 1.2

STRs by type of reporting entity (1)

	2023		2024		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2023)*
Banking and financial intermediaries and operators	**126,125**	**83.8**	**117,982**	**81.1**	**-6.5**
Banks and Poste Italiane	82,374	54.8	74,644	51.3	-9.4
Financial intermediaries and operators	43,746	29.1	43,326	29.8	-1.0
Electronic money institutions and points of contact of EU electronic money instit.	21,025	14.0	20,513	14.1	-2.4
Payment institutions and points of contact of EU payment institutions	16,220	10.8	17,148	11.8	5.7
Insurance companies	3,604	2.4	3,219	2.2	-10.7
Financial intermediaries - Article 106 of the Consolidated Law on Banking	1,361	0.9	1,299	0.9	-4.6
Asset management companies, SICAVs and SICAFs	443	0.3	431	0.3	-2.7
Trust companies - Article 106 of the Consolidated Law on Banking	216	0.1	149	0.1	-31.0
Investment firms	64	0.0	61	0.0	-4.7
Intermediaries and other financial operators not included in the categories above	813	0.5	506	0.3	-37.8
Companies managing markets and fin. instr.	**5**	**0.0**	**12**	**0.0**	**140.0**
Non-financial obliged entities	**23,879**	**15.9**	**26,155**	**18.0**	**9.5**
Professionals	**8,090**	**5.4**	**10,345**	**7.1**	**27.9**
Notaries and National Council of Notaries	7,721	5.1	9,960	6.9	29.0
Accountants, bookkeepers and employment consultants	207	0.1	266	0.2	28.5
Auditing firms and auditors	73	0.0	48	0.0	-34.2
Law firms, law and accounting firms and law practices	42	0.0	33	0.0	-21.4
Lawyers	24	0.0	11	0.0	-54.2
Other professional service providers	23	0.0	27	0.0	17.4
Non-financial operators	**3,766**	**2.5**	**6,263**	**4.3**	**66.3**
Cash/valuables-in-transit companies	1,034	0.7	556	0.4	-46.2
Gold traders or manufacturers and retailers of precious items	1,327	0.9	2,344	1.6	76.6
Virtual asset service providers	1,181	0.8	3,165	2.2	168.0
Other non-financial operators	224	0.1	198	0.1	-11.6
Gaming service providers	**12,023**	**8.0**	**9,547**	**6.6**	**-20.6**
General government entities	**414**	**0.3**	**1,264**	**0.9**	**205.3**
Total	**150,418**	**100.0**	**145,401**	**100.0**	**-3.3**

(1) The types of reporting entities are listed in Article 3 and 10 of Legislative Decree 231/2007.

The total value of executed suspicious transactions reported to the UIF in 2024 amounted to nearly €94.0 billion (compared with €95.5 billion in the previous year). Considering also the data on transactions that were attempted but not executed (€6.5 billion, down from €7.9 billion in 2023), the overall value of the reported transactions came to €100.5 billion. The distribution of reports by amount class remained broadly unchanged, with the majority relating to transactions between €50,001 and €500,000 (Figure 1.2), followed by those in the up to €50,000 class.

Table 1.3

Distribution of STRs received by region of transaction

	2023		**2024**		
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*	*(% change on 2023)*
Lombardy	27,462	18.3	27,832	19.1	1.3
Lazio	15,872	10.6	14,615	10.1	-7.9
Campania	15,903	10.6	15,981	11.0	0.5
Veneto	10,673	7.1	10,758	7.4	0.8
Emilia-Romagna	9,834	6.5	9,781	6.7	-0.5
Piedmont	8,731	5.8	8,041	5.5	-7.9
Tuscany	8,647	5.7	7,659	5.3	-11.4
Sicily	8,672	5.8	8,940	6.1	3.1
Puglia	6,356	4.2	6,594	4.5	3.7
Calabria	3,934	2.6	3,236	2.2	-17.7
Liguria	3,614	2.4	3,043	2.1	-15.8
Marche	3,069	2.0	2,983	2.1	-2.8
Trentino-Alto Adige	2,330	1.5	2,213	1.5	-5.0
Friuli Venezia Giulia	2,240	1.5	2,262	1.6	1.0
Abruzzo	1,883	1.3	1,824	1.3	-3.1
Sardinia	2,098	1.4	2,452	1.7	16.9
Umbria	1,335	0.9	1,366	0.9	2.3
Basilicata	993	0.7	730	0.5	-26.5
Molise	410	0.3	438	0.3	6.8
Valle D'Aosta	274	0.2	232	0.2	-15.3
Foreign	1,972	1.3	2,586	1.8	31.1
Online	14,116	9.4	11,835	8.1	-16.2
Total	**150,418**	**100.0**	**145,401**	**100.0**	**-3.3**

Figure 1.1

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

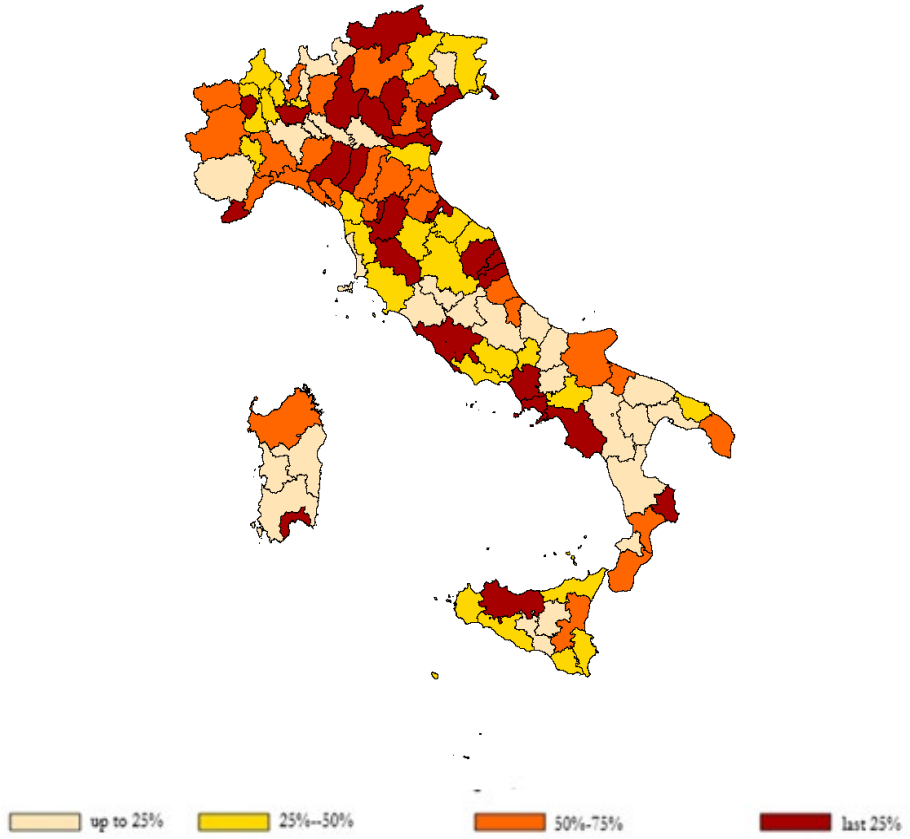
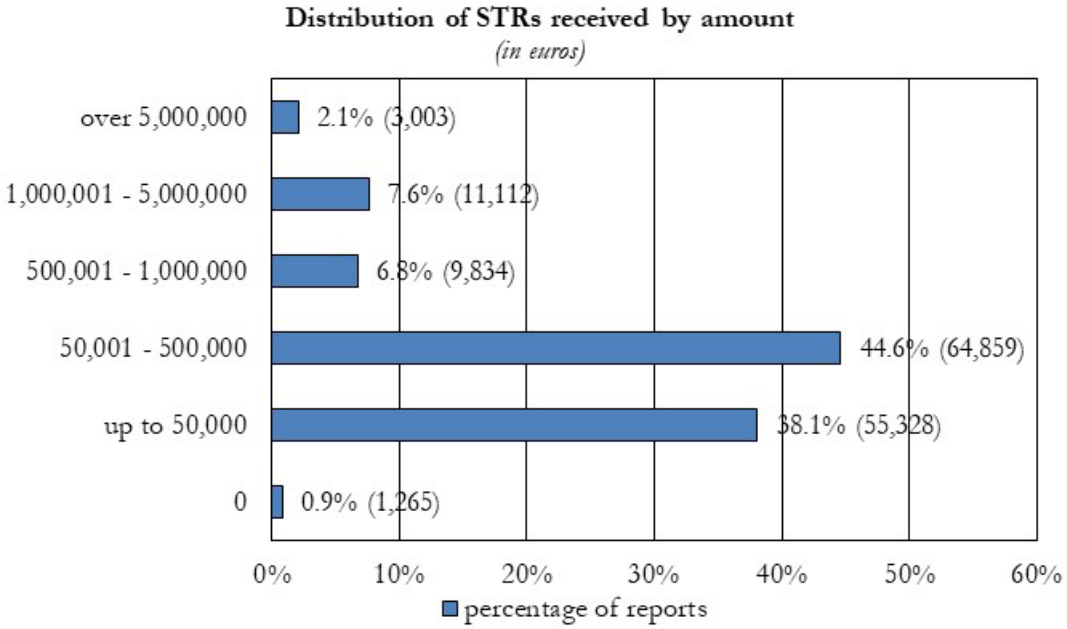


Figure 1.2



1.2. The quality of active cooperation

In 2024, the UIF continued its efforts to improve the quality of active collaboration through the enhancement of the QUASAR[3] monitoring system, the fine-tuning of the new feedback forms, and the implementation of targeted initiatives aimed at engaging with reporting entities on issues or areas of concern identified through the aforementioned monitoring.

The new feedback forms

The new feedback forms have been developed by integrating the original structure of the previous version – dating back almost ten years – with a careful selection of indicators from the QUASAR system. The pool of recipients will be expanded beyond the 'banks and Poste Italiane' and 'money transfer' categories to include all reporting entities that have exceeded a certain threshold of STRs submitted in the past year, thus further fostering dialogue with the UIF. The forms will be sent out at least annually, in addition to the quarterly communications relating to low-risk STRs (classes A and B), serving as an additional tool for reporting entities to self-assess the quality of their active collaboration. Like the previous version, the new feedback forms are not intended as a formal evaluation but rather aim to improve the quality of active cooperation. The forms now include a higher number of indicators that focus on additional qualitative aspects compared with those previously considered. The indicators are structured according to the four macro-areas of the QUASAR project:

A – Engagement level: provides a quantitative measure highlighting each entity's reporting contribution relative to operational and dimensional parameters.

B – Substantive quality: assesses the risk profile emerging from the reported context, any classification categories (phenomena), and whether the conditions for filing the STR were met, including in specific cases flagged by the UIF.

C – Formal accuracy: checks the formal correctness of the STRs in terms of compliance with the reporting instructions, proper use of the reporting form, completeness and consistency of the information provided, and clarity of the narrative.

D – Timeliness: reflects the promptness of the reporting entity both in submitting STRs and in responding to UIF follow-ups.

For each indicator, the form shows the previous year's data, the average for the reporting entity's reference group, and the corresponding variations. The new forms are currently being finalized: an initial version was shared with the 11 largest reporting entities to gather feedback, comments, and suggestions. This generated strong interest and confirmed the forms' usefulness. A number of areas for further reflection were identified, including the composition of the reference groups, the design of the indicators, and the timing of form dissemination. IT projects are currently underway to integrate the forms into the UIF's structured communication system with reporting entities.

New reporting entities and participation

In 2024, there were 384 new registrations on the Infostat-UIF portal (602 in 2023), primarily from professionals. Among newly registered entities, 21 per cent submitted at least one STR; the vast majority of the STRs submitted (786 out of 851 total) came from non-financial obliged entities, particularly virtual asset service providers. A total of 1,096 reporting entities submitted STRs in 2024, 174 of which were either newly registered or inactive over

[3] See UIF, *Annual Report 2023,* p. 15.

the previous four years. Among the reporters, 114 entities submitted at least 100 STRs (10 per cent of reporters), accounting for 91 per cent of total STRs.

Substantive quality

The share of STRs filed in 2024 that, based on data available in February 2025, were classified as low-risk (classes A and B)[4] suggests a possible correlation between the reduction in reporting volume and an improvement in the quality of active cooperation. These STRs accounted for 20.4 per cent of total reports, compared with 25.2 per cent in 2023, with class B STRs prevailing (15.4 per cent). The share of low-risk STRs from banks and Poste Italiane is broadly in line with the general figure (21.3 per cent, down by 5.4 per cent), whereas higher proportions persist among some categories, including professionals (27.7 per cent) and gaming service providers (25.2 per cent), though both are down from 2023 (when they amounted to 29.3 per cent and 34.5 per cent respectively). A further increase was observed among gold traders or manufacturers and retailers of precious items (from 59.1 per cent to 71.1 per cent).

A number of specific cases appear to be characterized by the presence of triggering factors that may indicate a precautionary approach to reporting or reliance on potential automatisms. For example, in 2024, over one-fifth of the STRs submitted by banks and Poste Italiane were primarily related to the use of cash, although this represents a decline compared to the previous year (24.6 per cent). For the same category, there was a slight increase in reports involving subjects under investigation (15.3 per cent, up from 14.3 per cent in 2023).

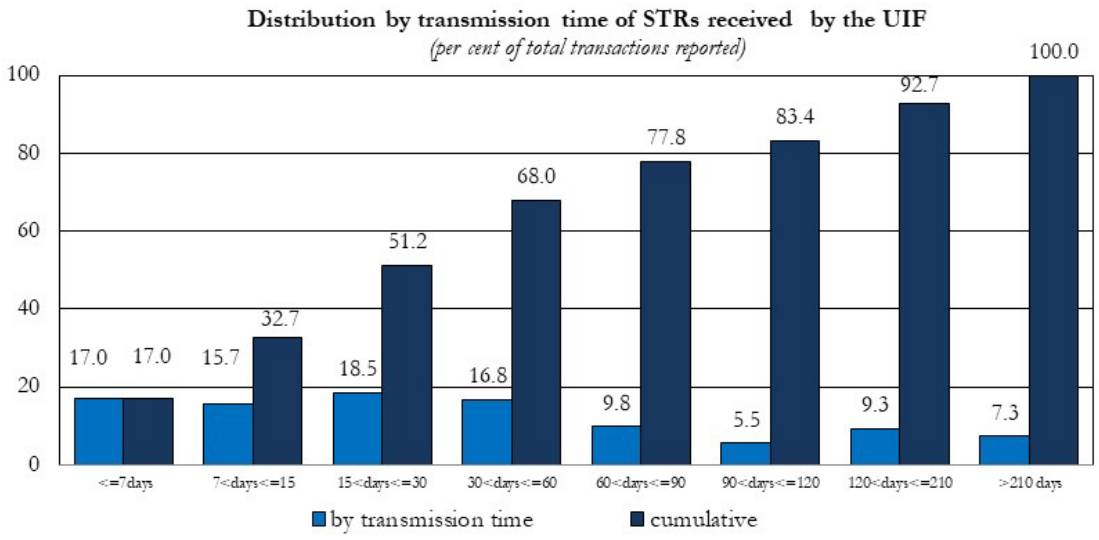
Formal accuracy

The reports received in 2024 with at least one finding that, while not blocking the transmission of the STR, showed an anomaly in formal correctness, amounted to almost 14,000 (9.7 per cent of the total, compared to 10.6 per cent in 2023).

Timeliness

51 per cent of STRs were submitted within one month from the execution of the related transactions; 68 per cent and 78 per cent were submitted within two and three months, respectively, in line with 2023 data (Figure 1.3).

Figure 1.3



[4] Type A STRs lack sufficient risk elements to support the suspicion of money laundering or terrorism, while Type B STRs show weak elements, including investigative ones, to support the suspicion. See. UIF, *Annual Report 2022*, p. 20 and UIF Communication of 27 March 2023 (only in Italian).

The percentage of STRs submitted within 30 days was higher among professionals (80 per cent) and banks and Poste Italiane (56 per cent), compared to other financial intermediaries (47 per cent), non-financial operators (46 per cent), and gaming service providers (13 per cent). This percentage was an improvement for banks and Poste Italiane (52 per cent in 2023), and a decline for non-financial operators and gaming service providers (53 per cent and 17 per cent, respectively, in 2023). Transmission times remained significantly longer for public administrations: 90 per cent of their STRs were submitted more than 90 days after the related transaction.

The UIF submitted 6,019 requests for additional information to reporting entities for financial analysis purposes (inquiries), 77.4 per cent of which were addressed to banks and Poste Italiane. 91.6 per cent of responses were received within seven days of the request; 3.5 per cent took more than 15 days, and 1.3 per cent exceeded 30 days. Significant differences were observed across the different categories of reporting entities: banks and Poste Italiane responded within seven days in 96 per cent of cases, while professionals and gaming service providers had substantially less timely response rates (49.5 per cent and 48 per cent, respectively), as did non-financial operators (69.8 per cent).

Assistance to reporting entities

The Unit handled around 2,400 requests for assistance from reporting entities in 2024, down 11 per cent from 2023. This decrease was mainly due to the simplification of the registration process on the Infostat-UIF portal. The introduction of automated controls in the new registration process enabled reporting entities to avoid formal errors, significantly reducing the rejection rate of registration requests (from 51 per cent to 10 per cent). A further simplification was introduced in February 2025, streamlining the procedures for reporting personal data updates by already registered reporting entities.[5]

1.3. Financial analysis

The number of STRs analysed and transmitted to the Investigative Bodies amounted to 143,850, down from 2023. This trend mirrors the contraction in incoming reports observed up to the third quarter (Table 1.4). The sharp increase in STRs received in December (15,661 STRs, compared to a monthly average of around 11,800 since the beginning of the year), mainly attributable to some payment and electronic money institutions, resulted in an increase of around 1,500 in the stock of STRs pending analysis compared to the end of 2023.

Table 1.4

Reports analysed by the UIF					
	2020	**2021**	**2022**	**2023**	**2024**
Number of reports	113,643	138,482	153,412	151,578	143,850
Percentage change on previous year	*6.9*	*21.9*	*10.8*	*-1.2*	*-5.1*

Processing times

Average processing times decreased to 13 days (from 15 in 2023), with 51.3 per cent of STRs assessed as high or medium-high risk analysed and forwarded to the Investigative Bodies within seven days, and 92.4 per cent within 30 days of receipt. Regardless of the risk profile assigned during analysis, 93.7 per cent of all STRs were reviewed and transmitted within the first 30 days.

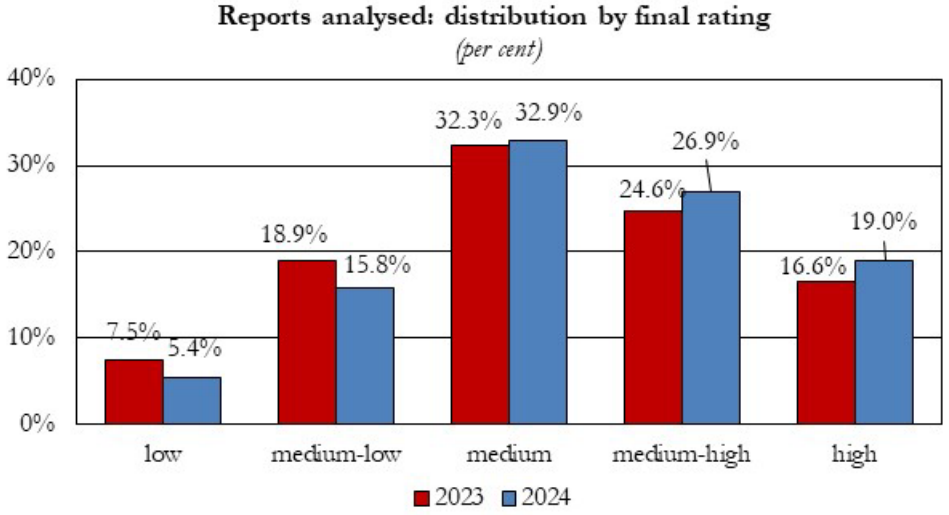
[5] See UIF Communication of 11 February 2025 (only in Italian).

Risk assessment

Efforts continued to fully redefine the conceptual model underlying the risk assessment of STRs, focusing on key components relating to the characteristics of involved parties and the nature of the reported activity. As part of this initiative, three new indicators have already been defined and integrated into the RADAR system to support risk assessment and guide financial analysis: financial ranking, which measures the financial importance of a subject within an STR; link rating, which evaluates the matches between two STRs based on the financial weight of shared subjects; subjective neutrality, which identifies reported subjects that are not relevant to the suspicion (e.g., banks executing the transactions).

The distribution of final risk ratings shows a continued decline in STRs classified as low and medium-low risk (21.2 per cent compared with 26.4 per cent in 2023), confirming the trend observed in the previous year. Meanwhile, 45.9 per cent of STRs were assigned a medium-high or high-risk rating (up from 41.3 per cent in 2023; see Figure 1.4).

Figure 1.4



Complexity

The increase in STRs classified as medium-high or high risk is linked both to enhanced exploitation of the data available to the Unit, facilitated by advancements in the CLAUT and LASER projects,[6] and to the growing complexity of the cases reported, partly due to innovative technologies and services for detecting suspicious transactions adopted by the reporting entities. The share of structured data within STRs also grew, with a steady rise in the number of reported subjects, transactions, and relationships. In 2024, over one fifth of all STRs involved more than ten subjects and transactions. On average, the volume of data included in the STRs increased across most categories of reporting entities compared with the previous years. This greater complexity in both STR flows and their underlying contexts has led to more extensive investigative efforts. In 2024, the Unit sent more than two requests for documents and information to reporting entities in 22.8 per cent of cases. Additionally, nearly 12 per cent of analyses resulted in the activation of international cooperation with one or more foreign FIUs.

Methodologies

In 2024, third-level analyses, including network analyses, were carried out by aggregating large numbers of STRs sharing similar operational patterns, common subjective or geographic elements, or links to specific investigative contexts. These efforts particularly focused on transactions involving the use of new technologies and/or services, as well as those relating to the misuse of public funds.

[6] See UIF, *Annual Report 2022*, p. 24.

This approach made it possible to detect emerging phenomena, complex money laundering schemes, and specific risk indicators that would not have been identified through the examination of individual reports. Such analyses rely heavily on the Unit's entire body of information, its enrichment through cross-referencing with external databases, and the acquisition of additional data from reporting entities. This often involves bulk requests for data related to operations with specific characteristics – for instance, financial flows to certain foreign accounts.

In contexts involving tax offenses, the perimeter of involved parties was reconstructed not only using financial data but also accounting records from the electronic invoicing system, which enabled the identification of company networks that would not have been detected solely through transactional analysis. The integration of electronic invoicing data with financial transaction records allows not only a more comprehensive understanding of the operational context but also an overall assessment of the consistency of the activity under analysis – a methodology with significant potential beyond the tax domain.

An in-depth investigation was conducted on a company which, from the accounting documentation provided to the reporting entity, appeared to have intensive operations, inconsistent with its financial movements. The analysis of issued and received electronic invoices revealed a substantial network of newly established companies (many of which were already recorded in the Unit's databases), whose operations were consistent with tax fraud schemes and the subsequent transfer of illicit proceeds to Southeast Asian countries amounting to over €300 million.

STRs from virtual asset service providers often reveal significant interconnections that may not be immediately visible in individual reports, partly due to the specific nature of the instruments involved. To address this, in 2024 a dedicated third-level analysis methodology was developed to identify key subjects and virtual addresses, uncover schemes involving multiple individuals, and reassess previously analysed STRs in light of new information. The analysis covered STRs submitted by virtual asset service providers in 2023, involving more than 2,000 individuals or entities and over 10,000 virtual addresses, using the tools available to the Unit, including social network analysis software, blockchain forensics platforms, and internally developed applications designed to map connections and assess the financial weight of involved parties.

This analysis uncovered an extensive network of foreign individuals who, consistent with the Unit's previous findings, appeared to operate an informal value transfer system, using also crypto-assets to facilitate internal transfers within the group.

Forensic analysis of crypto-assets

The analysis of the STRs related to crypto-assets also revealed the use of new technologies aimed at making the reconstruction of financial flows more complex and not always traceable with forensic analysis tools. In more detail, the Unit identified cryptocurrency transfers that were not recorded on the main blockchain, as they were executed through layer-2 technologies, aimed at increasing validation capacity and speeding up transaction execution, as well as privacy-oriented applications or tools that facilitate the movement of crypto-assets across different decentralized networks.

1.4. Suspension orders

In 2024, the Unit initiated 188 administrative procedures with a view to possible suspension orders for suspicious transactions – an increase compared with 2023. The total value of the transactions under review was approximately €63 million. In 101 of these cases, information was forwarded to the Anti-Mafia Investigation Directorate (DIA) due to

connections between the parties involved and organized crime. The number of inquiries initiated by the UIF based on the monitoring of reported unexecuted transactions, without specific information by the reporting entities, totalled 78. Similarly to 2023, suspension orders were concluded on average within five working days of their start. A total of 28 suspension orders were adopted, for a value of suspended transactions of €4.7 million (Table 1.5); of these, nearly one-third resulted from inquiries initiated by the UIF (nine orders for a value of suspended transactions of €9.8 million).

Table 1.5

Suspensions					
	2020	**2021**	**2022**	**2024**	**2024**
Number of suspension orders	37	30	32	25	28
Total value of transactions suspended (*millions of euros*)	13.0	18.0	108.7	8.7	4.7

As usual, most investigations (87 per cent) were initiated at the request of insurance companies, while those stemming from reports forwarded by banks accounted for 9 per cent, an increase compared to 2023 (5 per cent). Consistent with the origin of the proceedings, the most recurrent transactions examined for suspension concerned insurance policies, primarily early redemptions, attributable to persons involved in criminal investigations or linked to organized crime circles.

1.5. Investigative findings

The transmission of STRs by the UIF to the Investigative Bodies is followed by feedback flows that indicate the level of interest in the reports and are essential for guiding UIF's activity in identifying and processing future reports involving similar or related cases. These flows are also used by the Unit to provide reporting entities with qualitative assessments on the effectiveness and reliability of their reports. A discussion is ongoing between the UIF and the Finance Police aimed at improving the effectiveness of received feedback and, more broadly, at assessing the actual usefulness of the STRs not directly used in investigations.

With regard to the STRs transmitted to the Investigative Bodies during 2023-24, as of April 2025, the Finance Police had issued nearly 48,000 positive feedbacks, in line with the percentage recorded in 2023 for the 2022-23 period: 84.5 per cent of positive feedbacks referred to reports assessed as high or medium-high risk. In the same period, 89.8 per cent of the positive feedbacks sent by the Anti-Mafia Investigation Department concerned STRs rated as high or medium-high risk. Exchanges with the National Anti-Mafia Directorate (DNA) included both general feedback on the data contained in the STRs and nominative feedback on subjects reported to the UIF. As regards the former, for the reports sent in 2023-24 positive feedback amounted to over 9,600, 87.1 per cent of which referred to STRs rated as medium-high and high risk, while the nominative feedback concerning the reports received by the UIF in 2024 showed approximately 15,000 subjects, counted in as many STRs, that were present in the archives of the National Anti-Mafia Directorate.

The investigative value of the STRs is further evidenced by their extensive and concrete use in the activities carried out by the Anti-Mafia Investigation Directorate in the context of judicial investigations and asset verification procedures aimed at applying preventive measures. According to information from the Anti-Mafia Investigation Directorate, in 2024

more than half of all preventive measures were proposed with the support of data and information from the STRs: the resulting seizure and confiscation orders concerned assets worth approximately €72 million and €120 million respectively, corresponding to about 80 per cent and 76 per cent of the total value of assets seized and confiscated during the year. The data contained in the STRs were also widely used in judicial police activities, contributing to seizure and confiscation orders involving assets valued at about 60 per cent and 55 per cent of the total, respectively.

2. RISK AREAS AND TYPOLOGIES

2.1. Context

In 2024, active collaboration revealed the increasing complexity of money laundering schemes designed to conceal illicit activities, the parties involved, and the destination of illicit proceeds. Such schemes often have an international dimension and involve frequent use of innovative financial instruments and channels, operated by intermediaries and operators of various kinds. Many of them provide their services in countries other than those in which they are established, leveraging regulatory arbitrage opportunities. These arrangements result in large-scale fund transfers to foreign accounts held by hard-to-identify beneficiaries, often acting as hubs for proceeds from illicit activities primarily relating to tax offences, but also relating to public resources unduly obtained or misused or connected to organized crime. These offences – typically involving tax evasion, public fund abuse and corruption, and organized crime – remain predominant in STR flows, but their financial structuring is increasingly complex, to make it difficult to detect and trace them.

The widespread use and impact of technology remain significant across the cases reported, with continued growth and evolution in cyber fraud and laundering schemes based on crypto-assets.

2.2. Tax evasion

STRs relating to tax offences account for over 20 per cent of total reports, confirming the scale of the phenomenon. Again in 2024, the most common cases involved suspected invoice fraud, present in nearly 40 per cent of tax-related STRs, followed by fund transfers between individuals and legal entities connected to them (in 37 per cent of STRs of the same type).

Investigations into fraud and tax evasion cases revealed extensive use of virtual IBANs (v-IBANs) and correspondent banking services, which serve as effective concealment tools across various illicit contexts. The use of such services for money laundering is part of the evolving strategies of criminal networks to hamper identification of the final recipients of financial flows, to the benefit of hidden centres of interest. In addition to informal systems running parallel to the banking system (underground banking), traditionally used for transferring money abroad, more sophisticated methods have emerged, allowing a rapid layering of transactions across multiple jurisdictions.

International money laundering schemes and joint analyses

Within complex transnational laundering schemes – identified by analysing numerous reports and via a joint analysis with European FIUs – recurring financial intermediation channels were detected operating in a money-laundering-as-a-service logic. They exploit EU regulatory grey areas and divergent national implementations, in the absence of a harmonized European AML supervisory framework.

The analyses revealed the frequent involvement of EU-authorized payment institutions (PIs) and electronic money institutions (EMIs) operating under the freedom to provide services, often via agent networks, as well as non-EU PIs and EMIs, not authorized to operate in the European Economic Area (EEA), holding master accounts in EU Member State banks, with v-IBANs opened for foreign clients and used to receive payments from Italian counterparties.

Financial investigations highlighted suspiciously large illicit fund flows from Italy to China, mediated by a foreign payment agent with a European passport, publicly promoted by the international press and by some reporting entities as a bank or PI despite lacking valid EU licences. Clients in Italy and other EU countries, along with the cross-border provision and distribution of services, have created considerable uncertainty regarding business location and applicable regulations, also exacerbated by the not fully harmonized EU regulatory framework. Behind this apparent legitimacy was a payment channel for laundering funds largely coming from extensive networks of Italian companies being investigated for invoicing fraud and misuse of public funds, including tax credits and resources from the National Recovery and Resilience Plan (NRRP). Funds of illicit origin amounting to more than €100 million, originating from Italy, were funnelled via a triangular scheme into an account held by the agent at a PI in one EU country, then forwarded to China through a correspondent account in another EU state.

Given the transnational scale and systemic relevance of the phenomenon, the joint analysis exercise proved effective for assessing both AML and prudential aspects, since it expanded cooperation among FIUs. Multilateral, real-time exchanges made the best use of all available data and enabled discussions with supervisory authorities in the countries involved about the potential compliance shortcomings uncovered in the analysis.

Tax credit transfers

STRs on the transfer of tax credits under Decree Law 34/2020 (the 'Relaunch Decree') declined again in 2024, from 743 in 2023 to 619. In this regard, some in-depth analyses uncovered new attempts to liquidate tax credits without using standard transfers, as their transferability is now legally restricted. Specifically, numerous securitization proposals were identified, mainly targeting construction companies with substantial tax credits. To launch such operations, these companies paid significant fees (consulting or transaction costs) to various special purpose vehicles (SPVs), many of which were linked to the same individuals. SPVs then used these funds to issue transfers to foreign accounts, some of which were held by Italian individuals with no apparent role in the securitization transactions and who thus served merely as conduits. The analyses pointed to potential fraud against the original credit holders, considering that in some cases, months later, the securitization transactions had never materialized, and the SPVs involved were removed from Banca d'Italia official lists shortly after their transactions were published in the Gazzetta Ufficiale della Repubblica Italiana.

Shell companies

As in 2023, further analyses continued to focus on the characteristics of shell companies, which play a central role in tax offences by issuing invoices for non-existent transactions to obtain undue advantages. Research in 2024 analysed the turnover of these companies to provide reporting entities with additional useful elements for identifying this type of entity at an early stage and reporting them to the UIF.

The analysis focused on a sample of 32 companies classified as shell companies by judgments of the Third Criminal Division of the Court of Cassation handed down in the period 2018-20 and which had filed financial statements for two or more years. The findings showed common revenue peaks among shell companies. The average growth rate was 131 per cent (101 per cent excluding outliers), the average time from initial to peak revenue was nearly 3 years (2 years and 4 months excluding outliers) and the average lifespan of shell companies was 4 years and 3 months (3 years and 7 months excluding outliers).[7]

[7] See A. Pellegrini, 'A research on the Italian fiscal shell companies turnover', *Journal of Money Laundering Control*, 27(6), 2024, pp. 1092-1103.

2.3. Misuse of public funds and corruption

STRs involving public support measures continued to confirm the recurrence of cases where guaranteed loans were granted to beneficiaries with problematic profiles, often detectable during the initial assessment. These critical issues relate to the eligibility criteria for such financing and to the documentation produced to support the request and the creditworthiness, which are not always adequately assessed by lending intermediaries, including EU-based institutions operating under the freedom to provide services. In some instances, the public guarantee was used to mitigate risk across almost the entire portfolio of the lender, effectively becoming integral to its business model by adopting policies aimed at transferring the credit risk to the State without implementing adequate safeguards. Furthermore, some cases revealed potential conflicts of interest among the intermediaries, linked to the inclusion of commission fees into the financed capital or the use of disbursed funds to repay pre-existing debts held with the same intermediary. Such practices contradict both the purposes of the public intervention and the intentions declared when accessing the measure.

NRRP and public contributions

In 2024, STRs connected with the implementation of the National Recovery and Resilience Plan (NRPP) increased to 805, compared with 309 in 2023. Over 90% of these originated from general government bodies, although they were concentrated among a small number of reporting entities.[8] The most frequent anomalies involved access to public funds by applicants lacking the necessary requirements or presenting an economically inconsistent profile, and the misuse of such funds for purposes other than the intended goals, often directed towards private gain.

Similar instances of potential misuse of public resources have also been observed in the context of public subsidies not included in the National Recovery and Resilience Plan. Some STRs have highlighted irregular activity by companies in the development, production and distribution of film and audiovisual works, benefiting from a tax credit (the 'Tax Credit Cinema') proportional to the expenses incurred for the production of such works. Specifically, it was found that these companies received funds, in the form of capital contributions or loans, from other firms operating in sectors unrelated to cinema. These funds were used to issue bank transfers for the payment of eligible expenses, thereby increasing the amount of the tax credit to the benefit of entities, which subsequently returned the transferred funds to the originating entities. This scheme was therefore aimed at maximizing the fiscal benefit and generating higher tax credits based on expenses not actually sustained.

Further scrutiny concerned a non-profit entity primarily funded through public funds. Between receiving the grants and executing the related projects, the funds were invested through a financial company linked to an individual with personal ties to the financial manager of the entity. Additionally, irregularities were found in the use of public subsidies to finance a newly established company, in which another firm – connected to the family of the financial manager of the non-profit entity – had acquired an indirect stake for a price significantly lower than its actual value. A few months later, the financed company distributed profits to its shareholders, including the company linked to the financial manager, who thereby received benefits far exceeding the amount initially invested to acquire the stake.

Guarantees in favour of public administrations

New cases of counterfeit sureties have emerged in the area of guarantees issued in favour of public administrations. These sureties, issued to multiple companies often located in the same geographic area, were intended to secure compliance with contractual obligations

[8] See UIF, 'Le informative di operazioni sospette connesse all'attuazione del PNRR' , Newsletter, 2, 2025 (only in Italian).

with various public entities. Specifically, these companies had entered into surety agreements in favour of public administrations, issued by a foreign intermediary authorized to operate in Italy. However, the contracts were signed by a person falsely claiming to be a special attorney, with no formal connection to the actual guarantor. The guarantee agreements were arranged by a professional operating in the same area as the companies involved, who acted as an escrow agent collecting payment for the sureties on behalf of the guarantor, and by insurance brokers, some of whom had already been implicated in similar fraudulent guarantee schemes involving public administrations.

Corruption

The analysis of STRs concerning potential corruption scenarios confirms the recurrence of complex operational schemes designed to conceal the provision of undue benefits to political figures or senior public officials. These schemes often involve intermediaries such as foreign entities with opaque and difficult-to-trace ownership structures, or the execution of complex, closely timed real estate transactions.

In this context, attention was given to the activities of an employee of a publicly owned Italian company who received substantial bank transfers from a foreign trust linked to his family. The trust had been funded by a foreign firm with commercial ties to the public company, from which the latter had recently made a large-scale purchase, as well as by other entities connected to that same foreign company. Another case involved the purchase of a luxury property by a relative of a politically exposed person (PEP), jointly with an entrepreneur operating in the same sphere of influence as the PEP. A few months later, the PEP's relative bought another property, which was then exchanged with the entrepreneur – for more than the original purchase price – to acquire the latter's share of the luxury asset.

2.4. Organized crime

The approach to STRs with ties to organized crime continued to rely on the indicators introduced in 2023, which also take into account contextual information derived from connected STRs, to more effectively identify the relational networks underlying such reports. In 2024, STRs directly linked to organized crime interests accounted for approximately 15 per cent of the total (compared with 18 per cent in the previous year). An additional 18 per cent of reports included potential contextual connections to organized crime, identified through the connected STRs (16 per cent in 2023).

STRs relating to organized crime, including indirectly, received feedback indicating (investigative) interest on the part of the Investigative Bodies and the National Anti-Mafia Directorate (DNA) in 35 per cent of cases, up from 24.5 per cent the previous year, largely due to an increase in positive responses from the DNA. Of these reports, 6 per cent underwent second-level analysis (up from 5.4 per cent in 2023); 50.8 per cent of suspension procedures were found to be connected to organized crime contexts. Regarding geographic distribution, Lombardy accounted for 19.7 per cent of these reports, followed by Campania (16.1 per cent), Lazio (10.1 per cent) and Sicily (7.0 per cent), while online activity decreased slightly year-on-year (7.9 per cent compared with 9.3 per cent in 2023). In 2024, the three provinces with the highest number of STRs linked to organized crime were Milan (11.5 per cent), Naples (10.6 per cent) and Rome (8.5 per cent), collectively representing 30.6 per cent of such reports (about 29.8 per cent in 2023).

About one third of these cases involved cash transactions and invoice fraud, with funds transferred abroad – often to v-IBANs or accounts in Southeast Asian countries – conducted by networks of companies and individuals often flagged in the DNA database. Similarly to 2023, roughly 14 per cent of STRs with links to organized crime involved fraud, cybercrime and crypto-asset transactions.

Numerous requests were made to exchange damaged banknotes, worth considerable sums, on behalf of companies – mainly operating in fuel distribution – belonging to the same economic group. The beneficial owners of these companies were found in DNA records and had previous convictions relating to organized crime. The interest of organized crime in acquiring and managing catering and hospitality businesses is confirmed, including acquisitions funded in part by NRRP-backed public grants. One case observed involved the purchase of a hospitality facility at a price above the market value estimated by a specific expert's report on the property, by a company with employees under investigation for connections to organized crime. The facility received NRRP incentives and payments from firms awarded many public contracts.

In 2024, reporting flows also continued to highlight involvement in the photovoltaic and renewable energy sector by companies directly or indirectly linked to organized crime. Analysis of STRs revealed a recurring pattern: multiple energy-sector companies, often sharing the same professional address, having complex shareholdings, frequently involving foreign parent companies with hard-to-trace beneficial owners and clear links to criminal organizations.

2.5. Further case studies

The increasing digitalization and continuous technological advancement underpin a steady rise in cases linked to cybercrime or enabled by innovative tools and channels.

SMS and WhatsApp fraud

In this context, the analysis of numerous reports made it possible to reconstruct a scam perpetrated by an extensive network of young men residing in Italy, in the same geographical area. The scam involved sending messages on smartphones using SMSes or other applications such as WhatsApp. The investigations revealed that these individuals were holders of prepaid cards with IBANs that were topped up by more than 900 different individuals, mostly women, through transactions generally below €1,000. In some cases, the payments were made following explicit requests sent via text messages, in which the fraudsters falsely claimed to be in dangerous or emergency situations. The amounts paid were systematically transferred to a foreign company linked to a Chinese beneficial owner, via wire transfers intended for the purchase of virtual items on a platform managing a gaming app popular among children and adolescents.

Scams and crypto-assets

Cases involving the use of crypto-assets remained numerous and of particular interest in 2024 too, as they continued to feature a recurring variety of money laundering methods. The reports continue to highlight the frequent purchase of crypto-assets using funds derived from various types of illegal activity, especially fraud, including through innovative schemes. These cases confirm the recent trend that sees funds being collected directly via crypto-asset transfers, without first passing through traditional bank accounts, thereby making it more difficult to detect the criminal nature and scope of and the parties responsible for the illegal activity.

One particularly noteworthy case involved a network of individuals residing in the same Italian city, originally from the same Southeast Asian country. Over a short period, they deposited significant amounts of cash into newly opened accounts, inconsistent with their known income and financial profiles. The funds were then routed – via foreign virtual IBANs – for the purchase of crypto-assets, which were subsequently transferred to other recurring contacts from the same country, one of whom was under investigation at home for fraud. This pattern suggests the possibility that what appeared to be an informal remittance channel may in fact have served as an atypical laundering mechanism for the proceeds of fraud, either perpetrated in collusion with the depositors or targeting them as victims.

Further analysis revealed weaknesses in the anti-money laundering and counter-terrorist financing (AML/CFT) frameworks of certain Virtual Asset Service Providers (VASPs), including inadequate customer due diligence and insufficient scrutiny of fund origin. In some cases, as the investigation confirmed, the VASPs themselves were found to be compromised, directly implicated in fraudulent schemes or money laundering, and at times exploiting their presence in official national registers to appear credible.

Stablecoins in money laundering schemes

A broader review of STRs from VASPs highlights the growing use of stablecoins, which are crypto-assets pegged to stable reference values, typically fiat currencies. These assets provide the speed of transnational transfers combined with greater anonymity, making them attractive tools for laundering.

Several investigations revealed coordinated activity among foreign nationals who were all clients of the same VASP. These individuals deposited large amounts of euros into their wallets, converting them into stablecoins via trading operations, which were then exchanged through peer-to-peer (P2P) channels into the local currency of the users' home country, often involving hundreds of local counterparties. The shared behavioural patterns and operational similarities pointed to a coordinated structure designed to move funds of uncertain and possibly illicit origin, via crypto conversion. This method operates in parallel with more traditional schemes such as cash withdrawals using prepaid cards issued to front men.

The nature of stablecoins, particularly their limited price volatility compared with other types of crypto-assets, makes them an attractive alternative payment mechanism. They have the potential to disrupt conventional crypto-based laundering models, which typically involve converting illicit fiat funds into crypto-assets (or vice versa in the case of offences originating in the virtual system). The use of stablecoins may reduce or even eliminate the need for fiat currency altogether, depending on the type of predicate offence. This hypothesis is supported by various STRs from VASPs describing high-value transactions in stablecoins recorded in wallets, without any associated fiat movement, and involving unclear beneficial owners.

Digital channels and AML risks

STRs submitted by operators using digital channels (like smartphone apps) to provide their services to the public are increasingly flagging suspicious behaviour suggestive of account misuse by persons other than the legitimate owners. Red flags include anomalous connection data and discrepancies in registration info (e.g. IP addresses, email domains or device IDs). In addition to identity theft or a certain voluntary sharing of credentials to third parties, some cases indicate that suspicious activity may originate from accounts opened remotely in a coordinated manner. These processes often involve semi-automated workflows and generative AI tools (such as deepfakes) for identity verification. Such operations are likely centrally managed by technically sophisticated criminal organizations. These activities pose a growing AML/CFT risk, especially as the traditional physical distribution networks continue to shrink, a trend also affecting conventional obliged entities.

Manipulation of investment funds market

One case of interest emerged involving potential market manipulation relating to investment fund transactions. Specifically, there were repeated buy and sell operations involving shares of a closed-end real estate fund, carried out with suspicious timing, suggesting pre-arranged agreements between counterparties. These operations were carried out by recurring and sometimes interlinked individuals, often working through the same financial intermediary and with the involvement of investment professionals. The activity appeared to be aimed at artificially inflating the value of the financial instruments held before final liquidation, potentially generating advantages, including at fiscal level.

Embezzlement

As regards embezzlement, a case was analysed of a professional entrusted with managing the insurance payout from a fatal car accident on behalf of the victim's heirs, some of whom

were minors. The sums intended for the latter were credited to accounts in the minors' names, with the professional being granted power of attorney. However, the funds were instead transferred to the professional's personal account and withdrawn in cash on multiple occasions. Other insurance payouts were paid directly into the professional's account and never passed on to the rightful beneficiaries.

Russian sanctions

Reports continued to flow in throughout 2024 (1,243 cases, consistent with the previous year), stemming from suspicions of potential attempts to circumvent the international sanctions imposed on Russian individuals and entities. These figures confirm the ongoing focus on this issue. The most significant STRs concerned transactions involving Russian businesses or citizens, either directly or through third-party companies based in other countries. Further analysis uncovered new triangulation schemes for financial flows, including the use of crypto-assets – particularly stablecoins – which may facilitate the movement of substantial sums outside traditional banking circuits, enabling possible mechanisms for evading sanction.

One such scheme involved companies based in Central Asia, seemingly operating as crypto-asset service providers that were not very transparent due to limited information on beneficial ownership and to the absence of open-source intelligence confirming their operations. These firms appear to have received funds from Russian subjects through a correspondent account of an Italian financial intermediary held at a foreign bank, which were then transferred to a European crypto-asset platform.

3. COMBATING THE FINANCING OF TERRORISM

In 2024, developments in the Israeli-Palestinian conflict and its broader escalation within the Middle East had repercussions on the global terrorist threat landscape. As anticipated in last year's assessment, carried out on the basis of trends observed in the latter part of 2023, the risk of terrorism financing was heightened by the potential for jihadist groups to exploit the conflict as a catalyst for propaganda and incitement to violence. Within the EU, additional threats emerged from extremist groups seeking to subvert democratic order, including anarchist and neo-fascist organizations. In Italy specifically, planned acts by such groups were thwarted by law enforcement before being carried out. As a result, these incidents had minimal impact on suspicious activity reporting by obliged entities, which largely reflected only the arrests themselves.

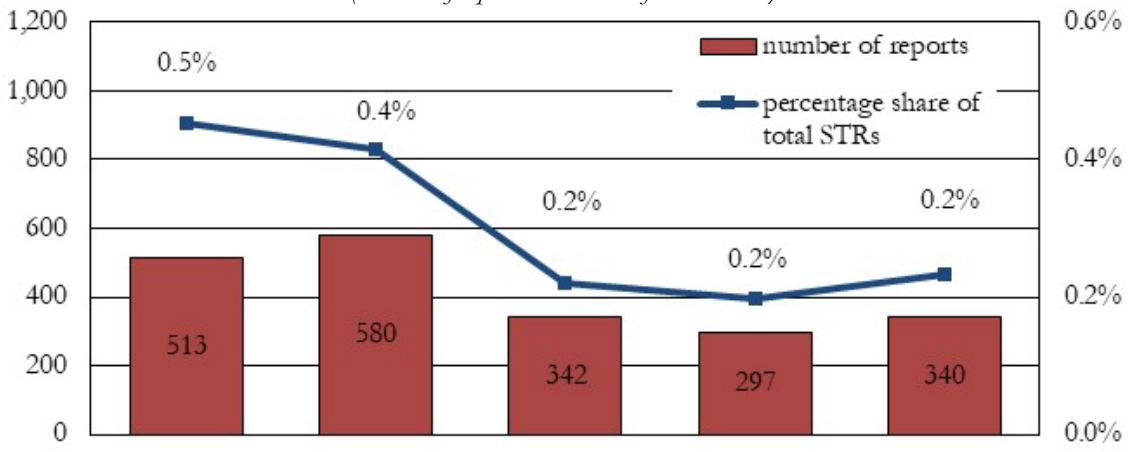
3.1. Information flows

In 2024, 340 STRs relating to terrorist financing were received, an increase of 14.5 per cent compared to 2023. Despite this rise, their proportion remains marginal, accounting for only 0.2 per cent of the total number of reports (see Figure 3.1).

Figure 3.1

Financing of terrorism reports received

(number of reports and share of total STRs)



This increase compared with 2023 can be attributed one-third to the financial sector and two-thirds to the non-financial sector (see Table 3.1). The growth in the non-financial segment is almost entirely due to reports submitted by some public administration bodies (27 STRs), alongside an increase in reports from virtual asset service providers (6 STRs). The contribution from professionals remains modest and stable. The financial sector continues to account for the majority of reports, although for the first time its share has fallen below 90 per cent. There has been a decline in STRs from electronic money institutions (EMIs), continuing a downward trend since 2020. However, this sector shows a contrasting trend in terms of the number of transactions reported, rising from 53.2 per cent in 2023 to 54.5 per cent in 2024 (approximately 38,000 transactions), reflecting their tendency to submit fewer reports that are, nonetheless, highly detailed in documenting financial flows.

Table 3.1

Terrorism financing reports by type of reporting entity

	2023		2024	
	(number of reports)	*(% share)*	*(number of reports)*	*(% share)*
Banking and financial intermediaries	**280**	**94.3**	**293**	**86.2**
Payment institutions and contact points	119	40.1	131	38.5
Banks and Poste Italiane	120	40.4	129	37.9
EMIs and contact points	35	11.8	29	8.5
Other intermed. and fin. operators (1)	6	2.0	4	1.2
Non-financial obliged entities	**17**	**5.7**	**47**	**13.8**
Notaries and Nat. Council of Notaries	13	4.4	7	2.1
Other non-financial entities (2)	4	1.3	40	11.8
Total	**297**	**100.0**	**340**	**100.0**

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

Geographical distribution

As in 2023, 80 per cent of STRs were linked to transactions across nearly all provinces of Central and Northern Italy, while the remaining 20 per cent originated from specific areas in the South, particularly the coastal provinces of Sicily, Campania, and Puglia. A residual concentration was observed in the province of L'Aquila, where STRs were triggered by the arrest of several foreign nationals residing in the area on terrorism-related charges. This geographic distribution highlights significant concentrations of STRs, relative to the resident population, in areas most affected by migration routes and in regions with a greater presence of immigrant communities originating from countries with a high terrorism risk.

In 2024, the UIF received 62 requests and spontaneous disclosures from foreign FIUs concerning suspected terrorism financing. Of these, 42 per cent came from EU FIUs and one-third from the Israeli FIU alone.

The risk associated with international terrorism financing remains elevated, particularly in the Middle East, with numerous reports involving suspected use of fake charitable activities to channel funds into conflict zones such as the Israeli–Palestinian area among others (such as the Kurdish–Turkish front). Additional reports concerned accounts held abroad by individuals arrested in Italy for terrorism charges and requests for information about operations relating to the manufacturing and trade of military drone components for terrorist use. Cross-border information flows on this topic mostly involved individual transactions, primarily via e-wallets or money transfer systems, connected to individuals listed on international sanctions lists or suspected of terrorist affiliations based on open-source intelligence or extremist messages posted on social media.

3.2. Analyses and types of operations

As in previous years, terrorism financing STRs in 2024 were mostly based on subjective suspicions. These were often triggered by the identification of clients linked to terrorism investigations or listed in international sanctions lists (UN, EU, OFAC) or, in fewer cases, linked to the Russia–Ukraine conflict. STRs triggered by financial anomalies were fewer and primarily submitted by banks. A common feature among these reports was the recurrence of cash operations, typically donations, which also appeared in about half of the reports concerning non-profit entities (66 STRs, up from 33 in 2023. Some of these were related to a single individual listed in international counterterrorism databases and under investigation

by Italian authorities). Use of crypto-assets remained marginal but showed a slight increase, with links to both jihadist groups (based on listed wallet addresses) and individuals known for previous involvement in subversive organizations or the Russia–Ukraine conflict. The Palestinian context recurred frequently in the cases reported, confirming that even reporting entities perceive a potential terrorism financing risk in environments susceptible to jihadist propaganda. The UIF prioritized analysis of cases with stronger grounds for suspicion – such as links to listed elements – and where financial connections could be uncovered through methodologies also used in money laundering investigations. This included applying models of criminal behaviour relating to terrorism financing,[9] network analysis tools, and blockchain analysis for crypto-related transactions (see Section: 'Financial Analysis' in Chapter 1).

About 70 per cent of the terrorism financing STRs disseminated by the UIF in 2024 received feedback of interest from the Investigative Bodies. This corresponds to 441 STRs, including not only the 340 reports originally categorized as terrorism financing but also STRs of other categories reclassified by the UIF as being related to terrorist financing in light of the overall information available. Nearly one-quarter of these reports had at least one match within the databases of the National Anti-Mafia Directorate.

3.3. International activities

At international level, the UIF participated in training activities organized by the Egmont Group and ECOFEL (Egmont Centre of FIU Excellence and Leadership) focused on specific terrorism financing contexts. As part of the FATF project 'Comprehensive Update of Terrorist Financing Risks', the UIF contributed an overview of the terrorist threats most relevant to Italy's risk landscape, such as small cells and lone actors, and shared analytical approaches developed to identify them, both in relation to traditional financing channels and to more technologically advanced, though still marginal, methods observed in Italy.

[9] See the box 'Connections between crime and the financing of terrorism', *Annual Report 2023*, p. 36.

4. DATA MANAGEMENT AND STRATEGIC ANALYSIS

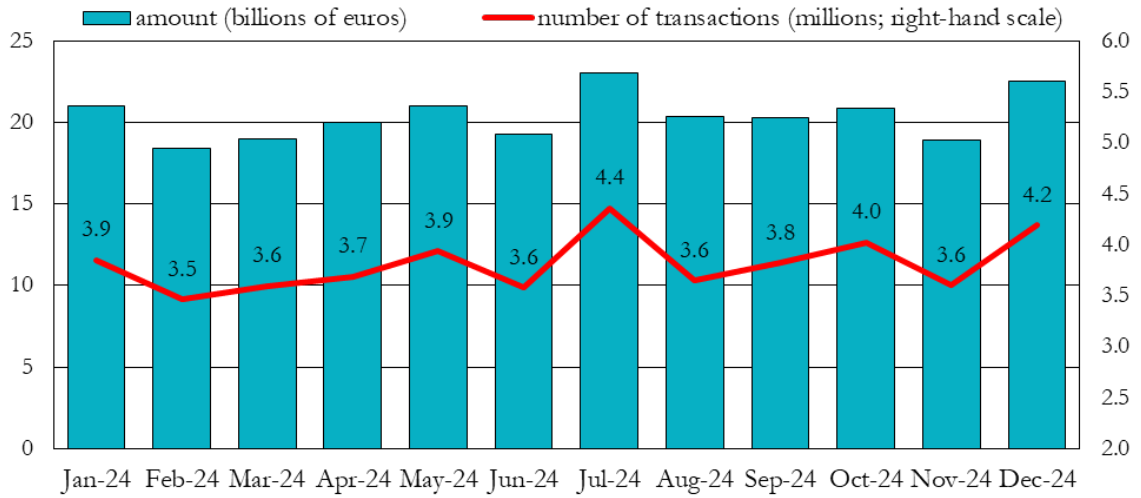
4.1. Threshold-based communications

In 2024, threshold-based communications recorded 45.7 million cash deposit/withdrawal operations, for a total amount of €244.5 billion, marking for the first time since the start of data collection a slight decline from the previous year (-1.7 per cent and -2.7 per cent, respectively). The monthly average stood at 3.8 million operations (about 260,000 withdrawals and 3.5 million deposits) and around €20.4 billion in total amounts (-2.8 per cent compared to 2023; see Figure 4.1).[10] Deposits continue to vastly outnumber withdrawals, accounting for 93.1 per cent of all operations by number and 95.2 per cent by value, primarily due to high-value cash deposits made by large-scale retailers. The average amount per transaction remained stable (about €5,470 for deposits and about €3,710 for withdrawals).

Figure 4.1

Threshold-based communications

(billions of euros and millions of transactions)



Distribution by regions

At the regional level, the highest total value of transactions was recorded in Lombardy, Veneto, Lazio, Campania and Sicily, which together accounted for 58.1 per cent of the amounts. In relation to nominal GDP in 2023, instead, the largest amounts were recorded in Veneto, Campania, Calabria, Puglia and Sicily (Figure 4.2).

Distribution by amount classes

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 4.3). On the other hand, there was a decrease in transactions above €100,000, which amounted to 37,180 (-9.0 per cent compared with 2023), totalling around €9.8 billion (-4.5 per cent).

Transaction types

The overall decline in operations did not affect any single transaction type disproportionately. Among deposits, the most common types remained cash payments via ATMs or continuous cash machines (38.6 per cent), over-the-counter payments (29.6 per cent) and payments to cash handlers (29.3 per cent), with percentages not very different from those observed for 2023. Most of the withdrawals (88.9 per cent) referred again to

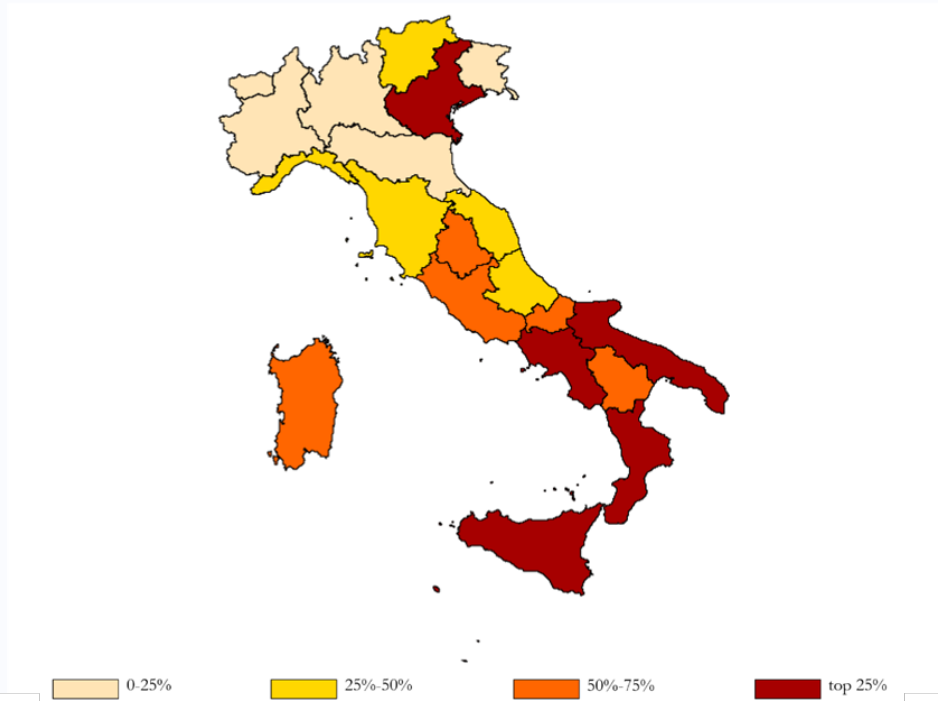
[10] The figures are subject to corrections by the reporting entities; the statistics reported are based on data as at 3 March 2025.

transactions by way of branch withdrawal forms or from cash handlers or from savings books.

Figure 4.2

Threshold-based communications: amount by region

(as a percentage of nominal GDP; quartiles)



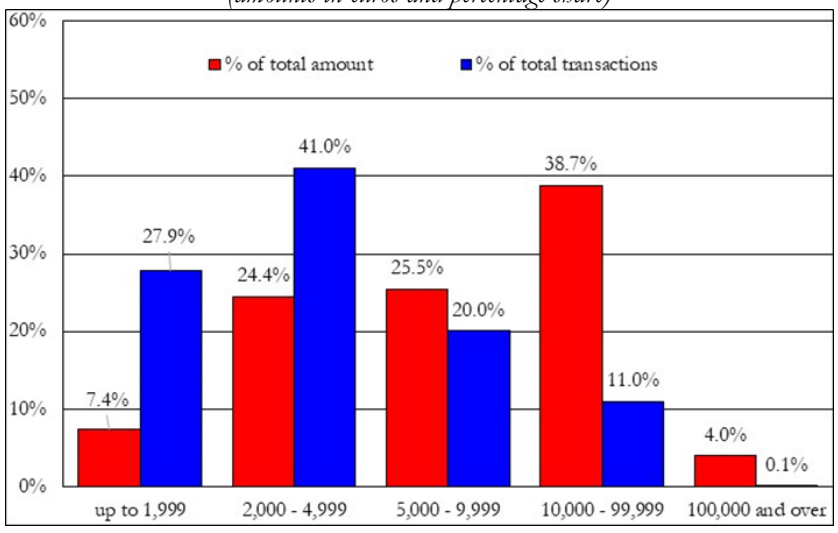
Reporting entities

At the end of 2024, there were 641 registered reporting entities. Banks, from which 99.3 per cent of the amounts reported in the threshold-based communications originate, constitute the vast majority of active reporting entities (343 out of a total of 361; Table 4.1).[11] The other types of operators (PIs and EMIs) account for less than 1 per cent of the amounts because their transactions are generally below the reporting threshold.

Figure 4.3

Threshold-based communications: transactions classified by amount

(amounts in euros and percentage share)



[11] 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.

Table 4.1

Transactions contained in threshold-based communications by type of reporting entity

	Amounts		Number of transactions	Average amount
	(millions of euros)	*(% share)*	*(thousands)*	*(euros)*
Total	**244,477**	**100.0**	**45,735**	**5,346**
Banks and Poste Italiane	**242,698**	**99.3**	**45,337**	**5,353**
Top 5 reporting entities	151,814	62.1	27,923	5,437
Other obliged entities	90,884	37.2	17,415	5,219
Payment institutions and points of contact of EU payment institutions	**1,434**	**0.6**	**272**	**5,270**
Electronic money institutions and points of contact of EU electronic money institutions	**345**	**0.1**	**125**	**2,749**

Data quality controls

The Unit continued to monitor the quality of the data flows submitted by obliged entities. Although the main anomalies identified in previous years have generally been corrected, widespread reporting errors, inconsistencies, and incomplete data have persisted. These were examined with the relevant reporting entities and duly resolved through the submission of corrective flows.

In light of these findings, and to improve the reliability of the information, the system of automated controls applied during the data acquisition phase was revised. The new controls, which came into effect in October 2024,[12] allowed for a more accurate representation of specific cases and a closer alignment of the acquired data with the guidelines set out in the document 'Information and data in threshold-based communications' (only in Italian). The Unit will continue to monitor the commitment of obliged entities to improving data quality over time, including during inspections.

4.2. SARA reports

In 2024, there was an increase in both the number of transactions underlying SARA data (+5.1 per cent) and in the total value of amounts (+8.1 per cent), confirming the upward trend observed over the past three years (see Table 4.2). More than 97 per cent of the amounts reported came from the banking sector, which accounts for around 30 per cent of the reporting entities.[13]

Statistical controls identified approximately 25,000 anomalous records involving 770 intermediaries (including 405 banks). In 5.4 per cent of the cases, the reporting entities found errors and corrected the transmitted data; 111 cases were investigated to assess whether an STR should be sent; and 119 cases were found to be related to STRs already transmitted to the UIF. Requests for assistance regarding SARA and ORO data (about 1,350) continue to decline, owing to the stability of the regulatory framework and the increasing operational quality of reporting entities.

[12] See UIF Communication (only in Italian) of 14 May 2024.

[13] The SARA data are subject to correction by the reporting entities; the data used in this chapter is updated to 7 March 2025.

The total value of cash transactions was €173.4 billion (-3.4 per cent compared with 2023). This included a decrease in withdrawals (to €8.9 billion, -4.3 per cent) and deposits (to €164.5 billion, -3.3 per cent).[14] A decline in amounts was observed in 99 out of 107 provinces.

The total number of cash transactions also fell (-2,3 per cent). Figure 4.4a highlights the difference in the propensity to use cash between Central-Northern Italy and the South.

Table 4.2

Aggregate anti-money laundering reports (SARA reports)

	Number of reporting entities - 2024	**Total amount** *(billions of euros)*	**Number of underlying transactions**
Banks, Poste Italiane and CDP	438	52,514	499,369,841
Asset management companies	259	376	13,282,983
Other financial intermediaries	193	426	7,603,763
Trust companies	182	18	103,128
Investment firms	123	118	2,735,767
Insurance companies	68	195	4,793,591
SICAFs	68	1	904
Payment institutions and points of contact of EU payment institutions	64	79	33,634,876
Trusts under Article 106 of the Consolidated Law on Banking	33	120	557,832
Electronic money institutions and points of contact of EU electronic money institutions	22	157	77,943,221
Total	**1,450**	**54,004**	**640,025,906**

Anomalies in the use of cash

The econometric analysis developed some time ago by the Unit[15] has classified the diffusion of cash on the basis of its use, identifying the share of cash operations considered physiological (i.e., attributable to socio-economic and financial factors such as the diffusion of alternative payment instruments and the availability of financial services in the area). This approach enables the isolation of the anomalous component, not explained by these factors, which may be indicative of potential illicit activities (see Figure 4.4b).

In 2024 too, anomalous uses of cash were more concentrated in the provinces of Central and Northern Italy. Compared to the previous year, there was a significant increase in the risk of cash-related money laundering in the northern provinces of Rimini, Mantua, Verbano-Cusio-Ossola and Monza-Brianza, as well as in Potenza in the South; the most marked decrease was in the districts of Pistoia, Massa Carrara, Grosseto and Pesaro-Urbino.[16]

In the SARA data, the majority of incoming and outgoing transactions consist of bank transfers, which – along with remittances – include information on the location of the counterparty and their financial intermediary. In 2024, the value of foreign transfers reached

[14] The total value is lower than that recorded for threshold-based communications (€244.5 billion) due to the differences in the thresholds envisaged and in the criteria for their application (€10,000 in total, even when several transactions are individually worth more than €1,000 per subject and month, in the case of threshold-based communications, and €5,000 per transaction in the case of SARA data).

[15] 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.

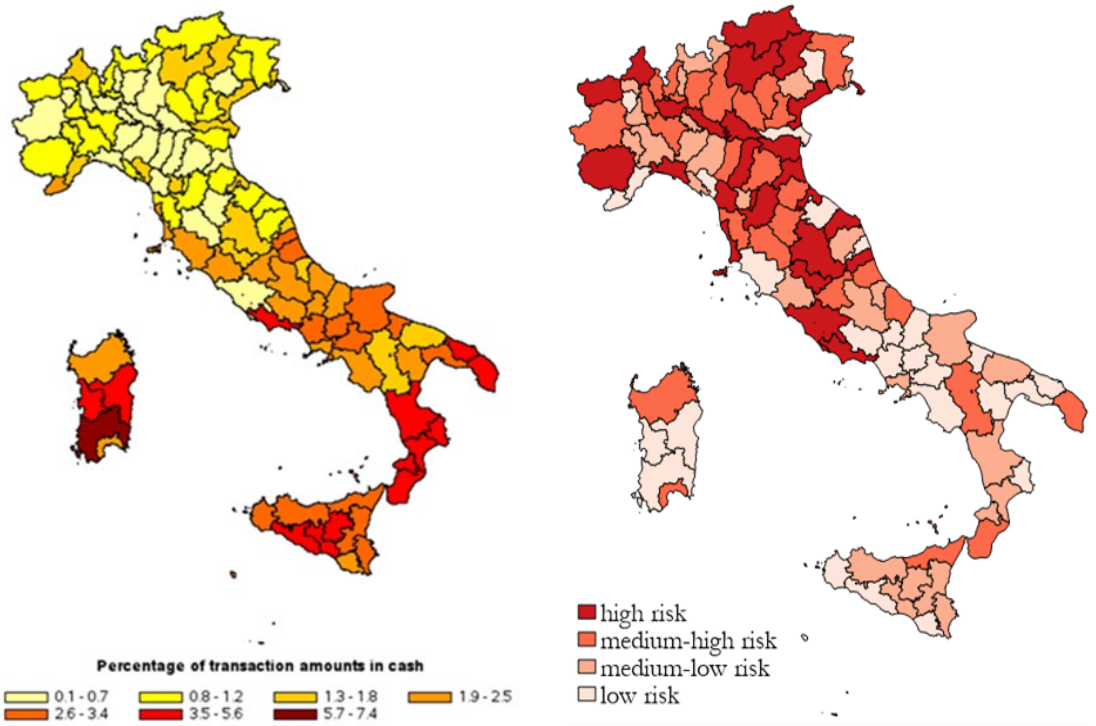
[16] Only provinces for which a change of two risk classes, positive or negative, was observed were mentioned.

€4,417 billion (+3.2 per cent, with similar changes in outgoing and incoming flows (Table 4.3).

Figure 4.4

Use of cash and anomalies, by province
2024

a) Use of cash (1) (2) **(b) Anomalies in the use of cash** (3)



(1) Share of cash transactions in total transactions. - (2) For uniformity with the preceding years, the SARA data used do not include the transactions of general government or of financial and banking intermediaries resident in Italy, in the European Union or in countries considered equivalent by the MEF Ministerial Decree of 10 April 2015. - (3) Preliminary results. The target variable (use of cash) is updated to 2024, some explanatory variables to 2022 (the last year available as of March 2025). The shadow economy is measured as a share of underground economy at the province level, as estimated by Istat.

Flows with EU countries increased compared with the previous year (+3.7 per cent incoming and +6.0 per cent outgoing), accounting for 70.0 per cent of total cross-border wire transfers. In contrast, transactions involving non-EU countries remained broadly stable overall, with a 2.7 per cent decrease in outgoing flows and a 2.0 per cent increase in incoming flows.

Flows with tax havens

Cross-border flows with low-tax or non-cooperative jurisdictions[17] declined significantly in both directions. This trend was largely influenced by Switzerland's removal from official lists, as the country alone had accounted for over 43 per cent of total flows to/from high-risk jurisdictions in the previous year. Compared to the previous year, Switzerland and South Africa were no longer among the top ten counterparties, while

[17] The list of non-cooperative countries and/or tax havens used is taken from the ministerial decrees implementing the TUIR (Ministerial Decree of 4 May 1999) updated in July 2023, the lists published by the FATF in February 2024, the 'EU list of non-cooperative jurisdictions for tax purposes' (updated in February 2024) and the list of countries identified by the European Commission in Delegated Regulation (EU) 2016/1675 as amended by Regulation (EU) 2024/163. Compared to the analysis published in UIF's 2023 Annual Report, Croatia and Bulgaria (added to the FATF grey list in June and October 2023, respectively), Cameroon, Kenya, Namibia, and Vietnam were included, while Albania, Cambodia, Jordan, Morocco, and Switzerland were removed.

Bulgaria and Croatia were added to the official lists in 2024. The changed composition of high-risk jurisdictions compared to 2023 had a notable impact on the provincial incidence of these flows as a share of total foreign transfers (see Figure 4.5).

As with cash, by means of an econometric analysis, it is possible to distinguish the provincial component of foreign transfers that can be traced back to economic and financial fundamentals from the anomalous component, as it cannot be justified based on these factors (see Figure 4.5b).

The highest anomalies in outgoing flows were observed in northern areas (Liguria and the provinces of Biella, Sondrio, Trento, Trieste, Gorizia, and Rimini), in central regions (Tuscany and Marche), and in parts of the South (Molise and Puglia). For incoming flows, a higher incidence of high-risk provinces also emerged in some central areas and, more markedly, in Puglia, Calabria, Sicily, and Sardinia.

Table 4.3

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

	Outgoing	Incoming	Total
Total	**2,109**	**2,308**	**4,417**
to EU countries	**1,488**	**1,604**	**3,092**
France	451	500	951
Germany	401	411	812
Netherlands	117	130	247
Belgium	104	116	220
Luxembourg	82	105	187
to non-EU countries	**621**	**704**	**1,325**
United Kingdom	294	295	589
United States	104	136	240
Switzerland	41	71	112
China	26	13	39
Serbia	11	11	22
***of which*: tax havens**	**82**	**95**	**177**
Abu Dhabi	15	15	30
Turkey	13	17	30
Russian Fed.	6	12	18
Hong Kong	10	8	18
Dubai	5	6	11
Bulgaria	5	6	11
Singapore	5	5	10
Croatia	4	5	9
Monaco	3	4	7
Taiwan	2	2	4

(1) See Figure 4.4, note 2.

Figure 4.5

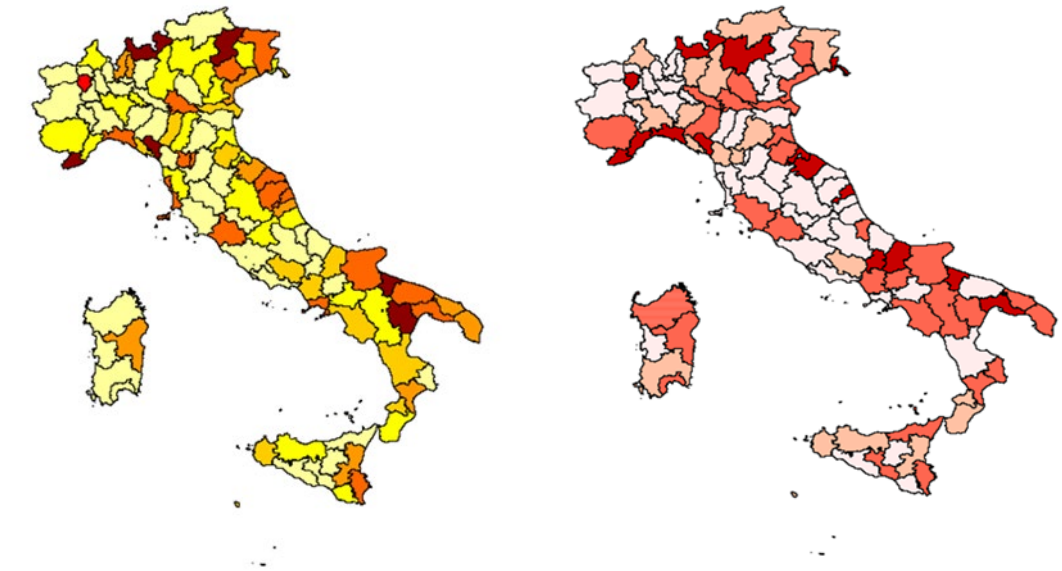
Credit transfers 'at risk'

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

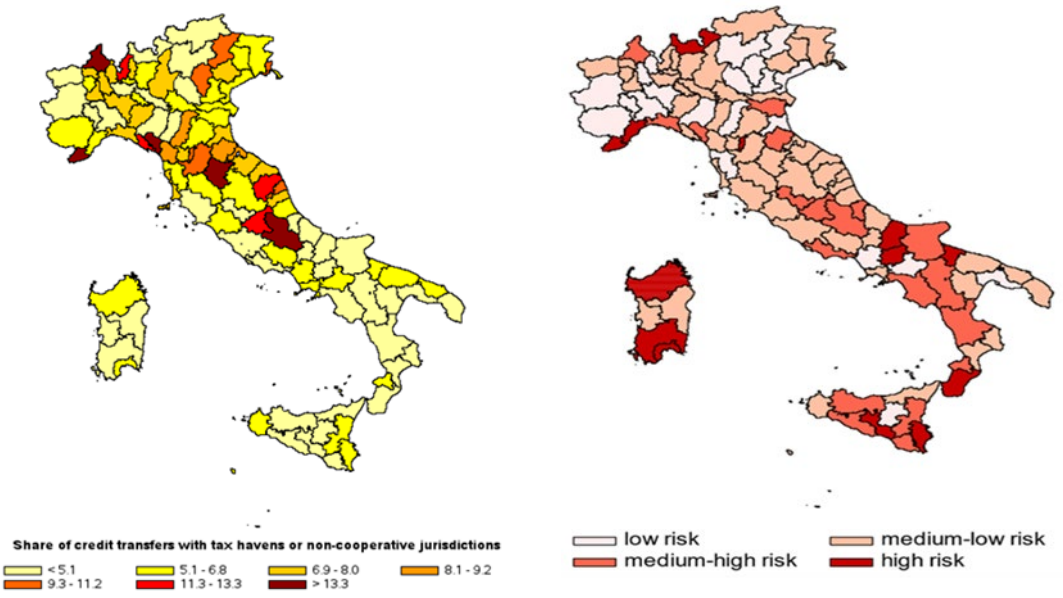
b) Anomalies in cross-border credit transfer (2)

2024 **2023**

Outgoing cross-border credit transfers



Incoming cross-border credit transfers



(1) See Figure 4.4, note 2. - (2) The maps on anomalies refer to 2023, the latest year for which all the data needed to estimate the model are available.

4.3. Gold declarations

In 2024, advance declarations recorded a trend reversal compared to the previous year, increasing in value by 21.9 per cent (Table 4.4).

Table 4.4

Declarations of gold transactions

	Advance declarations (1)		**Ex-post declarations**		
	Number of declarations (transactions)	**Declared value** *(millions of euros)*	**Number of declarations**	**Number of transactions**	**Declared value** *(millions of euros)*
Sales	1,406	1,020	60,182	145,905	36,639
Gold loan (concession)	2	2	1,303	2,401	1,382
Gold loan (restitution)	0	0	377	676	292
Other non-financial transactions	1	0	214	243	175
Transfer export–import	24	4	279	360	656
Collateral awards	0	0	10	11	0
Investment gold delivery services	2	7	23	35	11
Total	**1,435**	**1,033**	**62,388**	**149,631**	**39,155**

(1) Advance declarations refer to transfers of gold abroad and must be made before crossing the border. If the transfer implies a sale or a financial transaction, this transaction must be included in the ex-post monthly declarations.

The most frequently reported type of operation continues to be sales, representing 98.7 per cent of the total. Ex-post declarations also recorded a significant increase, with an overall rise in declared value of 45.7 per cent.[18] Among ex-post declarations, purchase and sale operations – representing 93.6 per cent of the total – grew by 47.0 per cent. Other categories also showed notable increases, including loans for use in restitution (+124.7 per cent), delivery services for investments (+474.3 per cent), and other non-financial operation, which posted an 873.1 per cent increase in value. The remaining categories exhibited less marked growth. The growth in declared value was driven by increases in both the average declared gold price (+22.1 per cent) and the quantity of gold traded (+19.3 per cent; Figure 4.6).

Categories of reporting entities

The number of participants in the gold transaction reporting system increased by 144, reaching 1,214 participants (Table 4.5). The number of active reporting entities also grew by 72 units, including 38 individuals. Professional operators continue to submit the majority of both advance and ex-post declarations, with an 89.4 per cent share, while the share of banks remained stable at 9.6 per cent.

[18] The ORO data are subject to correction by the reporting entities; the data used in this chapter is updated to 17 February 2025.

Figure 4.6

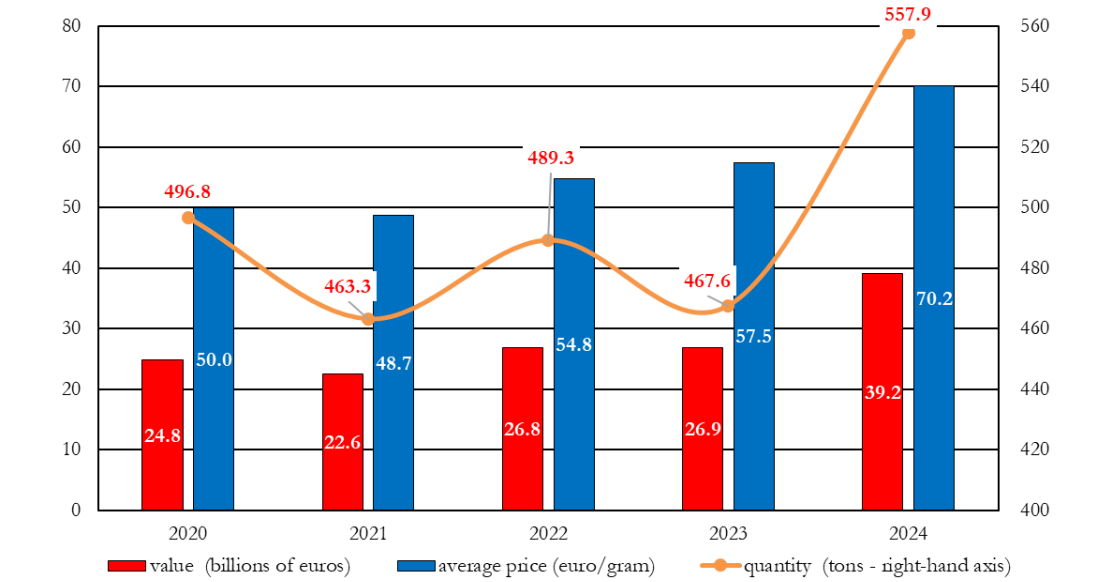


Table 4.5

Reporting entities engaged in gold transactions

	Number of reporting entities registered	Number of reporting entities active in the year	Number of declarations
Banks	56	24	6,127
Professional gold dealers	550	411	57,049
Other, natural persons	447	83	273
Other, legal persons	161	30	374
Total	**1,214**	**548**	**63,823**

Transactions with foreign countries

Transactions with foreign countries increased by 46,6 per cent compared with the previous year. The main counterparty countries, accounting for 83.7 per cent of the value of foreign gold transactions, remain the United Kingdom (37.5 per cent), Switzerland (16.0 per cent), Turkey (10.8 per cent), the United Arab Emirates (9.0 per cent), the United States (6.5 per cent) and Canada (4.0 per cent). The most significant changes concern the increase in the percentage share of Turkey (+5.1 percentage points) and a decrease in those of Switzerland (-2.4) and the United Arab Emirates (-2.7).

4.4. Strategic analysis

The strategic analysis aims to identify vulnerabilities, schemes and trends to better understand money laundering phenomena or factors that may undermine the effectiveness of the prevention system. The UIF conducts its strategic analysis along two main lines. The first involves the examination of STRs to identify new laundering schemes and anomalous behaviours. The second focuses on financial flows and laundering phenomena by economic sector, geographic area, and payment instruments, in order to assess their risks and describe their dynamics.

Organized crime infiltration into the economy

The strategic analysis dedicated to monitoring the risks linked to organized crime infiltration into the legal economy has continued. In this context, a project was completed to explain and classify the motives that drive criminal organizations to penetrate the legal economy.

Methods of organized crime infiltration into the legal economy

The study[19] presents a conceptual framework that explains and classifies the motives behind organized crime infiltration into the economic fabric.

These motives largely fall into three main categories. The first, 'functional', relates to firms that directly support criminal activities – e.g., facilitating money laundering, as is the case with shell companies, or employing individuals to gain consensus and control over specific territories. The second, 'competitive', involves firms that benefit from illicit activity by increasing their competitiveness and ensuring further profits for criminal organizations – for instance, by using intimidation to secure market share. The third, 'relational', is based on the use of firms to expand the criminal organization's network of contacts, thus laying the groundwork for further growth and profit.

Empirical evidence shows that companies founded by criminal organizations are primarily driven by functional motives. In contrast, mid-sized firms, often infiltrated post-establishment, tend to reflect competitive motives. Larger, well-established firms, also infiltrated after their establishment, are typically used for relational purposes. The latter scenario entails a significantly higher risk of sustained criminal presence in the economy.

This classification has important implications for countermeasures. Unlike transactions carried out by firms in the first two categories, which are more likely to be detected due to their direct involvement in criminal activity, transactions linked to relationally infiltrated firms are far less likely to be detected. Tackling this form of infiltration therefore requires supplementing conventional investigative techniques with enhanced economic and financial analysis capabilities – including the development of predictive algorithms to flag potentially collusive firms.

Local public administrations and organized crime

A further serious and widespread threat is the influence exerted on local general government bodies. In 2024, a dedicated project was completed to examine the ties between organized crime and local administrations in Italy.

The risk of mafia infiltration in Italian public administrations

The study analyses mafia infiltration in Italian municipalities between 2016 and 2021, using data on municipal councils dissolved due to mafia infiltration, as well as figures on the main revenue and expenditure items of municipal budgets.

By comparing municipalities that were disbanded due to mafia infiltration with a control group of municipalities with similar characteristics that were not dissolved, the analysis identifies distinct expenditure patterns. These include higher operational costs, rigid expenditure structures, and the misallocation of funds to sectors often exploited by organized crime, such as construction and waste management, both strategic for money laundering. Furthermore, in the dissolved municipalities, a lower efficiency in revenue collection was observed – attributable either to weaker administrative capacity or to deliberate tax exemptions for politically connected actors.

The study also develops a machine learning algorithm to estimate the risk of infiltration across all Italian municipalities, especially those not yet dissolved. Validation exercises show that higher risk scores are associated with lower transparency in public

[19] See J. Arellano-Bover, M. De Simoni, L. Guiso, R. Macchiavello, D. J. Marchetti e M. Prem, '*Mafias and firms*', UIF, Quaderni dell'antiriciclaggio – Analisi e Studi, 24, 2024.

procurement, as measured by a UIF-developed indicator,[20] and a higher concentration of firms potentially linked to organized crime within the same territories.

Strengthening institutional cooperation

An agreement was signed with the Central Directorate of Criminal Police at the Ministry of the Interior and with the Anti-Mafia Investigation Directorate (DIA) to facilitate the systematic exchange of information flows regarding UIF's experimental risk indicator on criminal infiltration in Italian limited companies – developed using financial statement data.[21]

As part of the broader framework for anti-money laundering measures, further investigations were carried out in 2024 on tax irregularities among Italian businesses and their improper receipt of public subsidies.

'Interposed' companies and …

A study was completed on 'interposed' companies i.e., those positioned between shell companies and the companies actually active in carrying out VAT fraud schemes. Unlike shell companies, these firms possess production assets and use the banking system to finance their operations. However, like shell companies, and unlike fully operational businesses, they exhibit significantly faster liquidity cycles, largely driven by the issuance and receipt of false invoices used in fraudulent schemes.

… the offences committed by firms benefiting from public subsidies

Simultaneously, work continued on developing indicators to identify irregularities in the use of public funds. This involved comparing the characteristics of all businesses receiving public support with those of firms – receiving the same forms of funding – that have been reported via STRs for a connection with suspected misappropriation. The analysis confirmed that some features, such as recent incorporation or sharp increases in share capital, are more frequently associated with illicit conduct.

Active cooperation

Concerning active cooperation by reporting entities, a statistical methodology was also developed to estimate the degree of potential underreporting of STRs by banks, based on the characteristics of intermediaries and territorial context factors – used as proxies for exposure to money laundering risk.

Child pornography

A pilot project was launched to apply machine learning in the fight against child pornography. Using a sample of STRs previously classified as related to such offences, the model aims to identify additional STRs potentially linked to this crime.

Risk profiles derived from gold declarations

The gold declarations database was also intensively used. A first area of investigation concerned compliance with the reporting obligations underlying gold data transmission and the money laundering risks faced by sector operators. Domestic and cross-border gold trade trends and client profiles were also analysed in order to detect potential anomalies. In parallel, joint analysis of the databases on gold declarations, STRs, and threshold-based communications was initiated, incorporating external sources as well, to build anomaly indicators that leverage all available information. Finally, the experiment launched last year on applying social network analysis to transactions derived from gold declarations was further developed.

Identifying anomalies in SARA data

SARA data are continuously monitored to detect both macroeconomic discontinuities in foreign wire transfer flows to and from Italy, and potentially anomalous individual positions. In addition to the reporting intermediaries, the activity may require the cooperation of other relevant authorities. The investigations initiated in this context have focused on the

[20] See M. Gara, S. Iezzi e M. Siino, *'Corruption risk indicators in public procurement: A proposal using Italian open data'*, UIF, Quaderni dell'antiriciclaggio – Analisi e studi, 23, 2024.

[21] See P. Cariello, M. De Simoni e S. Iezzi, *'A machine learning approach for the detection of firms linked to organized crime in Italy'*, UIF, Quaderni dell'antiriciclaggio – Analisi e studi, 22, 2024.

foreign and cash operations of non-profit organizations, as well as flows potentially linked to the shadow banking phenomenon.

National Analysis of money laundering risks

The UIF, in collaboration with all actors of the Italian anti-money laundering system, contributed to the update of the National Analysis of the risks of money laundering and the financing of terrorism, covering the period 2019–2023. On one hand, corruption, extortion, tax evasion and offenses, drug trafficking, and bankruptcy and corporate crimes were identified as highly significant threats. On the other, the widespread use of cash and the extent of the shadow economy represent the main systemic vulnerabilities. The vulnerabilities of each sector subject to anti-money laundering obligations were examined. Particularly high-risk scenarios emerged from the analysis of suspicious transaction reports (STRs): unusual activity involving the increasing use of crypto-assets, transactions carried out through virtual IBANs and correspondent accounts, and the undue receipt of public funds from the NRRP (National Recovery and Resilience Plan) or from publicly guaranteed loans. Finally, the inherent risk of terrorist financing was assessed as fairly significant.

5. INSPECTIONS

5.1. Inspections and off-site controls

In 2024, the UIF initiated 20 inspections, 19 general and one targeted, as well as four off-site controls (Table 5.1). The obliged entities subject to inspection were selected based on specific risks or vulnerabilities, taking into account issues of concern that had emerged from previous inspections or from STRs filed by other obliged entities.

Table 5.1

Inspections and off-site controls

	2020	2021		2022		2023		2024	
Total	**3**	**10**	**4**(1)	**16**	**1**(1)	**17**	**17**(1)	**20**	**4**(1)
Banks	2	6	1	5	1	7	12	3	-
Trust companies	-	1	-	1	-	2	-	1	-
PIs, EMIs and other financial interm.	1	1	3	4	-	3	3	5	-
Asset management companies and securities investment firms	-	-	-	-	-	1	-	-	-
Insurance companies	-	-	-	-	-	-	-	-	-
Gaming service providers	-	-	-	1	-	1	-	5	1
Other entities (2)	-	2	-	5	-	3	2	6	3

(1) Off-site controls. - (2) Including debt collection companies, auditing firms, valuables-in-transit companies, real estate agencies, gold traders or manufacturers, auction houses, VASPs, and Crypto-Asset Service Providers (CASPs).

As usual, the audits took place in a context of constant liaison and cooperation with the sector supervisory authorities and the investigative and judicial bodies. Cooperation between the UIF and Banca d'Italia also materialized this year through the mutual participation of staff in some inspections.

Inspection findings

Inspections at some banks revealed that the collection and assessment of information for the purpose of filing STRs did not always follow risk-proportionate criteria, particularly regarding the origin of funds invested in foreign investment funds not subject to regulation or oversight by a national supervisory authority. Weaknesses were also observed in arrangements aimed at ensuring active cooperation, especially regarding enhanced due diligence, the monitoring of customer transactions by the territorial network, and the effectiveness of controls on the network itself.

Specifically, some institutions failed to incorporate significant information into risk profiling, such as clients' involvement in investigations formally notified to the inspected entity. Cross-border transaction monitoring procedures were found inadequate in detecting anomalies due to the failure to adapt these tools to clients' specific operational features. The inspections highlighted recurring transactions corresponding to known indicators or anomaly patterns – especially those relating to tax crimes – that triggered alerts but were not properly evaluated by the territorial network for active cooperation.

The inspections conducted at a credit guarantee consortia revealed a general underestimation of anomalies relating to the issuance of guarantees, potentially relevant for AML/CFT purposes. In co-financing activities carried out jointly with a bank, there was no investigation into the origin of the funds used for repayment, particularly in cases of early or near-immediate loan repayment. Also lacking was the identification of shared elements among multiple businesses or their representatives, which could have helped detect more complex anomalies.

One inspection in the fiduciary services sector, where clients are engaged remotely, revealed issues in customer profiling and transaction monitoring. Risk profiles were not updated, even in the presence of STRs sent to the UIF or investigative interest from authorities. Ongoing transaction monitoring was not assisted by IT tools. Furthermore, the capacity to detect suspicious transactions was hampered by the absence of feedback or updates regarding the data collected, e.g. on the financial situation of the client or the origin of the funds. Operational practices also failed to document the evaluation process for flagged anomalies deemed unworthy of reporting to the UIF.

In 2024, extensive ATM cash withdrawals, carried out with payment cards issued by an EU-based EMI operating under the freedom to provide services, were analysed. The off-site inspection revealed a concentration of withdrawals in areas known for high organized crime activity. Sequential use of multiple payment cards aimed to bypass cash withdrawal limits was also observed in these areas. International cooperation helped to investigate the phenomenon in depth, uncovering significant corporate, financial, and personal links among cardholders. Many operational patterns appeared tied to suspected invoice fraud, sometimes within organized crime contexts. Findings have been shared with the National Anti-Mafia Directorate (DNA).

Inspections continued in the gold and precious metals sector with the dual aim of increasing knowledge of the sector's operating practices and increasing the degree and quality of operators' participation in the AML prevention system. The inspections took into account, among other things, the characteristics of domestic and foreign transactions, especially with high-risk countries.

Risks in the gold sector – UIF initiatives

The gold and precious metals sector carries multiple ML/FT risks. Gold has always been globally recognized as a cash-equivalent exchange medium and is highly attractive for money laundering and terrorist financing due to its high intrinsic value, low traceability, and ease of being smuggled as small objects (scrap gold).

The national market features numerous, often small-scale operators with different business models, a significant volume of transactions with non-EU countries – also considered risky as regards AML aspects and the foreign supply chain for precious metals. Some segments of the market (e.g. gold traders) also rely heavily on cash and the widespread use of metal in trade-based money laundering schemes as an underlying commodity and as an alternative form of value.

Operators in this sector are subject to various national and supranational regulations that serve complementary goals in combating money laundering and related offenses. However, the lack of a dedicated supervisory authority has hindered both risk analysis and the implementation of tailored secondary regulations.

Participation in the AML/CFT system remains limited to a small number of operators, in terms of STRs transmitted to the UIF, and modest in terms of quality and quantity (2,344 transactions in 2024).

The inspections conducted by the Unit at major sector operators revealed low awareness of AML obligations, reflected in regulatory and operational safeguards inadequate to prevent money laundering risks.

Shortcomings were found in due diligence, record-keeping, and the detection and reporting of suspicious transactions. Information collected about foreign suppliers as part of supply chain due diligence procedures was not used for active cooperation purposes

nor assessed for consistency and compatibility with the client's subjective, economic and financial profile.

In November 2024, the UIF held a seminar for gold sector operators, aimed at training and raising AML/CFT awareness. Speakers included representatives from competent authorities and industry associations. The event covered sector risks and regulatory developments, while also discussing the critical elements found during the inspection activity, the financial analysis of the STRs and the checks conducted on the gold declarations made pursuant to Law 7/2000. The initiative helped investigate the shortcomings in the application of reporting obligations and to strengthen cooperation with industry associations.

Inspections in the gaming sector revealed AML control weaknesses. The available customer information was not proportionate to the risks, and tools for detecting potential anomalies were limited. Furthermore, possible synergies from sharing information on customers among gaming companies belonging to the same group were not being leveraged for active cooperation. During remote customer onboarding, appropriate checks on the authenticity of the identification documents provided were not always carried out. Weaknesses were also found in the verification of potential anomalies relating to the use of non-cash payment instruments, such as payment cards not registered to the holder of the gaming account. Furthermore, there was a limited involvement of agents and physical top-up points in identifying potentially suspicious transactions carried out by customers. Further investigations – based on the use of threshold-based communications relating to cash transactions for control purposes – enabled the UIF to initiate inspections on two gaming service providers who were recipients of significant fund transfers originating from payment cards. These cards had been mostly topped up using cash and were registered to individuals who appeared to be connected to each other.

Inspections conducted at auction houses confirmed the presence of inadequate AML safeguards. Processes for risk profiling of customers, transaction monitoring, and identification and assessment of potentially suspicious transactions were found to be missing. Data retention procedures, often limited to paper-based formats, were not adequate to ensure compliance with legal requirements. In many cases, no independent inquiries were made into the origin of the goods submitted for auction, with reliance placed solely on the direct knowledge of the customer and on the established practice of sending auction catalogues to investigative authorities in advance. Transactions carried out with winning bidders were mostly occasional in nature and, even when involving amounts above legal thresholds or otherwise significant, no information was gathered regarding the origin of funds or their consistency and compatibility with the customer's profile.

In 2024, off-site inspections were concluded on two major real estate intermediaries affiliated with banking groups. The inspections revealed that significant information – such as the actual business activities carried out by the client or the origin of the funds used – was not being obtained. The ability to detect suspicious transactions was impaired by the limited availability of information regarding payments made during the real estate transactions, as well as concerning individuals later designated as buyers (Article 1401 of the Italian Civil Code).

As usual, the UIF informed the other supervisory authorities of the results of the checks for the aspects falling within their respective competencies (see Section 'Cooperation with other authorities' in Chapter 6).

5.2. Sanction procedures

In 2024, the UIF initiated eight sanctioning proceedings for failures to report suspicious transactions, ascertained during inspections. Two sanctioning procedures were initiated for violations of the restrictions on the use of cash, as set out in Article 49(1) of Legislative Decree 231/2007, against an auction house and a gaming and betting licensee. A sanctioning proceeding was also launched for the breach of the ban on transferring luxury goods – including works of art and collectibles – with value exceeding the legal threshold,[22] within the framework of financial sanctions adopted by the EU in connection with the Russia-Ukraine conflict.

The UIF handled the preliminary phase of nine sanctioning proceedings concerning gold transfers – the Italian Ministry of Economy and Finance (MEF), as the competent authority for the decision-making phase, endorsed the UIF's assessments and imposed the related sanctions.

Table 5.2

Administrative irregularities

	2020	2021	2022	2023	2024
Failure to report suspicious transactions	12	4	9	2	8
Failure to submit aggregate data	1	-	-	-	-
Violation of Article 49(1), Leg. Decree 231/2007	1	-	1	-	2
Failure to declare gold transactions	12	13	11	8	9
Failure to freeze funds and assets	-	-	2	-	1

In cooperation with Banca d'Italia, the UIF continued its systematic participation in their respective collegial bodies responsible for assessing irregularities, in order to ensure the effective enforcement of AML sanctioning regulations. In some cases, the findings from the UIF's supervisory activity were used by Banca d'Italia to adopt measures within its own remit.

[22] Regulation (EU) 833/2014, as amended by Regulation (EU) 428/2022.

6. COOPERATION WITH OTHER AUTHORITIES

6.1. Cooperation with the judicial authorities

In 2024, the judicial authorities and the Delegated Investigative Bodies forwarded 373 requests for cooperation (-9.2 per cent compared with the previous year). Responses provided by the UIF fell by 4.6 per cent, due to a reduced time window within which the Unit supplies follow-up information after the initial reply. The number of STRs submitted increased by 7.9 per cent, a rise attributable to the complexity and scale of the contexts arising from some requests made by the judiciary (Table 6.1).

Table 6.1

Cooperation with judicial authorities

	2020	2021	2022	2023	2024
Requests for information from judicial authorities	558	510	313	411	373
Responses to judicial authorities (1)	1,188	1,463	1,059	777	741
Number of STRs forwarded	2,927	3,420	2,854	2,756	2,975

(1) 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.

Cooperation and dialogue with foreign FIUs (Art. 12)

Specific cooperation requests from the judicial authority concerned investigations into organized crime, money laundering and self-laundering, fraud, corruption, unauthorized financial activity, false statements, and breaches of immigration regulations. The activation of international cooperation (see Section 'Cooperation with foreign FIUs' in Chapter 7) covered cases of fraud, most often perpetrated online and also involving investments in crypto-assets, as well as investigations into tax crimes, mafia crime, unauthorized financial activities, corruption and other crimes against public administrations, terrorism, and criminal association aimed at international drug and human trafficking.

The main foreign counterparties activated at the request of the judicial authority in 2024 were the FIUs of Lithuania, Spain, Luxembourg, Switzerland, the United Kingdom, Belgium, Germany, and Ireland.

Memorandum of Understanding between the UIF and the Finance Police

In July 2024, the UIF and the Finance Police signed a Memorandum of Understanding on preventing the use of the financial system for money laundering and terrorist financing purposes. The agreement aims to consolidate all areas of cooperation between the two authorities and manage them in an organized way, including coordination of supervisory activities, with the goal of more effectively directing their respective efforts toward high-risk sectors and phenomena, and strengthening international cooperation through the sharing of information exchanged with foreign FIUs. The new agreement outlines procedures through which the UIF provides the NSPV with STRs and other information exchanges for developing risk indicators. It also establishes regular dialogue on novel or complex cases, the development of advanced analytical methods, and confidentiality safeguards. The Memorandum foresees research activities on emerging forms of crime and innovative laundering channels, as well as training events for staff and obliged entities to improve the quality of active collaboration. Implementation of the agreement is overseen by a steering committee and operational working groups.

The total number of complaints under Article 331 of the Italian Code of Criminal Procedure made within the framework of the technical reports submitted to the investigative bodies decreased slightly (Table 6.2). Among these are the complaints regarding the misuse of the UIF's name and logo submitted again in 2024 by the Unit.[23]

Table 6.2

Reports to judicial authorities					
	2020	**2021**	**2022**	**2023**	**2024**
Reports pursuant to Article 331 of the Italian Code of Criminal Procedure	257	508	408	436	417
of which: submitted to the judicial authorities	1	0	0	2	3
made in connection with technical reports sent to investigative bodies	256	508	408	434	414
Informative reports for investigative purposes	11	3	6	0	3

6.2. Cooperation with supervisory authorities and other institutions

Supervisory authorities

In 2024, the Unit submitted 49 AML/CFT disclosures to the sector supervisory authorities. The reports to the Directorate General for Financial Supervision and Regulation and to Banca d'Italia's Anti-Money Laundering Supervision and Regulation Unit concerned, among other matters: the granting of loans backed by public guarantees, including in relation to fictitious capital increases by the beneficiary companies; fund transfers, presumably originating from scams, carried out via foreign money transfer operators that appear to provide remote payment services without authorization; unusual concentrations of financial flows, traceable to Chinese nationals, executed by Italian intermediaries to recurring foreign counterparts; repatriation from abroad of funds of suspected illicit origin through a trust company; activity of bank clients involving numerous transactions to and from gaming and betting operators; possible inconsistencies between the actual use of funds raised in an equity crowdfunding initiative and the real estate project allegedly financed. Disclosures to Consob included possible online trading scams, suspicious conduct by an asset management company's financial advisor, and information concerning two listed companies related to shareholding transfers, possibly aimed at circumventing EU restrictions on transactions involving Russian counterparts and potentially constituting insider trading. With Ivass, insights were shared regarding suspected unlawful activity and fraud in the insurance intermediation sector.

Other institutions

The findings of an inspection at a non-supervised trust company were shared with the Italian Ministry of Enterprises and Made in Italy and Revenue Agency, for assessment of the trust company's ownership structure compliance with the Agency's guidelines. The results of inspections at gaming service providers were submitted to the Customs and Monopolies Agency.

The use of forms of partnership in the AML/CFT field has received positive recognition at international and European level. The creation of a joint public–private forum for sharing and discussion on strategic topics provides a valuable opportunity to enhance anti-money laundering and counter-terrorist financing efforts.

Public–private partnership

The UIF participates in a Public-Private Partnership (PPP) initiative with the Anti-Mafia Investigation Directorate (DIA) of Piedmont and Valle d'Aosta, the Economics and Finance Police Unit of the Finance Police of Turin, the AML Supervision and Regulation Unit of

[23] See UIF Communication (only in Italian) of 28 February 2024.

Banca d'Italia, Intesa Sanpaolo S.p.A., and Anti Financial Crime Digital Hub Scarl. The initiative – a pilot project with potential for nationwide extension – consists of a series of technical and methodological meetings aimed at enhancing the collective knowledge base and analytical approaches of all actors through the exchange of diverse perspectives and expertise. The UIF subsequently launched discussions with the SNA Unit of Banca d'Italia and with ABI to establish a new PPP initiative focused on identifying and sharing emerging AML/CFT risks and defining possible mitigation strategies. The initiative will involve public authorities and selected private stakeholders.

COLAF

Decree Law 19/2024 established the UIF's participation in the Committee for combating fraud against the European Union (COLAF), under the Presidency of the Council of Ministers – Department for European Policies. The UIF contributed to the drafting of the EU Anti-Fraud Architecture Questionnaire and participated in the October 2024 hearing of COLAF at the European Court of Auditors.

The Committee, chaired by the Minister for European Policies or a delegate, serves consultative and strategic functions for coordinating fraud and irregularity prevention in taxation, common agricultural policy, and structural funds. It also deals with issues relating to the flow of communications concerning the receipt of EU funding and the recovery of undue payments, as well as those relating to the drafting of questionnaires for the annual reports to be sent to the European Commission as required by Article 280 of the Treaty establishing the European Community. These functions now also cover the NRRP, in order to strengthen a unified strategy for preventing and combating fraud and other offences involving Plan-related funding, cohesion policies for 2021–2027, and associated national funds.

The UIF continues its engagement in the Open Government Partnership , a global initiative led by governments and civil society to promote transparency, participation, anti-corruption, accountability, and public sector innovation.

6th Action Plan for Open Government

The 6th National Action Plan for Open Government 2024–26 has begun, with the UIF involved in Objective A, 'Promote the culture of integrity and transparency in public decision-making processes', and specifically in Commitment 2, 'Spreading awareness of threats to the integrity of public decision-making processes and strengthening the skills of public administration and civil society organizations'.

Together with the National School of Administration and the Department of Civil Service, the UIF is conducting a new round of interviews with AML communication managers in several public administrations. The aim is to analyse organizational structures, practices, and procedures for identifying, assessing, and reporting suspicious transactions. The information gathered, structured around key factors relevant to the obligation to report, will be aggregated to develop a model of active AML cooperation for dissemination across a wide range of public sector entities to promote active cooperation.

6.3. International financial sanctions

In 2024 and 2025, the EU adopted further sanctions against Russia and Belarus. In addition to new restrictions, the freezing of funds and economic resources was extended to individuals and entities primarily linked to Russia's defence sector.[24] For Russia, a new

[24] For the 13th package of sanctions, see Regulations (EU) 2024/753 and 2024/745. For the 14th, see Regulations (EU) 2024/1746, 2024/1739, 2024/1745, and 2024/1776. For the 15th, see Regulations (EU) 2024/3183, 2024/3189, 2024/3192, and 2024/3177. For the 16th, see Regulations (EU) 2025/389, 2025/390, 2025/392, and 2025/395.

sanctioning regime was introduced with Regulation (EU) 2024/2642, featuring further restrictive measures against destabilizing activities.[25]

To improve the effectiveness of targeted financial sanctions, on 3 July 2024 the Council released the latest best practices for proper implementation of EU restrictive measures, especially clarifying the concepts of ownership and control by designated persons, essential for asset freezing obligations.[26]

The UIF issued specific notices to alert the private sector to newly designated subjects subject to freezing measures and checked for funds traceable to them held by Italian financial intermediaries. The findings of these checks were promptly shared with the FSC to enable it to take the measures within its powers to identify the resources to be frozen. The UIF, as a member of the Committee's Network of Experts, supported the drafting of authorization or denial measures for requests on the transfer of funds or resources concerning listed entities, as well as responses to queries about the implementation of EU regulation-based obligations.

Following a FSC measure of 9 May 2024, the UIF began collecting[27] new reports from credit and financial intermediaries concerning all non-EU fund transfers – direct or indirect – exceeding a cumulative amount of €100,000, made by EU-based legal persons, entities or bodies whose ownership is more than 40 per cent held by Russian persons.[28] With the UIF Communication (only in Italian) of 6 June 2024, the Unit defined the content, format, and submission procedures for these reports. A technical working group was set up at the FSC to analyse the information flows and support the identification of transactions, entities, or business sectors presenting a high risk of violating or circumventing the restrictive measures or a serious risk of misuse of funds for purposes inconsistent with those measures.

The group, which includes the Customs and Monopolies Agency, Finance Police, and the UIF, is in charge of carrying out a pre-analysis of the communications received by the MEF and the UIF, in order to identify possible violations and circumvention cases, as well as significant phenomena and patterns relating to transactions, entities, geographical areas or sectors at risk of circumventing EU sanctions. Their findings are submitted to the Network of Experts in order for the CSF to make subsequent decisions and to forward the conclusions to the European Commission.

After new designations under the sanctions regime against the Democratic People's Republic of Korea, the UIF issued a special notice and conducted standard checks for funds tied to newly listed entities. No new assets were identified for freezing in 2024 under this regime. The total value of frozen funds increased, mainly due to sanctions against Libya and Russia. For Libya, the update of frozen positions led to the identification of additional accounts linked to designated persons. For Russia, the increase was due to new designations during the year, additional frozen operations, and updates to already frozen positions. Except for Belarus, where one more transaction was frozen, changes in other sanction regimes were due to updates to existing frozen positions.

[25] The first designations – 16 individuals and 3 legal entities – were introduced with Regulation (EU) 2024/3188 of 16 December 2024.

[26] UIF, 'Quaderni dell'antiriciclaggio - Rassegna normativa' (only in Italian), 2nd half of 2024, pp. 11-13.

[27] The reporting obligation was introduced in December 2023 under Regulation (EU) 2023/2878.

[28] Art. 5-novodecies, Regulation (EU) 2014/833. See UIF, *Annual Report 2023*, pp. 53-54.

Table 6.3

Measures to freeze funds at 31/12/2024					
COUNTRIES AND ENTITIES	**Accounts and transactions frozen**	**Persons to whom freezes applied**	**Amounts frozen**		
			EUR	**USD**	**CHF**
ISIL and Al-Qaeda	3	3	5,252	0	0
Belarus	5	3	6,882	0	0
Iran	3	1	44,322	158,453	0
Lybia	9	2	15,319,073	0	0
Syria	22	5	12,819,518	244,592	144,251
Ukraine/Russia	197	89	279,155,530	0	0
DPR of Korea	3	4	7,897	0	0
Total	**242**	**107**	**307,358,474**	**403,045**	**144,251**

Representatives of the UIF took part in several meetings held within the framework of a project organized by the Council of Europe ('Effective implementation of the sanctions regime and enhanced cross-border cooperation in EU Member States'), aimed at strengthening the capacities of national competent authorities in identifying sanctioned entities and promoting the sharing of relevant information both at the domestic and cross-border levels.

7. INTERNATIONAL ACTIVITY

7.1. Cooperation with foreign FIUs

Requests to foreign FIUs

In 2024, the UIF exchanged information with 111 foreign FIUs. The Unit sent 723 requests for information, an increase compared with the previous year due to the greater information needs of the judicial authorities (see Table 7.1). The number of requests arising from internal analyses concerning cross-border operations remained substantially stable, with most cases concerning cash withdrawals made in Italy using foreign payment cards and the transfer to other countries of funds from government subsidies, particularly those relating to Italy's Superbonus tax credit for home renovations, mainly relating to energy efficiency, and to the NRRP. In numerous instances, international cooperation involved financial flows routed through virtual IBAN services provided by foreign payment service providers (PSPs) (see also the 'Tax Evasion' section in Chapter 2).

Cross-border STRs sent by the Unit to other European FIUs increased by approximately 17.3 per cent. Anomalies in prepaid card top-ups, suspected invoicing fraud, and the involvement of individuals under investigation in Italy were the most frequent phenomena.

Table 7.1

Information exchanges with foreign FIUs

	2020	2021	2022	2023	2024
Requests sent	**1,050**	**834**	**790**	**693**	**723**
of which: requested by judicial authorities	575	364	334	266	301
and required for internal analysis	475	470	456	427	422
Cross-border reports sent	**2,015**	**6,888**	**6,896**	**8,753**	**10,267**
Requests/spontaneous comm. received	**1,546**	**1,697**	**1,657**	**1,436**	**1,508**
Egmont network	695	872	776	634	638
FIU.NET channel	851	825	881	802	870
Cross-border reports received	**23,089**	**25,018**	**80,934**	**77,176**	**65,692**

Requests from foreign FIUs

The number of requests and spontaneous disclosures received has remained largely stable in recent years, although the level of detail and quality of the information has improved steadily. When handling requests from foreign FIUs, the Unit shares all the information in its possession or that it has the power to obtain in order to further investigate suspicious transactions. However, difficulties persist in accessing investigative information – which is often of particular interest to foreign FIUs – due to constraints in the national legal framework. These limitations hinder the timeliness and effectiveness of information exchange, unlike in the case of other administrative FIUs, including European ones. The need to ensure broader access to such information was also reiterated in the Sixth Anti-Money Laundering Directive. It is therefore desirable for national legislation to be aligned with the directions set out by the European legislator, promoting institutional synergies capable of overcoming the strict constraints currently in place.

Cross-border information received from other European FIUs remains significant, albeit in slight decline.[29]

Cross-border reports – Emerging phenomena

New methodologies for analysing cross-border reports are currently being explored in response to their considerable growth in recent years and to enhance the informational value of the data by identifying significant phenomena. These pilot initiatives involve the use of machine learning algorithms to identify typologies and categories automatically. Named Entity Recognition techniques are also being employed to extract structured data from unstructured texts (e.g. entities, amounts, relationships and locations).

The new classification criteria identify a broader range of phenomena and allow for the automatic selection of cases for priority processing, such as those relating to suspected terrorist financing. The initial trials have highlighted recurring phenomena, including the use of crypto-assets, cybercrime, child pornography and the involvement of individuals under investigation or linked to organized crime.

Cooperation for the suspension of transactions

Again in 2024, a significant number of information exchanges involved requests to freeze financial accounts or suspend suspicious transactions.

The UIF received 75 requests for assistance from foreign FIUs in identifying and recovering funds of potentially illicit origin transferred to Italy, for the purposes of asset recovery. In some cases, successful cooperation was facilitated by recall procedures initiated by the foreign intermediaries themselves; in others, by the freezing of financial accounts by Italian intermediaries. These latter measures enabled foreign FIUs to activate international judicial cooperation channels for the execution of seizures and confiscations. In another 47 cases, the FIUs reported to the Unit that they had applied suspension measures to accounts held abroad and asked whether the Italian authorities were interested in recovering the funds, often held by individuals under investigation in Italy. Given the short duration of such measures, often limited to a few days, the UIF promptly committed its investigative counterparts to determining whether the judicial authorities were interested in maintaining the freeze and pursuing recovery. In many instances, this interest was confirmed through the issuance of European Investigation Orders and precautionary measures executed via mutual legal assistance.

Cooperation cases

Cooperation with FIUs in Northern Europe has frequently concerned cyber frauds targeting foreign entities. The recovery of funds was often hampered by the rapid dissipation of illicit proceeds through instant wire transfers, purchases of crypto-assets, or cash withdrawals immediately after crediting funds. The illicit funds were frequently passed among various groups of individuals in an effort to layer the flows and hinder traceability. The wire transfers – often involving round numbers and large amounts – were generally linked to vague invoice payments and were inconsistent with the profiles of the individuals or companies involved, which were frequently recently established entities with a small workforce. Suspicions of tax-related offences continued to characterize exchanges with Eastern European FIUs. Another recurring phenomenon in information exchanges with other FIUs is the use of underground banking systems for money laundering purposes, particularly involving individuals from Asia and, more specifically, the People's Republic of China. A joint analytical effort is currently under way on this issue, involving FIUs from other European countries implicated in these financial flows.

[29] The reduction in volume is mainly attributable to a revision of the transmission criteria by one counterpart FIU.

Joint analysis

The UIF participated, along with the FIUs of Spain and the Netherlands, in a joint analysis concerning STRs relating to fund transfers to a single payment account opened in another European country and held by a payment agent operating with a European passport. The UIF identified cases involving tax fraud or the undue receipt of public funds (see the Section on 'Risk areas and typologies' in Chapter 2) and noted inconsistencies in prudential supervision approaches, which require further attention and harmonization at EU level.

Recourse to joint analysis activities, promoted by the AML Package, enabled the FIUs to better identify mainly cross-border phenomena. Joint analyses also promote the sharing of workflows, methodologies, experiences and expertise, thereby enhancing the value of diverse national approaches. In recent years, the UIF has promoted and coordinated several joint exercises with other European FIUs.

7.2. The EU FIUs Platform and the FIU.net network

Working groups

Work on the development of criteria for the selection and classification of cross-border reports and the definition of STR formats and a common model for intermediaries' responses to FIUs continued on the Platform.[30] A project jointly led by the UIF and the Spanish FIU to draw up the methodology for joint analysis exercises – in support of the AMLA, given its future coordination role – is nearing completion.

The draft methodology outlines the criteria and procedure for selecting cases for joint analysis, launching the respective exercises, conducting the analyses, preparing the final report, and disseminating the outcomes to national authorities and at EU level. The group coordinated by the UIF and the Dutch FIU continues its work on mapping priority areas for the development of IT tools, support and training. The UIF has shared a new set of anomaly indicators with the European Commission and the FIUs on the Platform, also in anticipation of AMLA guidance on the subject.

The Unit participates in the EU FIUs' project to find harmonized operational modalities and best practices for the dissemination and use of exchanged information. The objective is to ensure their alignment with the consent granted by the FIUs and to support the consistent implementation of the applicable EU legislation.

FIU.net NG

Work on the 'Next Generation' FIU.net (FIU.net NG), dedicated to collaboration and information exchange among EU Financial Intelligence Units, was concluded. The network became operational in February 2025, and its management is scheduled to be transferred to AMLA by July 2027.

The works were carried out by the Commission, the current service provider, based on a process defined within the framework of the governance provided for in the Service Level Agreement signed with the FIUs. Compared with the previous version, the new infrastructure benefits from enhanced IT technologies, ensuring higher standards of confidentiality and security in the exchange of information. Additionally, the new system incorporates an updated data format, designed to enrich the quality of information exchanges among FIUs, support more advanced forms of cooperation, and sustain increasing volumes of data flows. The UIF is part of a working group tasked with facilitating smoother integration with internal FIU databases and full interoperability with domestic systems.

[30] The drafting of these technical implementation standards is expected to be completed by the AMLA by 10 July 2026. See Article 69(3) of Regulation (EU) 2024/1624.

7.3. Relations with foreign counterparties and technical assistance

In 2024, the UIF continued to engage in technical assistance and support activities within the framework of the Egmont Group.

A UIF representative participated as a teacher in a training programme focused on threats, risks, and cases relating to terrorist financing, delivered to FIUs from some Central and East African countries. The UIF participated in a meeting with the Public Prosecutor of Marseilles to share best practices concerning cooperation between the respective FIUs and judicial authorities. The UIF also welcomed a delegation from the FIU and the investigative and administrative authorities of Kosovo, which were interested in gaining a comprehensive understanding of the Unit's operational activities. Furthermore, the UIF met with representatives from the Central Bank of the United Arab Emirates to explore its organizational model, given that the UAE FIU's placement within the Central Bank is similar to that of the UIF. A bilateral meeting was held with the FIU of San Marino to review joint cases of common interest and to further strengthen cooperation between the two Units. UIF personnel took part in a Council of Europe conference on the strategic analysis functions of FIUs, during which key findings were shared regarding a machine-learning based indicator designed to identify companies at risk of mafia infiltration based on their financial statements.[31]

Secondment to the UIF

Under the initiative promoted by ECOFEL, the UIF hosted a secondment programme for the benefit of Kyrgyzstan's FIU. There was a particular focus on synergies with investigative counterparts and the UIF's contribution within the FSC (Financial Security Committee) to the update of the National Risk Assessment on money laundering and terrorist financing.

7.4. Participation in the FATF and other bodies

Mutual Evaluation

In 2024, the FATF launched the Mutual Evaluation of Italy as part of its fifth round of assessments. A dedicated task force established at the Ministry of Economy and Finance (MEF) is coordinating activities and liaising with the FATF. The final evaluation report is expected to be approved by February 2026.

Revision of Standards

The assessment covers both formal compliance with FATF standards (technical compliance) and the effectiveness of the AML/CFT measures implemented (effectiveness). The new methodology places increased emphasis on effectiveness, pays greater attention to the specificities of non-financial entities and professionals, and considers the main risks and contextual factors of the country assessed.

The FATF has completed its revision of Recommendation 1 on the risk-based approach, aimed at mitigating financial exclusion and de-risking phenomena. Work on the revision of Recommendation 16 concerning transparency in fund transfers ('travel rule'), to better align with technological developments, evolving market conditions, changes in business models, and the new ISO20022 messaging standard for payments, also continued.

Revision of FATF standards on payment transparency

The revision of R.16 is part of a set of initiatives undertaken by international bodies – including the FATF, FSB, CPMI, IMF and World Bank – to enhance the speed, efficiency and transparency of cross-border payments and remove existing frictions, in line with the G20's 2020 lines of action.

[31] See UIF, *Annual Report 2023*, p. 47.

The revision also aims to expand disclosure obligations to previously unregulated areas. Specifically, the proposed amendments cover: *i)* the update of the information set required for remitters and beneficiaries in cross-border transfers (for EU Member States, those involving third countries); *ii)* the introduction of new mechanisms for verifying such information; *iii)* the reformulation of the exemption for purchases of goods and services by card (card exemption), and the introduction of a requirement for additional information other than the card number; *iv)* the definition of a general principle that account numbers must not be used to obscure the identification of the jurisdiction where accounts are held, which is especially relevant to the use of virtual IBANs;[32] and *v)* the introduction of disclosure requirements for cross-border cash withdrawals, with no minimum threshold, which include at least the account holder's name and the card number.

Discussions on these elements proved challenging, particularly in striking a balance between the need for efficiency in cross-border payments and the requirements for prevention and for timely and broad access to information by authorities. Regarding card-based withdrawals in particular, not revising the standards would result in persistent gaps that would prevent FIUs and investigative authorities from promptly tracing significant cash flows.

The revision of the methodology was completed following changes to the asset recovery standards, which require the allocation of suspension powers to the FIUs or other authorities;[33] work also began on the related guidelines for authorities and reporting entities.

The exercise of suspension powers is now considered in evaluating the effectiveness of related measures and the level of international cooperation. Moreover, with regard to international suspensions, although the competent authorities in the respective countries may differ in nature, the methodology does not require direct 'diagonal' cooperation between FIUs and other types of authorities, in line with Egmont Group principles.

The FATF published a new *guidance* on the correct application of transparency safeguards for beneficial ownership of trusts and similar arrangements under Recommendation 25, as well as a *guidance* for the effective conduct of national risk assessment of money laundering.

The guidance on transparency provides detailed definitions of trust-like structures, methods for assessing the associated risks, and criteria for ensuring the adequacy, accuracy, and updating of beneficial ownership information. It also outlines how such information should be obtained, either through centralized registers or equivalent mechanisms.

In 2024, the FATF released its annual *Report* on jurisdictions' progress in achieving compliance with standards on virtual assets and on emerging risk profiles. The UIF contributed to the work through its participation in the Virtual Asset Contact Group.

Risks and typologies

As part of its assessment of emerging risks associated with online gaming and betting platforms, a UIF representative gave a presentation on a money laundering case involving suspected proceeds from fraud and payment card cloning on such platforms. The UIF also participates in two projects focused respectively on the methods used by terrorist organizations to collect and utilize funds, and on the effective use of informal cooperation

[32] See UIF, *Annual Report 2022*, p. 79.

[33] See UIF, *Annual Report 2023*, p. 62-63.

mechanisms in cross-border investigations. The latter is a joint initiative of the FATF, the Egmont Group, INTERPOL and the UNODC.

Russia's membership

The suspension of Russia's membership of the FATF, enacted in February 2023, remains in force, barring the country from all rights associated with organizational membership. The Russian Federation remains a member of the Eurasian Group (EAG), a regional body affiliated with the FATF.

OECD Anti-Bribery Convention

In 2024, the OECD Working Group on Bribery assessed that Italy had fully implemented the anti-money laundering commitments made as part of the review of the application of the OECD Convention on combating bribery of public officials in international business transactions.

7.5. Participation in the Egmont Group

IEWG

Within the framework of the Egmont Group's Information Exchange Working Group (IEWG), the UIF contributed to a project examining the role of FIUs in the implementation of international financial sanctions. The group identified several anomaly indicators associated with sanction evasion.

Frequent schemes include the execution of transactions via cash or crypto-assets, and the use of split payments aimed at avoiding reporting obligations. Other recurring indicators involve the interposition of third parties (including relatives), the use of complex corporate structures – often marked by frequent changes in the controlling structures – falsified documentation, and connections with countries showing strategic deficiencies in their AML/CFT frameworks. The work highlighted significant unevenness in the role of FIUs in this domain, stemming from both legal limitations (in some jurisdictions, sanction evasion is not a predicate offence for money laundering) and operational constraints (with responsibilities fragmented across multiple authorities, hindering the adoption of effective countermeasures). Only a small number of FIUs are tasked with coordinating and implementing sanction regimes. Most have more limited powers, such as collecting information from the private sector or sharing financial intelligence with national or international counterparts, typically as part of sanctions committees or bodies.

IT Group

The UIF is in the IT Professionals Group, which is working on developing interoperability features between the Egmont Secure Web and domestic FIU systems, as well as mechanisms for the voluntary sharing of datasets – building on developments at the European level with FIU.net's Ma3tch feature.

The new support and compliance procedure

In 2024, the UIF took part in the work of the Membership Support and Compliance Working Group (MSCWG), responsible for drafting the new Support and Compliance Process (SCP), scheduled for approval in July 2025. The SCP is intended to identify FIUs that fail to meet the binding requirements established in the Egmont Group Charter and the Principles for Information Exchange, and to outline appropriate countermeasures. These range from support and training initiatives provided by Egmont bodies to the imposition of sanctions in more serious cases. The process is designed to avoid duplicating similar initiatives carried out by the FATF or regional bodies. The SCP may be activated either by a formal complaint from a Group member citing difficulties in bilateral cooperation, or upon the emergence of deficiencies, such as those identified during a Mutual Evaluation.

These procedures, introduced by the Egmont Group in 2014, have been activated on multiple occasions in the past, particularly in relation to weaknesses in members' legal

frameworks. The adoption of targeted action plans for FIUs and the related monitoring process have provided a valuable complement to FATF procedures, especially in ensuring the effective alignment of national legal systems with the required standards.

8. THE LEGISLATIVE FRAMEWORK

8.1. The global and European context

8.1.1. The AML package and the establishment of the AMLA

The legislative acts comprising the AML Package were adopted in June 2024.[34] As part of this framework, the European Anti-Money Laundering Authority (AMLA) was established, with responsibilities for overseeing the AML system and supporting and coordinating the work of FIUs. Bruna Szego, former Head of the AML Supervision and Regulation Unit of Banca d'Italia, was appointed as AMLA's Chair. In its initial years of activity, AMLA is tasked with issuing guidelines and drafting regulatory technical standards.

8.1.2. Further European and international initiatives

Payment services

The legislative process for the Commission's proposals to adopt a directive (Payment Services Directive, PSD3) and a regulation (Payment Services Regulation, PSR) on payment services continues. The UIF is participating in the negotiations by contributing to the Italian delegation coordinated by the MEF.

The directive proposal brings electronic money institutions (EMIs) under the category of payment institutions (PIs) for licensing purposes and covers, among other areas, cash withdrawal services provided by retailers (cash-in shops) or independent ATM operators. The regulation proposal introduces provisions regarding the rights associated with the provision and use of payment services, including transparency obligations for operators. Payment service providers (PSPs) are required to implement transaction monitoring mechanisms and IBAN name check procedures for credit transfers to verify correspondence between the bank details and the name of the payee indicated by the payer; agreements for the sharing of fraud-related information may be established. These preventive measures must be aligned with AMLR requirements. Anti-money laundering implications are particularly relevant with regard to provisions related to cash withdrawal services by retailers and ATMs.

Instant Payments Regulation

Regulation (EU) 2024/886 on instant payments[35] (Instant Payments Regulation – IPR) was adopted in 2024. Its first obligations became applicable on 9 January 2025. The regulation ensures that euro instant payments are universally available under the same conditions as traditional credit transfers, covering transparency in fees for sending and receiving payments, as well as cybersecurity aspects related to beneficiary identity verification.

From an AML/CFT perspective, there is a need to prevent instant credit transfers from being initiated from accounts held by persons subject to targeted financial restrictive measures, and to immediately freeze funds received into such accounts. Under Article 5-quinquies of Regulation (EU) 2012/260, PSPs are required to verify, at least daily, whether any of their users are designated persons. It will be essential to assess when suspicious elements can be intercepted prior to execution of transfers, which must in any case be based on both subjective and objective indicators collected as part of AML obligations. Verification

---

[34] Reference is made to the following measures: *i*) Regulation (EU) 2024/1620 (AMLAR), establishing AMLA; *ii*) Regulation (EU) 2024/1624 (AMLR), on the prevention of the use of the financial system for money laundering or terrorist financing purposes; *iii*) Directive (EU) 2024/1640 (AMLD6), setting out the mechanisms to be established by Member States to prevent the misuse of the financial system for money laundering or terrorist financing purposes. Regulation (EU) 2023/1113 (the 'TFR'), also part of the AML Package, has already been transposed into the national legal system. For further details on the legislative framework, see the UIF's 'Quaderni dell'antiriciclaggio - Rassegna normativa' (only in Italian).

[35] The newly introduced point 1(b) of Article 2 of Regulation (EU) 2012/260, as amended by IPR, defines an instant payment as a 'credit transfer which is executed immediately, 24 hours a day, and on any calendar day'.

outcomes under IPR aimed at fraud prevention may be relevant for AML/CFT purposes, without triggering automatic links between verification activity and active cooperation obligations.

8.2. The Italian legislative and regulatory framework

8.2.1. Legislation

AML Package

In 2024, work began to implement and transpose the AML Package into national legislation, entailing a substantial reform of the existing framework.[36] It will be necessary to ensure alignment with AMLAR regulations, which will be largely applicable as of 1 July 2025. Discussions are ongoing to assess further adjustments to the current AML/CFT framework and the possible legislative options. Decree-Law No. 25/2025 established the Directorate for Preventing and Combating the Use of the Financial System for Illegal Purposes at the Ministry of Economy and Finance. The Directorate is responsible for financial crime prevention, financial system security, oversight and control of non-financial obliged entities, and sanctioning procedures.

Legislative Decree 204/2024

Legislative Decree 204/2024 aligned national legislation to the provisions of Regulation (EU) 2023/1113 (TFR),[37] regarding information accompanying transfers of funds and certain crypto-assets. Amendments were also made to Legislative Decree 231/2007.

The notions of 'crypto-assets', 'crypto-asset services' and 'crypto-asset service providers' (CASP) were introduced into the AML Decree, replacing for AML/CFT purposes 'service providers for the use of virtual currency' and 'digital wallet service providers'; the definition of 'self-hosted address' was also introduced.[38] CASPs are now included among financial intermediaries subject to anti-money laundering supervision by Banca d'Italia, with supervisory powers also attributed to the Finance Police, in coordination with the supervisory authority and the UIF for profiles concerning STRs and missed reporting. A reference was introduced to the risks associated with crypto-asset transfers involving one unhosted party, i.e., a counterparty not associated with a service provider capable of conducting adequate verification. Obliged entities must implement risk-mitigation measures, specifically to: i) adopt risk-based measures to identify and verify the sender or recipient of such transfers; ii) request additional information on the origin and destination of the crypto-assets; iii) continuously monitor transactions involving self-hosted addresses; iv) adopt measures to mitigate the risk of non-compliance and evasion of financial sanctions. Customer due diligence is required for crypto-asset transfers exceeding €1,000. Enhanced due diligence measures apply to business relationships involving crypto-asset service providers in third countries. CASPs are subject to the same sanctioning framework applicable

[36] Directive (EU) 2024/1640 (AMLD6) must be transposed by 10 July 2027. Earlier transposition deadlines are established for specific areas: access to beneficial ownership information (Article 74), to be transposed by 10 July 2025; rules on registers and access modalities (Articles 11, 12, 13, and 15), to be transposed by 10 July 2026; access to real estate information (Article 18), to be transposed by 10 July 2029.

[37] See the hearing of the UIF Director before the joint Justice and Finance Committees of the Chamber of Deputies on 27 November 2024 (only in Italian).

[38] Under the MiCAR Regulation, a crypto-asset is defined as 'a digital representation of value or a right that can be transferred or stored electronically using distributed ledger technology or similar technology'. Crypto-assets are classified into three categories based on associated risks, particularly whether their value is pegged to other assets. A CASP is defined as 'a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services'. A self-hosted address is defined as 'a distributed ledger address not linked to either of the following: a) a crypto-asset service provider; b) an entity not established in the Union and providing services similar to those of a crypto-asset service provider'.

to banking and financial intermediaries. Banca d'Italia is designated as the competent authority also for breaches of the TFR Regulation.

Legislative Decree 129/2024

Legislative Decree 129/2024 aligned national legislation with the provisions of Regulation (EU) 2023/1114 (MiCAR), outlining the framework of national competences for the supervision of crypto-asset markets and related services, and designating Banca d'Italia and Consob as the competent authorities.[39]

Legislative Decree 211/2024

On 17 January 2025, Legislative Decree 211/2024[40] entered into force, aligning national legislation with Regulation (EU) 2018/1672. It introduced amendments to Legislative Decree 195/2008 regarding currency regulations and to Law 7/2000 concerning declarations on gold transactions and the professional trade of gold. The reform has coordinated the provisions of Law 7/2000 with those of Regulation (EU) 2018/1672 on the controls on cash entering or leaving the EU, in order to avoid overlapping reporting obligations and to clarify compliance procedures. For transactions covered by the Regulation and Legislative Decree 195/2008, which require obligations to the Customs and Monopolies Agency (ADM), the reporting obligation to the UIF under Law 7/2000 is excluded. The definition of relevant gold has been expressly expanded to include material intended for melting to produce investment gold and gold primarily for industrial use. The reporting threshold has been lowered to €10,000, and relevance has been given to structured transactions.[41] The UIF has been formally designated as the competent authority (previously delegated by Banca d'Italia) to receive gold transaction reports and to issue instructions concerning the transactions subject to declaration, including their content and submission procedures. Violations of these instructions are now explicitly subject to sanctions. Responsibility for receiving communications from professional gold traders (OPOs) under Article 1(3) of Law 7/2000, as well as verifying the requirements to qualify as an OPO and managing the related register, has been transferred from Banca d'Italia to the OAM. This register forms a section of the register of gold traders.

Some provisions of the UIF Communication of 1 August 2014 on the 'Reporting of gold transactions' have been elevated to the status of primary legislation, particularly those regarding 'channelled' declarations, deadlines for submission, modalities of cross-border reporting, and report exemption for transactions involving Banca d'Italia.

Legislative Decree 211/2024 also reaffirmed the obligation to declare to the ADM any 'cash' physically carried across national borders for amounts equal to greater than €10,000. In line with Regulation (EU) 2018/1672, the definition of 'cash' includes currency, bearer negotiable instruments, highly liquid value stores,[42] and prepaid cards.

---

[39] The definition of the transitional regime is still pending. By 31 May 2025, VASPs already registered with the OAM are required to publish adequate information on their websites and inform their clients of the plans and measures they intend to implement to comply with MiCAR, or for the orderly termination of business relationships. By 30 June 2025, OAM-registered VASPs must submit an application for authorisation and, in such cases, may continue operating until 30 December 2025 or until the authorisation is granted or denied. After 30 June 2025, VASPs that have not submitted an authorisation request will cease operations and will be automatically removed from the register by the OAM. In communications dated 12 and 13 September 2024 respectively, Consob and the Banca d'Italia provided initial operational guidance.

[40] See also the hearing of the UIF Director before the joint Justice and Finance Committees of the Chamber of Deputies on 3 October 2024 (only in Italian).

[41] Gold transactions of the same type, carried out within the same calendar month with the same counterparty, amounting individually to at least €2,500 and in aggregate to at least €10,000, must be reported (Article 1(2-bis) of Law 7/2000).

[42] Specifically: a) coins with a gold content of at least 90%; b) bars, nuggets, or aggregates with a gold content of at least 99.5%.

The obligation to notify the ADM also applies to 'unaccompanied' cash transfers of €10,000 or more entering or leaving the national territory.

Self-regulatory Bodies and Representative Associations

Provisions were also introduced regarding temporary retention, seizure, sanctions, and cooperation and information exchange between authorities. The ADM shall transmit to the UIF: a) information not entered into the Customs Information System, without delay and no later than 15 working days from the date it is obtained; b) information entered into the Customs Information System via direct access granted to the UIF.

8.2.2. Regulatory and other measures

UIF and Banca d'Italia

With the Communication (only in Italian) of 12 December 2024, the SNA Unit of Banca d'Italia and the UIF issued guidance to obliged entities on anti-money laundering obligations related to the opening and management of payment accounts with virtual IBANs, along with some best practices observed among PSPs to mitigate ML/TF risks arising from their use.

UIF Instructions for the detection and reporting of suspicious transactions

The UIF is currently drafting new instructions for the detection and reporting of suspicious transactions, aimed at fostering full awareness among reporting entities regarding their roles and responsibilities, the need for specific assessments, and proper reporting practices, discouraging both automatic flagging and overly cautious approaches. The instructions recall the principles and rules of active cooperation in identifying, analysing, detecting, and reporting suspicious transactions. Clarifications are also provided on how the obligation to report (STRs) relates to other legal compliance requirements. Specific focus will be given to the suspension of suspicious transactions and the feedback (return flows) provided by the UIF. Organizational and procedural requirements to support active cooperation will also be outlined, in coordination with sectoral supervisory authorities' guidance. The draft regulation will be subject to consultation with authorities, industry associations, and self-regulatory bodies to ensure full alignment with its content and objectives.

Banca d'Italia

With its Provision (only in Italian) dated 27 November 2024, Banca d'Italia amended the 'Provisions on organization, procedures, and internal controls aimed at preventing the use of intermediaries for money laundering and terrorist financing purposes,' particularly regulating the procedures for submitting periodic AML reports. In November 2024, Banca d'Italia notified the EBA of its intention to comply with the Guidelines on information requirements in relation to transfers of funds and certain crypto-assets under the TFR Regulation (or 'travel rule' Guidelines).

Ivass

By Provision dated 4 June 2024, Ivass introduced amendments and additions to Regulation 44/19 concerning organization, procedures, internal controls, and customer due diligence, to fully implement the EBA Guidelines of 14 June 2022 on governance and internal controls in AML matters.

The National Council of Chartered Accountants and Accounting Experts (*Consiglio Nazionale dei dottori commercialisti e degli esperti contabili*, CNDCEC) approved new technical AML rules. As required by the UIF Provision of 12 May 2023, both the CNDCEC and the National Council of Notaries (CNN) identified relevant anomaly indicators in the context of their activities. Similar work was carried out by Assirevi and Assogestioni. The UIF collaborated with these bodies and associations during the selection process.

9. RESOURCES AND ORGANIZATION

9.1. Organization and resources

The staff

In 2024, the number of staff members in the Unit continued to grow, reaching 191 at the end of the year – four more than in 2023 – as a result of six departures and the addition of ten new staff members (including two newly hired employees). The distribution of personnel across the Directorates remains broadly consistent with the previous year: 95 employees were assigned to the Suspicious Transactions Directorate, 62 to the Regulation and Institutional Cooperation Directorate, 29 to the Information Exploitation and Technological Innovation Directorate, and three managers were assigned to support the Director. The average age of employees rose slightly to 46.2 years, and 49 per cent of total work activity was carried out remotely (compared to 44 per cent in the previous year).

Training

In 2024, the Unit continued to invest in strengthening the professional skills of its human resources. A total of 19 internal training initiatives were conducted, focusing on operational and institutional matters. UIF staff also participated in training programmes organized by Banca d'Italia (115 sessions with 122 UIF participants) and by external institutions.

9.2. IT projects

2024 saw significant efforts in modernizing analytical tools and in developing technological solutions to support new reporting obligations related to international sanctions.

New identity resolution system

The new IDRES register aims to centralize the management of identifying data for all subjects reported to the Unit across the various reporting channels. It improves the ability to recognize the same individual even when referenced with slightly differing personal data. IDRES facilitates the processing of names written in non-Latin scripts and can identify individuals using not only traditional identification elements but also relational information (e.g., joint ownership of the same financial account) and technological usage data (e.g., IP address, email, mobile phone number). These features enhance identification accuracy and reduce the operational burden of resolving ambiguous cases. Given the frequent need to process data sources relating to potentially high-risk contexts, IDRES is designed with high flexibility to handle new data sources and processing loads, and can easily adapt to future technological developments.

Graph analysis

The RADAR application has been enhanced with a Graph database to capitalise on the extensive network of relationships between subjects and financial accounts reported to the Unit. The network analysis, already used to analyse STRs from specific categories of reporting entities with highly fragmented operations, has now been extended to all types of reports. The new technology integrates fully with RADAR's traditional relational database, enabling innovative ways to explore and visualize information. Analysts can now access an overall view of relational and financial networks within a specific context, explore individual connections with ease, and retrieve relevant details. In the future, artificial intelligence solutions may be incorporated to build knowledge graphs, supporting analysts in identifying hidden links and recurring money laundering patterns.

Risk indicators

To enrich the information available to analysts, work continued on integrating new indicators into RADAR, particularly those that summarize high-risk factors (see Session: 'Financial Analysis' in Chapter 1). RADAR's graphic interface allows analysts to use these indicators to assess the significance of STRs and their broader operational context, especially

in complex cases, by highlighting subjects and relationships of financial relevance. The adopted technical solution is highly flexible, allowing for rapid future adaptation to new aggregation criteria and variables used to measure financial and investigative risk.

As part of the ongoing effort to reduce operational and security risks, the process for sending reports to the Investigative Bodies has been further automated, decreasing the manual steps involved in preparing and transmitting the STR files.

The suspension process – characterized by high confidentiality – has also been enhanced within RADAR, improving the speed, automation, and security of communication between reporting entities, UIF, and Investigative Bodies.

Testing of machine learning algorithms in high data security environments

Improving the allocation of resources based on the potential risk level of received STRs is a priority for the Unit. In this context, a research project was launched to promptly identify reports presenting little or no financial risk, which may be handled through specific procedures. Various machine learning models (e.g., gradient boosting, neural networks) were tested on data available at the time of report receipt. These models showed promising potential for automatically classifying the risk level of STRs. The models will be further refined for potential use as support tools for analysts.

The experimentation was carried out within the Blind Learning Environment developed by the IT Department of Banca d'Italia – a high-performance infrastructure designed to securely process sensitive data.

In July 2024, the UIF launched a new data collection on its Infostat-UIF portal, called Trasferimenti Russi (TRU), concerning extra-EU fund transfers involving Russian nationals (see Chapter 6, 'International Financial Sanctions').

9.3. Information security and confidentiality

Russian transfers

The protection of information confidentiality remains essential to the UIF, which in 2024 continued to strengthen its safeguards in close coordination with Banca d'Italia's IT Department, also in response to evolving threat landscapes. In April 2024, during *hearings* before the Constitutional Affairs and Justice Committees of the Chamber of Deputies and the Parliamentary Anti-Mafia Commission, the UIF Director outlined the IT, administrative, and internal controls in place to protect the Unit's sensitive information.

Treatment of PEPs

Due to the sensitivity of the subject, a specific indicator was developed to identify reports involving Politically Exposed Persons (PEPs), allowing for tailored handling procedures. The indicator is based on institutional Open Data, updated semi-annually, and refers to individuals who have held public office in the past two years.

In early 2025, following the methodology adopted by Banca d'Italia, the UIF conducted a new mapping of its internal processes to identify and manage its operational risk. For each process, inherent risks were identified – including those related to IT infrastructure and corruption – and a taxonomy and likelihood assessment of potential risk events was carried out. Based on existing preventive measures, some processes were rated as medium risk, while others were deemed low risk. Action plans to mitigate or prevent residual risks were then initiated.

The new technical agreement

The functionalities envisaged under the Memorandum of Understanding signed in December 2023 between the Anti-Mafia National Directorate (DNA), UIF, Finance Police (, and Anti-Mafia Investigation Directorate (DIA) were implemented to enable the secure exchange of sensitive information via the UIF's SAFE portal. To ensure security, portal access requires two-factor authentication, including a digital certificate communicated to the UIF during user registration. All data exchanges between users and the portal are protected by dual encryption (channel and end-to-end), ensuring that information cannot be accessed by outsiders and is only readable by the intended recipients. SAFE logs user activity to ensure full traceability of actions for auditing purposes. Currently, data exchanges use a user-to-application (U2A) model. Plans are in place to introduce application-to-application (A2A) exchanges to reduce manual operations and further enhance security.

9.4. External communication

External communication remains a strategic objective for the UIF. In addition to this *Annual Report* – presented at a dedicated public event – the Unit publishes on its website regular *Newsletters* providing updates on its activities and the main AML-related news, along with the *Quaderni dell'antiriciclaggio*, which include sections on Statistics, Analyses and Studies, and Regulatory Review. The new Regulatory Review ('*Rassegna normativa*') section highlights key developments in legislation and case law, and provides in-depth insights on money laundering and terrorist financing issues.

Awareness-raising and information activities, targeting obliged entities and the general public continued, as did the promotion of opportunities for in-depth discussion and debate with other national and supranational authorities. During the year, UIF staff spoke at over 90 informational and training events.

Among notable national initiatives were lectures and training activities hosted by the Naples Prosecutor's Office, the Training School of the Presidency of the Council of Ministers, the Finance Police's Economic and Financial Police School, the National School of Administration, the Financial Crimes Unit of the Postal Police, and various public sector bodies. Tailored initiatives were also organized for specific categories of obligated entities (e.g., fiduciary companies, asset management firms, professional gold traders) and professional associations. Two events were held as part of the series 'the UIF meets the reporting entities', along with a dedicated seminar on active collaboration among gold operators. At the international level, the UIF participated in events organized by the Council of Europe, the Italian Embassy in Romania, the World Customs Organization, the Banking Association for Central and Eastern Europe, and various foreign universities.

GLOSSARY

Administrations and bodies concerned

Pursuant to Art. 1(2)(a) of Legislative Decree 231/2007, these are the bodies in charge of supervising obliged entities not supervised by sector-specific authorities, i.e. the administrations, including tax agencies, which have supervisory powers or are competent to issue concessions, authorisations, licences or other enabling documents, however, denominated, with respect to obliged entities, and the bodies in charge of supervising the fulfilment of the requirements of professionalism and good repute, prescribed by the relevant sectoral legislation with respect to the aforementioned parties. For the sole purposes of the aforementioned decree, the definition of the administration concerned includes the MEF as the authority responsible for the oversight of statutory auditors and statutory auditing firms without statutory auditing assignments on public interest entities or entities subject to an intermediate regime, the Ministry of Economic Development (now MIMIT) as the authority responsible for the oversight of trust companies not registered in the register referred to in Art. 106 of the Consolidated Law on Banking.

Anti-Mafia Investigation Department (DIA)

Specialised investigative body with inter-agency composition, with jurisdiction throughout the country. Instituted within the Ministry of the Interior's Department of Public Security by Law 410/1991, it has the 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, is the natural person or persons, other than the customer, in whose interest or interests the continuing relationship is ultimately established, the professional service is rendered or the transaction is ultimately carried out.

Body for the administration of lists of agents and brokers (OAM)

Pursuant to Article (1)(1)(q) of Legislative Decree 231/2007, it manages the lists of financial agents and credit brokers, pursuant to Article 128-l of the Consolidated Law on Banking. The following are also kept at the OAM: i) the register of foreign exchange dealers, within which a special section devoted to providers of services relating to the use of virtual currency is set up (Article 17-bis (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 contracting parties and agents referred to in Art. 45 of Legislative Decree 231/2007; iii) the register of gold traders referred to in Article (1)(1)(q) of Legislative Decree 92/2017, within which a section dedicated to professional gold traders is established (Article 1(3-ter) of Law 7/2000, as amended by Article 1(1) of Legislative Decree 211/2024).

Central point of contact

Pursuant to Article 1(2)(ii) of Legislative Decree 231/2007, it is the person or structure, established in the territory of the Republic, designated by electronic money institutions, as defined in Article 2(1), point 3) of Directive 2009/110/EC, or payment service providers, as defined in Article 4, point 11) of Directive (EU) 2015/2366, with registered office and head office in another Member State, operating, without a branch, in the national territory through contracted entities and agents.

Contracting parties and agents

Pursuant to Article 1(2)(nn) of Legislative Decree 231/2007, these are the contracting operators or agents, however denominated, other than agents in financial activities registered in the list referred to in Article 128-c(2) and (6) of the Consolidated Law on Banking (TUB), which payment service providers and electronic money issuers, including those having their head office and central administration in another Member State, use for their activities in the territory of the Italian Republic.

Countries with strategic AML/CFT deficiencies identified by the FATF

This includes countries with weak anti-money laundering controls, identified by the FATF through public statements published three times a year. Based on these assessments (FATF *High-*

Risk Jurisdictions subject to a Call for Action – 21 February 2025 and *Jurisdictions under Increased Monitoring – 21 February 2025*), as of March 2025 the following countries were not aligned with the legislative and regulatory provisions against money laundering and terrorist financing: Algeria, Angola, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, Croatia, Haiti, Iran, Kenya, Lebanon, Mali, Monaco, Mozambique, Myanmar, Namibia, Nepal, Nigeria, Democratic Republic of Congo, Democratic Republic of Korea, Lao PDR, Syria, South Africa, South Sudan, Tanzania, Venezuela, Vietnam, Yemen.

Cross-border reports

Suspicious transaction reports received from an EU FIU, which concern another Member State and, pursuant to Article 53(1) of the Fourth Directive, must be promptly transmitted to the counterparties concerned. These reports are identified based on the methodology developed within the EU FIU Platform.

Designated persons

Pursuant to Article 1(2)(oo) of Legislative Decree 231/2007 Designated entities are natural persons, legal persons, groups and entities designated as recipients of freezing based on Community 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 who provide third parties, on a professional basis, including online, with private cryptographic key protection services on behalf of their clients, in order to hold, store and transfer virtual currencies. Legislative Decree 204/2024 introduced the notions of 'crypto-assets' and 'crypto-asset services,' thus superseding the previous notions of 'virtual currency' and 'digital wallet service providers'.

Egmont Group

An informal body was set up in 1995 by a group of FIUs to develop international cooperation and increase its benefits. In 2010, it became an international organization with a secretariat in Ottawa, Canada.

Financial Action Task Force - FATF)

An intergovernmental body set up within the OECD to devise and promote strategies to combat money laundering and terrorist financing, both nationally and internationally. In 2012, it issued 40 new Recommendations to combat money laundering, terrorist financing and the proliferation of weapons of mass destruction.

Financial Intelligence Unit (FIU)

A national central unit which, to combat money laundering and terrorism financing, is responsible for receiving and analysing suspicious transaction reports and other relevant information on money laundering, terrorist financing and related predicate offences, and for disseminating the results of such analyses. Depending on the choice made by the individual national legislator, the FIU can take on the nature of an administrative authority, a specialised structure set up within the police force or hinged within the judicial authority. Mixed models have been adopted in some states.

Financial Security Committee (FSC)

Pursuant to Article 3 of Legislative Decree 109/2007, it is the Committee set up at the MEF, chaired by the Director General of the Treasury, and composed of 15 members and their alternates, appointed by decree of the Minister of the Economy and Finance, based on nominations made by the Minister of the Interior, the Minister of Justice, the Minister of Foreign Affairs and International Cooperation, the Minister of Economic Development (now MIMIT), Banca d'Italia, Consob, Isvap (now Ivass), and the UIF, respectively. The Committee also includes a manager in service at the MEF, an officer of the Finance Police, a member of the managerial role or an officer of equivalent rank of the police forces referred to in Article 16 of Law 121/1981, in service at the Anti-Mafia Investigation Department, an officer of the Carabinieri, an officer of the Customs and Monopolies Agency and a magistrate from the Anti-Mafia Investigation Department. In order to perform its tasks concerning the freezing of economic resources, the Committee is supplemented by a representative of the State Property Office (Agenzia del Demanio). 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 powers, initially limited to coordination in the area of the financial fight against terrorism, were extended to include the fight against money laundering (Article 5(5)(6)(7), of Legislative Decree 231/2007).

Financing of terrorism

Pursuant to Article 1(1)(d), of Legislative Decree 109/2007, financing of terrorism means any activity aimed, by any means, at the supply, collection, provision, intermediation, deposit, custody or disbursement of funds and economic resources, howsoever carried out, intended to be used, directly or indirectly, in whole or in part, for the perpetration of one or more forms of conduct for purposes of terrorism, in accordance with the provisions of the criminal law, irrespective of the actual use of the funds and economic resources for the commission of the aforesaid conduct.

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 EU Financial Intelligence Units that enables structured, multilateral sharing of information, ensuring standardized implementation, promptness and security of information exchanges.

Freezing of funds

Pursuant to Art. 1(1)(b) of Legislative Decree 109/2007, it is the prohibition, under Community regulations and national law, on the variation, transfer, modification, use or management of funds or access to them, so as to change their volume, amount, location, ownership, possession, nature, destination or any other change that enables the use of funds, including portfolio management.

High-risk third countries

Pursuant to Art. 1(2)(bb) of Legislative Decree 231/2007, are those non-EU countries whose jurisdictions have strategic deficiencies in their national AML/CFT prevention regimes, as identified by the European Commission, through Delegated Regulation (EU) 2016/1675 as amended, in the exercise of powers under Art. 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, Cameroon, Democratic Republic of Congo, Gibraltar, Haiti, Jamaica, Mali, Mozambique, Myanmar, Nigeria, Panama, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Trinidad and Tobago, Uganda, United Arab Emirates, Vanuatu, Vietnam, Yemen, Iran and Democratic Republic of Korea (Delegated Regulation EU/2024/163 of 12 December 2023).

Laundering and use of money, goods or benefits of unlawful origin

Art. 648-a of the Italian 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 origin'. Art. 648-b makes punishable for illegal investment anyone who, apart from the cases of complicity in the predicate offence and the cases specified in Art. 648 and 648-a, 'invests money, assets or other utilities deriving from crime in economic or financial assets'. With regard to both offenses, 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 constitute money laundering, if committed intentionally: a) the conversion or transfer of property, carried out with the knowledge that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the

property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his actions; b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property or rights over such property, carried out with the knowledge that such property is derived from criminal activity or from an act of participation in such activity; c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity; d) participation in, association to commit, attempts to commit, aiding, abetting, facilitating or counselling the commission of any of the acts mentioned in the foregoing points.

Means of payment

Pursuant to Article 1(2)(s) of Legislative Decree 231/2007, these include cash, bank and postal cheques, bank drafts, bankers' drafts and other cheques assimilated or comparable to them, money orders, credit or payment orders, credit cards and other payment cards, transferable insurance policies, pledge policies and any other instrument available to transfer, manage or acquire, including by digital transmission means, funds, values 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 operates as an autonomous Council of Europe monitoring body on AML/CFT and is directly accountable to the Committee of Ministers, to which it submits its Annual Report and makes specific recommendations to member countries on the subject. It evaluates the anti-money laundering measures adopted by Council of Europe member countries other than FATF members. It is a FATF Associate Member as a regional group.

National Anti-corruption Authority (ANAC)

The Authority is in charge of preventing corruption in the public administration and its investee companies and subsidiaries, also through the implementation of transparency in all aspects of management, as well as carrying out supervisory activity in the area of public contracts, appointments and in every sector of the public administration that could potentially develop corruption phenomena, while avoiding aggravating proceedings with negative effects on citizens and businesses, by guiding the behaviour and activities of public employees, with interventions in consultative and regulatory fields, as well as through cognitive activity.

National Anti-Mafia and Anti-Terrorism Directorate (Direzione Nazionale Antimafia - DNA)

The DNA, established within the General Prosecutor's Office at the Court of Cassation by Decree Law 367/1991, converted with amendments by Law 8/1992, has the task of coordinating, at the national level, investigations into organized crime and dealing with proceedings relating to terrorism, also international (Decree Law 7/2015, converted with amendments by Law 43/2015). Pursuant to Art. 103 of Legislative Decree 159/2011, the Directorate is headed by a magistrate with the functions of national Public Prosecutor and two assistant prosecutors, together with, as their deputies, magistrates chosen from among those who have performed 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. Decree Law 105/2023 (converted with amendments by Law 137/2023) extended the National Public Prosecutor's powers of impulse and coordination also to proceedings concerning certain cybercrimes.

Non-cooperative countries and territories and/or Tax Havens - Ministerial Decree of 4 May 1999

Countries and territories listed in the black list contained in the Decree of the Minister of Finance of 4 May 1999 (most recently amended by the Ministerial Decree of 20 July 2023): Andorra, Anguilla, Antigua and Barbuda, Aruba, Bahamas, Bahrain, Barbados, Belize, Bermuda, Bonaire, Brunei, Costa Rica, Curaçao, Dominica, Ecuador, United Arab Emirates (Abu Dhabi, Ajman, Dubai, Fuijayrah, Ras El Khaimah, Sharjah, Umm Al Qaiwain), Philippines, Gibraltar, Djibouti, Grenada, Guernsey (including Alderney and Sark), Hong Kong, Isle of Man, Cayman Islands, Cook Islands, Marshall Islands British Virgin Islands, Jersey, Lebanon, Liberia, Liechtenstein, Macao, Maldives, Malaysia, Mauritius, Monserrat, Nauru, Niue, Oman, Panama, French Polynesia, Monaco, Saint Kitts

and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Samoa, Seychelles, Singapore, Sint Eustatius and Saba, Sint Maarten - Dutch part, Taiwan, Tonga, Turks and Caicos, Tuvalu, Uruguay and Vanuatu.

Non-cooperative jurisdictions for tax purposes identified by the European Union

The following countries on the EU list of non-cooperative jurisdictions for tax purposes: American Samoa, Anguilla, Fiji, Guam, Palau, Panama, Russia, Samoa, Trinidad and Tobago, United States Virgin Islands and Vanuatu (*Council Conclusions of 18 February 2025*).

Office of Foreign Assets Control (OFAC)

Agency of the U.S. Department of the Treasury that regulates and enforces economic and trade sanctions imposed in the conduct of foreign policy and national security against other foreign states, organizations and individuals.

Platform of European Union FIUs

European body chaired by the Commission and composed of the EU FIUs; active since 2006, it was formalised by the Fourth Directive, which also defined its mandate (Art. 51). This refers to enhancing cooperation, exchanging views, and advising on issues relating to the implementation of European rules of interest to FIUs and reporting entities.

Politically exposed persons

Pursuant to Article 1(2)(dd) of Legislative Decree 231/2007, these are natural persons who occupy or have occupied for less than one-year important public offices, as well as their family members and those known to have close ties with the aforementioned persons, as listed below: 1) Natural persons who hold or have held important public office. Those who hold or have held the following offices: 1.1 President of the Republic, President of the Council of Ministers, Minister, Deputy-Minister and Under-Secretary, President of the Region, Regional Councillor, Mayor of a provincial capital or metropolitan city, Mayor of a municipality with a population of not less than 15,000 inhabitants, as well as similar offices in foreign states; 1.2 Member of Parliament, Senator, Member of the European Parliament, Regional Councillor, as well as similar offices in foreign states; 1.3 Member of the central governing bodies of political parties; 1.4 judge of the Constitutional Court, judge of the Court of Cassation or of the Court of Auditors, State councillor and other members of the Council of Administrative Justice for the Region of Sicily and similar offices 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 offices in foreign states; 1.7 member of the organs of administration, management or control of companies controlled, even indirectly, by the Italian State or a foreign State, or companies in which the Regions, provincial capitals and metropolitan cities and municipalities with a total population of not less than 15,000 inhabitants hold a majority or full stake; 1.8 general manager of an ASL, hospital company, university hospital company and other bodies of the national health service; 1.9 director, deputy director and member of the management body or person performing equivalent functions in international organizations; 2) family members of politically exposed persons are: the parents, spouse or person linked to the politically exposed person in a civil union or de facto cohabitation or similar institutions, the children and their spouses as well as persons linked to the children in a civil union or de facto cohabitation or similar institutions; 3) persons with whom politically exposed persons are known to have close ties: 3.1 natural persons linked to the politically exposed person by virtue of joint beneficial ownership of legal entities or another close business relationship; 3.2 natural persons who only formally hold total control of an entity that is known to have been established, de facto, in the interest and for the benefit of a politically exposed person.

Providers of services related to the use of virtual currencies

Pursuant to Article 1(2)(ff) of Legislative Decree 231/2007, these are natural or legal persons who provide third parties, on a professional basis, including online, services related to the use, exchange, custody of virtual currencies, and their conversion from or into legal tender or digital representations of value. This includes services related to their conversion into other virtual currencies, as well as the issuance, offering, transfer, clearing, and any other service instrumental to the acquisition, negotiation, or intermediation in the exchange of such currencies. Legislative Decree 204/2024 introduced the notions of 'crypto-assets' and 'crypto-asset services', thus superseding the

previous notions of 'virtual currency' and 'providers of services related to the use of virtual currencies'.

Public administrations

Pursuant to Article 1(2)(*hh*) of Legislative Decree 231/2007, these are the general government bodies referred to in Article 1(2) of Legislative Decree 165/2001, the national public bodies, companies owned by public administrations and their subsidiaries pursuant to Article 2359 of the Italian Civil Code, limited to their activities in the public interest governed by national or EU law, as well as the entities in charge of national or local tax collection, whatever their legal form.

Sector Supervisory Authorities

Pursuant to Art. 1(2)(c) of Legislative Decree 231/2007, these are Banca d'Italia, Consob and Ivass in their capacity as authorities responsible for the supervision and control of banking and financial intermediaries, statutory auditors and auditing firms performing statutory audits of public interest entities and of entities subject to intermediate regimes, and Banca d'Italia in respect of non-financial operators carrying on the activities of safekeeping and transporting cash and securities or valuables by means of sworn special guards, in the presence of the licence referred to in Art. 134 TULPS, limited to the activity of handling euro banknotes, in the presence of the registration in the list referred to in Art. 8 of Decree Law 350/2001, converted, with amendments, by Law 409/2001.

Self-laundering

Pursuant to Art. 648-ter.1 of the Italian Penal Code, the offence of self-money laundering is punished for 'anyone who, having committed or conspired to commit an offence, uses, substitutes, transfers, in economic, financial, entrepreneurial or speculative activities, the money, goods or other utilities resulting from the commission of that offence, in such a way as to concretely hinder the identification of their criminal origin'. The rule was introduced by Art. 3(3) of Law 186/2014 and, most recently, amended by Art. 1(1)(f) of Legislative Decree 195/2021.

Self-regulatory body

Pursuant to Article(1)(2)(aa) of Legislative Decree 231/2007, is the body representing a professional category to which the current legal system attributes powers of regulation, control of the category, verification of compliance with the rules governing the exercise of the profession and the imposition, through the bodies set up for that purpose, of the sanctions provided for their infringement.

Special Currency Police Unit (NSPV)

A special department of the Finance Police, it operates in the fight against money laundering both as a police investigation body and as an administrative control body for the financial intermediation sector, together with Banca d'Italia and the Anti-Mafia Investigation Department.

Standardised archives

Archives by means of which the data and information required by the provisions issued by the competent sectoral supervisory authorities pursuant to Art. 34(3) of Legislative Decree 231/2007 are made available, according to the technical standards and analytical reasons specified therein.

Trade-based money laundering (TBML)

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 currency

Pursuant to Art. 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. Legislative Decree 204/2024 introduced the notions of 'crypto-assets,' thus superseding the previous notions of 'virtual currency'.

ACRONYMS AND ABBREVIATIONS

ADM	Customs and Monopolies Agency (Agenzia delle Dogane e dei Monopoli)
AG	Judicial authority (Autorità giudiziaria)
AMLA	Anti-Money Laundering Authority
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
ANAC	Italian National Anti-Corruption Authority
ANCI	National Association of Italian Municipalities (Associazione Nazionale Comuni Italiani)
ATM	Automated Teller Machine
AUI	Single Electronic Archive (Archivio Unico Informatico)
CASP	Crypto-Asset Service Provider
CDP	Cassa Depositi e Prestiti SpA
CNDCEC	National Council of Accountants and Bookkeepers
CNF	National Lawyers' Council (Consiglio Nazionale Forense)
CNN	National Council of Notaries (Consiglio Nazionale del Notariato)
COLAF	Committee for combating fraud against the European Union (Comitato per la lotta contro le frodi)
Consob	Companies and Stock Exchange Commission (Commissione Nazionale per le Società e la Borsa)
CPMI	Committee on Payments and Market Infrastructures
CSF	Financial Security Committee (Comitato di Sicurezza Finanziaria)
DDA	Anti-Mafia District Directorate (Direzione Distrettuale Antimafia)
DIA	Anti-Mafia Investigation Department
DNA	National Anti-Mafia and Anti-Terrorism Directorate (Direzione Nazionale Antimafia)
EAG	Eurasian Group (FATF regional group)
EBA	European Banking Authority
ECB	European Central Bank
ECOFEL	Egmont Centre of FIU Excellence and Leadership
EMI	E-money institution
EPPO	European Public Prosecutor's Office
ESW	Egmont Secure Web
EU	European Union
Europol	European Police Office
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
G20	Group of Twenty
Irpef	Personal Income Tax
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	Italian Ministry of Economy and Finance
NRA	National Risk Assessment
NSPV	Special Unit of the Currency Police of the Finance Police
OAM	Organization of Agents and Mediators (Organismo degli Agenti e dei Mediatori)

OECD	Organization for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control (USA)
OO.II.	Investigative Bodies (Organi investigativi)
PEP	Politically Exposed Person
PI	Payment institution
NRRP	National Recovery and Resilience Plan
PSP	Payment Service Provider
RADAR	Collection and Analysis of AML Data (Raccolta e Analisi Dati AntiRiciclaggio)
SARA	Aggregate anti-money laundering reports (SARA reports)
SGR	Asset management companies (Società di gestione del risparmio)
SICAF	Fixed-capital investment companies (Società di investimento a capitale fisso)
SICAV	Open-ended investment companies (Società di investimento a capitale variabile)
SIM	Investment firm (Società di intermediazione mobiliare)
STR	Suspicious Transaction Report
TUB	Consolidated Law on Banking (Legislative Decree 385/1993)
TUF	Consolidated Law on Finance (Legislative Decree 58/1998)
TUIR	Consolidated Law on Income Tax (Presidential Decree 917/1986)
TULPS	Consolidated Law on Public Security (Royal Decree 773/1931)
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
VASP	Virtual Asset Service Provider
VAT	Value Added Tax